DAS WIRTSCHAFTSMAGAZIN ZUR DIGITALISIERUNG

# DIGITALE WELT

SCIENCE MEETS INDUSTRY

**Ausgabe 1** ▪ Januar ▪ Februar ▪ März ▪ **2022**

## Cyber Security

**Über die Absicherung komplexer Systeme**

## Social-Engineering

Wie unvorsichtige Mitarbeiter das Unternehmen gefährden

**RANSOMWARE**

Wenn die Daten plötzlich verschlüsselt sind

## Multi-Clouds

Wie verteilte Infrastruktur geschützt werden kann

## Automatisierte Abwehr

Wie KI von morgen schon heute gegen Cyber Angriffe schützt

Die stellvertretende Leiterin des Center für Security Studies der ETH Zürich über Cyber Warfare

**Dr. Myriam Dunn Cavelty**

# Ransomware
## Eine aktuelle und stetig steigende Bedrohung

**Norbert Pohlmann**

Laut dem Bericht „Die Lage der IT-Sicherheit in Deutschland 2021“, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), ist eine spürbare Ausweitung Cyberkrimineller Erpressungsmethoden, etwa mittels Ransomware, aktuell festzustellen.

Ransomware ist eine böswillige Schadfunktion in Malware, die Daten auf dem jeweils kompromittierten IT-System (Notebooks, PCs, Smartphone, Server…) verschlüsselt. Ziel eines Angreifers ist es, die Nutzung der Daten oder des ganzen IT-Systems durch die Verschlüsselung zu unterbinden. Dadurch kann der Angreifer vom Besitzer des IT-Systems oder der IT-Systeme für den Schlüssel, mit dem die Daten entschlüsselt werden können oder/und das IT-System wieder freigegeben wird, Lösegeld verlangen.

Das Lösegeld wird in der Regel über digitale Währungen wie Bitcoin oder andere Kryptowährungen bezahlt. Eine Möglichkeit zur Festlegung der Lösegeldforderung ist, dass die Angreifer dafür öffentlich verfügbare Informationen wie etwa der Unternehmensgröße, Umsatz und Gewinn nutzen. Bei Privatleuten wird in der Regel ein fester Betrag, oftmals 500 Euro, festgelegt.

Synonyme für Ransomware sind Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner.

Der Angriffsvektor Ransomware ist momentan sehr aktuell und wird zunehmend mehr eingesetzt, da er ermöglicht, einen sehr hohen Schaden auf unterschiedlichen Ebenen zu verursachen.

Beispiele von Ransomware-Angriffen auf Unternehmen:

**Benzinpipeline in den USA**
Der Betreiber der größten Benzinpipeline in den USA, Colonial Pipeline, zahlte Hackern ein Lösegeld von 4,4 Millionen Dollar. Der Ransomware-Angriff hatte zur Folge, dass die Kraftstoffversorgung landesweit vorübergehend eingeschränkt war.

**Uniklinikum Düsseldorf**
Den Angreifern gelang es, 30 Server des Uniklinikums zu verschlüsseln. Dadurch konnte das Klinikum die zentrale Notversorgung nicht mehr sicherstellen, sodass circa 1000 Patienten in umliegenden Krankenhäusern untergebracht werden mussten. Eine Notfallpatientin, die in eine weiter entfernte Klinik gebracht wurde, verstarb kurze Zeit später.

**Funke Mediengruppe**
Angreifer verschlüsselten mehrere IT-Systeme des Verlags im gesamten Bundesgebiet. Die Zeitungen „Westdeutsche

Allgemeine Zeitung“, „Hamburger Abendblatt“ und „Berliner Morgenpost“ konnten aufgrund der Ransomware-Attacke nur als Notausgabe erscheinen.

**Kammergericht Berlin**
Mehr als 500 Computer und über hundert Server mussten wegen einer Ransomware-Attacke vom Netz genommen werden. Daraus resultierte, dass das Kammergericht über mehrere Monate nur per Telefon, Fax oder Brief erreichbar war.

**Wichtig ist die Planung von Gegenmaßnahmen:**
Dazu gehören unter anderem bereits getestete Reaktionskonzepte (Notfallplanungen), in denen sowohl die richtige Vorgehensweise für den Angriffsfall definiert ist als auch bestimmten Personen die entsprechenden Rechte zuzuweisen, um die notwendigen Maßnahmen zu ergreifen. Besonders relevant ist dabei, alle definierten Reaktionen gemeinsam im Detail zu trainieren, damit im Ernstfall schnell und erfolgreich agiert werden kann.
Daneben lässt sich durch ein vollständiges, und auf Wiederherstellung geprüftes, Backup der IT-Systeme in vielen Fällen ein Schaden verhindern oder zumindest minimieren.
Das BSI unterscheidet in seinem Bericht zwei unterschiedliche Erpressungsmethoden bei Ransomware, die einzeln oder zusammen (Double Extation) Anwendung finden werden.

**Lösegelderpressung:**
Cyber-Erpresser verschlüsseln IT-Systeme und fordern Lösegeld für die Schlüssel, damit durch eine Entschlüsselung, dass IT-System wieder nutzbar ist.

**Schweigegelderpressung:**
Dies ist eine erweiterte Angriffsstrategie dahingehend, dass vor der Verschlüsselung von Daten diese zunächst unrechtmäßig entwendet wurden. Unternehmen, die über funktionierende Backups verfügten und sich von daher theoretisch nicht auf Lösegeldverhandlungen einlassen müssten, wird dann mit der Veröffentlichung der entwendeten Daten gedroht, um so das Schweigegeld zu erpressen.

Dies bedeutet, im Fall eines Ransomware-Angriffs muss nunmehr grundsätzlich auch davon ausgegangen werden, dass die Daten dauerhaft kompromittiert sind und zwar auch dann, wenn ein Lösegeld oder/und Schweigegeld gezahlt worden ist.

Aus diesem Grund ist der beste Schutz vor Ransomware, alle IT-Systeme mit einer modernen und sicheren Anti-Malware Lösung auszustatten und alle Mitarbeiter/Nutzer dahingehend zu schulen, dass sie aufgrund ihres Sicherheitsbewusstseins nicht auf gängige Angriffsvektoren reinfallen – also weder auf Anhänge von unbekannten/unaufgefordert zugesandten E-Mails noch auf Links von manipulierten Webseiten klicken. Aber auch das systematische Überwachen des Datentransfers hilft, ungewöhnliche Aktivitäten zu erkennen und so das Stehlen von Daten zu verhindern. Dies ist ein essenzieller Schritt, um das Risiko zu minimieren Opfer einer Schweigegelderpressung zu werden.

Fazit: Die Brisanz des Angriffsvektors zeigt, dass sich Unternehmen und Privatleute generell mit den Möglichkeiten sowie der Vermeidung von Ransomware-Angriffen auseinandersetzen müssen, damit sie alles tun, um einen Schadensfall zu vermeiden.

Prof. Dr. Norbert Pohlmann ist Professor für Cyber-Sicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco. Außerdem ist Prof. Pohlmann Mitglied des wissenschaftlichen Beirates der Gesellschaft für Datenschutz und Datensicherung – GDD und Mitglied im Lenkungskreis der Initiative „IT-Sicherheit in der Wirtschaft“ des BMWi sowie Mitglied der Advisory Group der European Union Agency for Cypersecurity der ENISA. 2011 wurde es als „Professor des Jahres“ in der Kategorie Ingenieurswissenschaften/Informatik“ ausgezeichnet.

Im Sommersemester 2013 war er als Gastprofessor an der Stanford University im Fachbereich Computer Science, Silicon Valley, USA. Die vielfältigen Fachartikel sowie mehrere Lehr- und Sachbücher auf dem Gebiet der Cyber-Sicherheit dokumentieren seine Passion für das Gebiet und machen ihn zu einem nachgefragten Experten für Interviews und Diskussionen.

16
MYRIAM DUNN CAVELTY
Ein Angriff aus Nullen und Einsen.





**LESEN SIE ONLINE MEHR**
Fachbeiträge
Kolumnen
Blogs

Die nächste **DIGITALE WELT** erscheint am 03.03.2022

Cover: Thitichaya Yajampa/Shutterstock, Privat Fotos: Thitichaya Yajampa/Shutterstock, Privat

QAR LAB

QUANTUM APPLICATIONS & RESEARCH LABORATORY

# Das QAR-Lab

Das Quantum Applications and Research Laboratory (kurz QAR-Lab) – im Jahr 2016 von der Informatik-Professorin Dr. Claudia Linnhoff-Popien der LMU München gegründet – hat die Mission, die Technologie des Quantencomputings (QC) einem breiten Nutzerkreis in Forschung und Wirtschaft zugänglich zu machen. Bereits 2019 wurde das QAR-Lab im Ranking als eine der „World's Top 12" Forschungseinrichtungen auf dem Gebiet des Quantencomputings durch „The Quantum Daily" international bekannt.

## Unsere Schwerpunkte

Als Gründungsmitglied des europaweit einzigartigen Leuchtturmprojekts PlanQK („Plattform und Ökosystem für quantenunterstützte KI") leistet das Lab Pionierarbeit dabei, die Quantencomputing-Technologie auf dem Gebiet der Künstlichen Intelligenz zu nutzen.

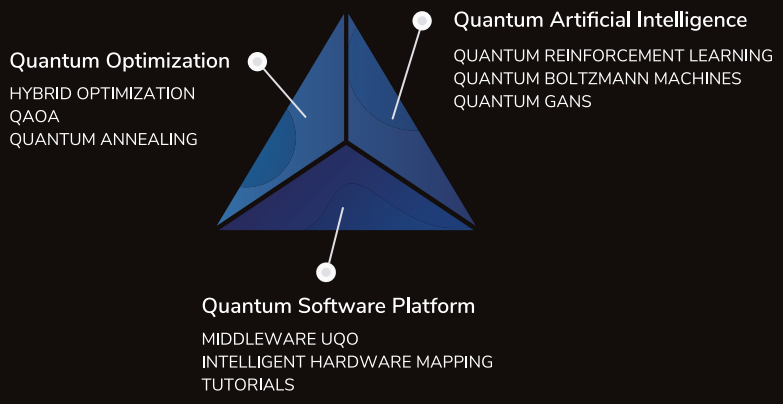
Das QAR-Lab hat – in Deutschland einzigartig – Zugang zu vier unterschiedlichen Quantencomputern und kann daher vergleichende Bewertung geeigneter Algorithmen durchführen.

Die Experten des QAR-Labs beschäftigen sich neben der Grundlagenforschung mit der Nutzung der Technologie für praxisnahe Anwendungen. Sie setzen auf Pilotprojekte für neue Technologien im Bereich QC und arbeiten an der Umsetzung von quantenunterstützten KI-Algorithmen für industrielle Use Cases im Rahmen von Forschungskooperationen mit großen Industriepartnern, die die Technologie erproben wollen.

Das QAR-Lab der LMU baut ein bayerisches Ökosystem für Anwenderkompetenz auf und stärkt den Standort München auf der deutschen Quantencomputing-Landkarte.

Finanziell gefördert wird das Lab seit 2019 vom Bundesministerium für Wirtschaft und Energie (BMWi) und seit 2020 vom Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie (StMWi).

## Unsere Forschungsschwerpunkte




BECOME QUANTUM READY!

## Kooperationsmöglichkeit mit dem QAR-Lab

Nutzen Sie die Expertise des QAR-Labs, um sich im internationalen Wettbewerb rechtzeitig Wissen über Quantencomputing anzueignen. In einer Kooperation mit dem QAR-Lab werden Sie von Anfang an kompetent unterstützt. Wir gehen mit Ihnen die ersten Schritte oder begleiten Sie den ganzen Weg.
Unsere Experten wissen, welche Quantenhardware für welche Herausforderungen in einem Betrieb am geeignetsten sind.

## Unser Ziel

**Schwere Anwendungsfälle**
Die Lösung mit heutigen Techniken braucht viel Rechenzeit oder geht gar nicht.

**Wichtige Anwendungsfälle**
Eine bessere/ schnellere Lösung hat einen großen Effekt, bspw. bei der Einsparung von Kosten oder der Verbesserung der Organisation.

**Passende Anwendungsfälle**
Es gibt ein (prospektives) Lösungsverfahren incl. QC-HW, das einen Vorteil bringt.

**Frühe Anwendungsfälle**
Eine QC-basierte Lösung ist relativ bald (schon mit NISQ?) umsetzbar.

**Kontaktieren Sie uns: www.qar-lab.de**

Prof. Dr. Claudia Linnhoff-Popien
Leitung QAR-Lab
Ludwig-Maximilians-Universität München
Oettingenstraße 67
80538 München
Telefon: +49 89 2180-9153
E-Mail: qar-lab@mobile.ifi.lmu.de

# DIGITALISIERUNG *in Zahlen*

*Laut einem Report von* **RouterNetwork** *werden in* **81%** *aller Data Breaches Passwörter geleakt.*

*Laut einer Studie der* **Harvard Business School** *und der* **New York University** *verlängerte sich die durchschnittliche Arbeitszeit im Homeoffice um rund* **50 Minuten** *pro Tag.*

*Die Firma* **NSO**, *welche die Spionagesoftware Pegasus entwickelt und verkauft, hat mehr als* **50.000** *Telefonnummern von Politikern, Managern, Journalisten, Regierungskritikern etc. auf ihrer Überwachungsliste.*

*Laut einer* **Bitkom**-*Umfrage gaben* **53%** *der befragten Berufstätigen Ende 2020 an, dass Digitalisierung das Berufsleben eher positiv verändert.*

*Laut einem Bericht von* **Amnesty International** *wurden mit der Spionagesoftware Pegasus mehr als* **600** *Politiker ausspioniert.*

*In den* **USA** *waren dieses Jahr mindestens* **200** *Firmen von Ransomware Angriffen betroffen.*

*Der Roboterhubschrauber „Ingenuity“ wurde von mehr als* **12.000** *Entwicklern via Open Source Beiträge auf* **GitHub** *unterstützt.*

*Laut einer Studie des Cybersecurity-Unternehmens* **Netskope** *hat die Verbreitung von Malware über die Cloud im zweiten Quartal 2021 um* **68%** *zugenommen.*

*Laut einem Report von* **Reportlinker.com** *wurden zwischen März und April über* **300.000** *Hacker-Webseiten registriert, die ihre Opfer mit coronavirus- und pandemiebasierten Schlüsselwörtern lockten.*

*Das* **Bundeswirtschaftsministerium** *hat einen Förderantrag für eine Open Source Business Alliance mit* **15 Mio.** *Euro über dreieinhalb Jahren bewilligt.*

Foto: 123RF

# Nur mit Vertrauen in die digitale Transformation

## Ein Gespräch mit Alexander von Gernler

Einst als zwischenmenschliche Kategorie für den soziale Umgang untereinander in den ethischen Kanon unserer Normen aufgenommen, so hat die zunehmende Digitalisierung ein neues Bewusstsein von Vertrauen generiert: Sind unsere sensiblen Daten, mit denen wir im Internet einkaufen oder unsere Bankgeschäfte tätigen, wirklich sicher? Oder wie sieht es mit den staatlichen Prozessen aus, die längst von der Funktionstüchtigkeit des Internets abhängen? Was passiert im Falle eines groß angelegten Hacker-Angriffes mit unserem Alltag? Die genua GmbH arbeitet an der IT-Sicherheit digitaler Infrastrukturen in komplexen, kritischen oder gesetzlich regulierten Umfeldern. Über die substanzielle Mitarbeit am Internet-Standard RFC 8391 zu Post-Quanten-Signaturen hat sich genua weltweit einen Namen gemacht. Für Alexander von Gernler, Abteilungsleiter für Research and Innovation, steht die IT-Sicherheit mehr denn je auf dem Prüfstand, denn nur mit Vertrauen gelänge die digitale Transformation.

**Gerade durch die Corona-Pandemie und deren Folgen hat sich wieder ein Stück mehr unseres Alltags in World Wide Web digitalisiert, was gerade die Fragen nach IT-Sicherheit verstärkt aufkommen lässt. Welche Rolle nimmt das Thema „Cyber-Security" für Sie ein? Beobachten auch Sie ein verstärktes Interesse an diesem Thema?**

Cybersicherheit ist selbstverständlich eines der Kernthemen für genua. Als Hersteller und Anbieter anspruchsvoller Sicherheitslösungen wie Firewalls, VPN-Gateways, Absicherungsmöglichkeiten für mobiles Arbeiten und einigen anderen Dingen ist gerade in der Pandemie dieses Thema keineswegs spurlos an uns vorüber gegangen.

Während wir also einerseits als Arbeitgeber selbst dafür sorgen mussten, dass alle unsere Angestellten möglichst schnell, reibungsfrei und sicher ins Pandemie-bedingte Home-Office wechseln konnten, mussten wir quasi gleichzeitig eine enorm gestiegene Nachfrage nach genau solchen Lösungen bedienen. Weil uns dieser Spagat geglückt ist, haben wir 2020 auch einen Rekordumsatz deutlich über Plan geschrieben, und auf die gestiegene Nachfrage sogar noch mit einem neuen Produkt geantwortet, das Mitte 2021 auf den Markt gekommen ist: Mit dem softwarebasierten VPN-Client genuconnect sind unsere anspruchsvolleren Kunden nun auch in der Lage, von ihrem Dienstnotebook aus Verbindungen in ihre Firma aufzubauen, über die sie selbst als VS-NfD (Verschlusssache – nur für den Dienstgebrauch) eingestufte Dokumente bearbeiten dürfen. Die Entwicklung und sogar die Zulassung der Lösung durch das BSI haben wir während der Pandemie in einer sehr sportlichen Zeit absolvieren können – und das alles mit einem bereits verteilt arbeitenden, crossfunktionalen Team.

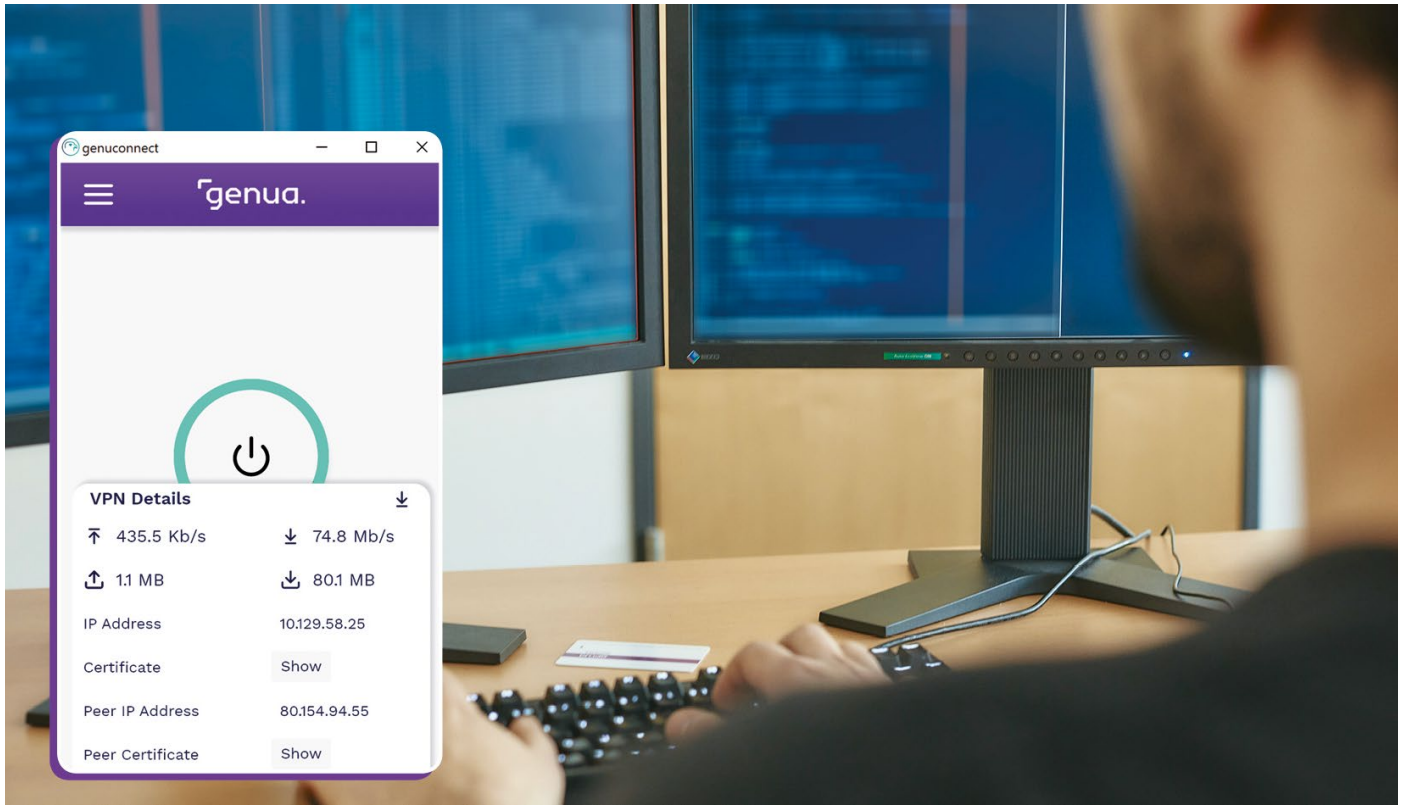
**Ist Cyber-Security ein Problem, das eher das Unternehmen oder das Individuum bedroht?**

Gemäß dem Prinzip „Follow the Money" würde ich sagen, dass eine Verschiebung in der Zielgruppe der Angreifer stattgefunden hat. Noch bis vor einem oder zwei Jahren war es vollkommen üblich, dass bei Privatleuten die Festplatte verschlüsselt wurde und diese dann um Lösegeldzahlung per Bitcoin-Transfer gebeten wurden. Daran hat die Angreiferseite wohl festgestellt, dass ihr Konzept prinzipiell sehr gut funktioniert und sich auf die Suche nach wertvolleren Zielen gemacht.

**„Heute kommen Angriffe auf Privatleute zwar noch vor. Den Hauptteil an Umsatz machen solche illegalen Unternehmungen aber damit, dass sie sich systematisch und organisiert Firmen vornehmen, und bei denen die Geschäftsdaten verschlüsseln."**

Heute kommen Angriffe auf Privatleute zwar noch vor. Den Hauptteil an Umsatz machen solche illegalen Unternehmungen aber damit, dass sie sich systematisch und organisiert Firmen vornehmen, und bei denen die Geschäftsdaten verschlüsseln. Eine Firma, die von so einem Angriff betroffen ist, steht dann vor der Wahl, hart zu bleiben und jeden Tag Hunderttausende oder Millionen von Umsatz zu verlieren, oder aber zu zahlen – in der Hoffnung, dass sie dadurch schneller wieder zum eigentlichen Geschäft zurückkehren kann.

Ich habe übrigens vorhin bewusst den Begriff „illegale Unternehmung" gewählt. Was wir sehen, ist eine Anwendung der arbeitsteiligen Wirtschaft auch bei den Angreifern. Hier werden Aufgaben verteilt, und zwar entlang der so genannten „Kill Chain", also der für einen erfolgreichen Angriff nötigen Schritte. Die eine Gruppierung kümmert sich um das Scouting




**Mit dem pandemiebedingten Trend zu Home-Office und Remote-Work erhöhen sich die Angriffsflächen für Cyber-Kriminelle. Um hochsensible Kommunikation zwischen z. B. einem Dienst-Notebook und einer Behörden-IT oder einer Unternehmenszentrale im Geheimschutzumfeld trotzdem zuverlässig zu schützen, helfen softwarebasierte VPN-Clients wie genuconnect.**

von Zielen, die andere besorgt Exploits für Sicherheitslücken, die dritte stellt Verschlüsselungs-Malware zur Verfügung usw. Oft sind solche Firmen auch mit Kenntnis oder wenigstens Duldung des Staates aktiv, in dem sie sitzen.

**Sicherer zu machen, heißt paradoxerweise nicht, gänzlich sicher zu sein. Was ist das größte Problem in puncto Cyber-Security, an dem Sie arbeiten? Was ist aus Ihrer Sicht die größte Herausforderung für die kommenden Jahre?**

Wir stehen einem vielfachen Wachstum gegenüber, das sich in seiner Zusammenwirkung leider potenziert: Einerseits wächst die schiere Anzahl der IT-Systeme, und wenn wir den Voraussagen gerade aus dem Feld der Internet of Things (IoT) glauben dürfen, dann stehen wir noch am Anfang der Entwicklung, was die Zahl mit dem Internet verbundener Rechner anbelangt.

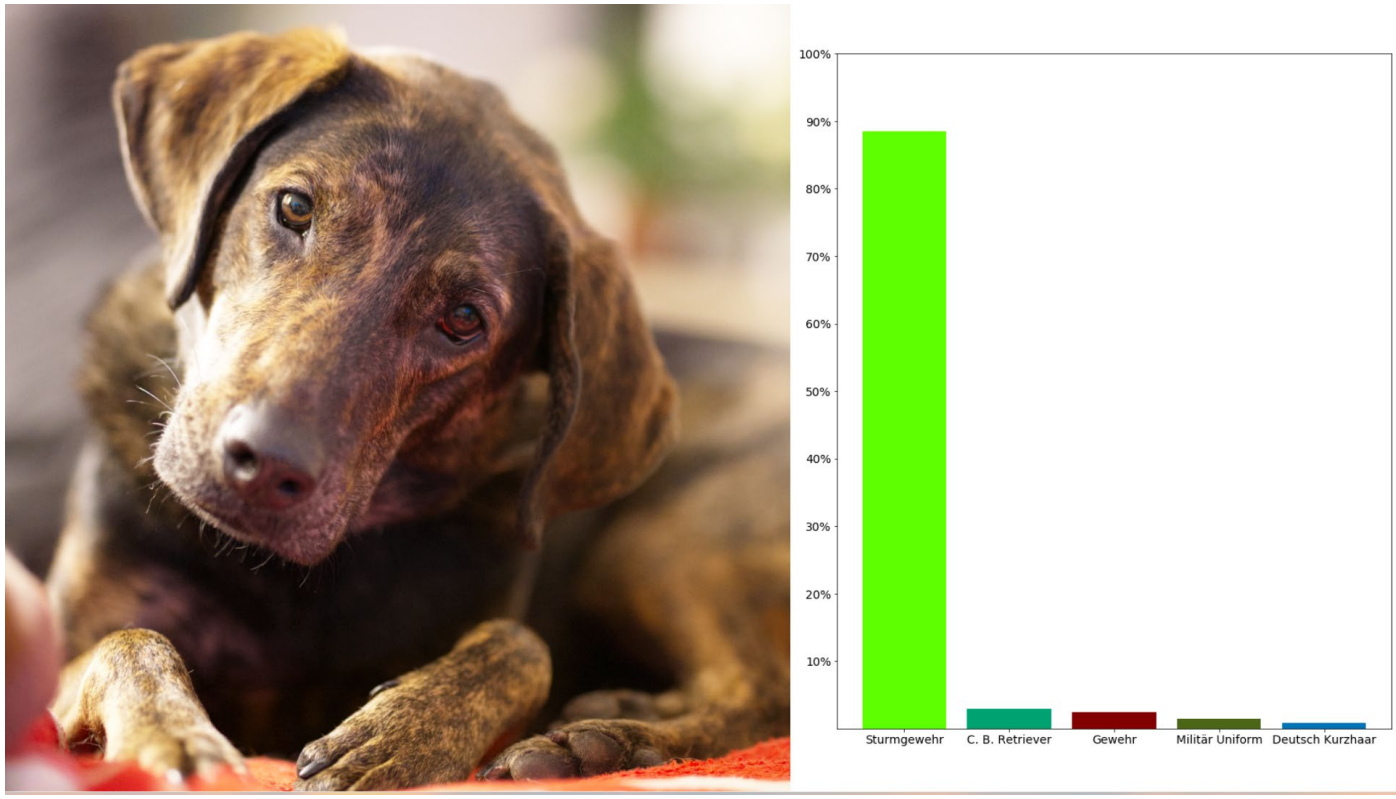
Zum anderen wächst die innere Komplexität von eingesetzten Komponenten. Führen Sie sich nur vor Augen, dass es damals in den 1980er Jahren möglich war, als einzelne Person einen Rechner wie den Commodore C-64 technisch völlig zu verstehen – die Komplexität war einfach so gering. Heutzutage scheitern Sie als einzelner Mensch bereits an Quellcode-Konglomeraten wie dem Linux-Kernel oder dem Firefox-Browser der Mozilla-Foundation. Das ist so viel Quellcode, das können Sie alleine nicht mehr überblicken. Und heutige Systeme sind aus vielen dieser sehr komplexen Komponenten zusammengesetzt. Dass sich damit Fehler und somit Sicherheitslücken einschleichen, ist zwangsläufig nicht vermeidbar.

Als Folge der ersten beiden Entwicklungen werden zum einen viel mehr Menschen benötigt, die IT-Systeme warten, in Betrieb halten und dafür auch zutreffende Sicherheitskonzepte entwerfen. Wir sehen aber gleichzeitig bei einem vorherrschenden Fachkräftemangel, dass es immer schwieriger wird, an qualifiziertes Personal zu kommen – auch und gerade bei Systembetreuenden. Nun trifft also eine erheblich vergrößerte Angriffsfläche auf immer stärker überfordertes und tendenziell schlechter qualifiziertes Personal.

Und als ob das noch nicht genug wäre, rüsten auch die Angreifer auf: Wo es viel Geld zu holen gibt, da kann ich mir auch als Angreifer gute Spezialisten einkaufen, die dann einerseits mit ihren eigenen guten Fähigkeiten hacken, andererseits aber auch Angriffstools entwerfen, die den Angriff etwa durch heuristische Algorithmen oder sogar maschinelles Lernen unterstützen.

**Wie bewerten Sie das verstärkte Aufkommen von Künstlicher Intelligenz und Quantencomputing? Sehen Sie hinter diesen mächtigen Technologien potenzielle neue Gefahren? Oder ist es genau andersherum: Lassen sich gerade diese Techniken dazu gebrauchen, für mehr Cyber-Security zu sorgen?**

Was neben dem bereits erwähnten Einsatz von KI auf der Angreiferseite oft vernachlässigt wird: KI-Algorithmen können




**Adversarial Attacks: Was für einen Menschen offensichtlich ist, kann für eine KI-Bilderkennungssoftware durch die Manipulation nur weniger Pixel zum Problem werden. So kann etwa ein Bild eines lieben Hundes nach einer subtilen Änderung von der KI als „Maschinengewehr" klassifiziert werden.**

auch selbst Ziel von Angriffen sein – je nachdem, was durch sie geschützt wird. Wie wir aus der Forschung im Bereich der adversarial attacks längst wissen, kann ich etwa einer bilderkennenden KI durch leichte, für das menschliche Auge nicht wahrnehmbare Änderungen Bilder unterschieben, die die KI dann völlig anders klassifizieren wird. So etwa ein modifiziertes Bild eines lieben Hundes, dass nach der subtilen Änderung von der KI als „Maschinengewehr" klassifiziert wird. Solche Angriffe sind immer denkbar, wenn eine KI etwas aufgrund von Eingabedaten von außen entscheiden soll. Wie auch schon in der klassischen IT-Security darf man halt den Eingabedaten nie restlos trauen.

Wie KI zur Erhöhung der Sicherheit benutzt werden kann, bearbeiten wir gerade konkret in einem unserer Forschungsprojekte. Ziel ist dort die „intelligente Firewall", die den Benutzenden einerseits ein besseres Lagebild zu ihrem Netz präsentiert und andererseits mit sinnvollen Handlungsvorschlägen zur Einrichtung von Netzrichtlinien (realisiert unter anderem etwa durch Firewall-Regeln) unterstützt.

**Und im Bereich Quantencomputing?**

Beim Quantencomputing ist für uns die stärkste Bedrohung für die IT-Sicherheit nach wie vor die Tatsache, dass funktionierende Quantencomputer mit den Algorithmen von Shor und Grover viele unserer heute verwendeten, so genannten „traditionellen" Kryptoverfahren wie RSA brechen oder andere Verfahren wie AES erheblich schwächen können. Das ist auch der Grund, warum wir zu dem Thema bereits das zweite Forschungsprojekt durchführen und ein drittes schon in der Beantragung haben. Die Erfolge aus dieser Bemühung können sich sehen lassen: So haben wir als mittelständisches Unternehmen an der Erschaffung des RFC 8391 zu Hash-basierten Signaturen nach dem XMSS-Verfahren mitgewirkt. Zudem wir liefern auch schon seit Jahren Softwareupdates und Patches für unsere Produkte nicht nur mit einer konventionellen Signatur aus, sondern zusätzlich mit einer Post-Quanten-Signatur nach dem erwähnten Verfahren.

Was die Erhöhung der Cybersicherheit durch Quantencomputer betrifft: Hier wäre eine andere Anwendung von Quanteneffekten, nämlich die so genannte Quantenkommunikation oder Quantum Key Distribution deutlich interessanter. In diesem Feld ist aber noch vieles sehr unsicher, und die Dinge schütteln sich erst. Wir beobachten die Entwicklungen dort aufmerksam, auch zusammen mit der Bundesdruckerei. Es wäre aber noch zu früh für ein abschließendes Urteil, was praktische Anwendbarkeit betrifft.

**Wo sehen Sie aktuell die größten Gefahrenquellen für Sicherheitslücken unseres digitalen Alltags? Wie sieht „Cyberkriminalität" tatsächlich aus? Was sind die häufigsten Cyberangriffstechniken?**

Ich habe mich vor kurzem wieder mal mit einem langjährigen Weggefährten getroffen, der im Themenfeld Incident Response und Cyberforensik unterwegs ist. Der hat immer eine

gepackte Reisetasche herumstehen und ist bereit, jederzeit irgendwo hinzufahren, wenn es brennt. Wenn also mal wieder ein Ransomware-Trojaner ein Krankenhaus verschlüsselt hat, oder Ähnliches. Sein Urteil war ernüchternd für mich:
Die meisten Angriffe gelingen nicht deshalb, weil die Angreifer über hoch spezialisiertes Wissen verfügen, das beste Skillset aufbieten können oder völlig überraschende Taktiken anwenden. Sondern die meisten Angriffe gelingen, weil die Angreifer auf jahrelang ungepatchte und auch ansonsten schlecht gewartete IT-Systeme treffen und sich mit absolut billigen Standardangriffen ihren Weg in das Firmennetz bahnen können. Auch innerhalb der Firmennetze wurden dann meist keinerlei weitere Sicherheitsvorkehrungen (so genannte „Defense in Depth“) getroffen. Oft hängt alles in einem flachen Netzsegment zusammen, ohne dass noch weiter mit kleineren Firewalls zoniert wurde.
Fazit: Wir würden schon deutlich besser da stehen, wenn einfach alle ihre Hausaufgaben machen würden, was die heute übliche Praxis bei der Absicherung von IT angeht. Netze zonieren; Belange separieren; Patches einspielen, wenn sie verfügbar sind; Warnmeldungen tatsächlich nachgehen; Offline-Backups einrichten, und das Wiedereinspielen tatsächlich ausprobieren; einen Notfallplan aufstellen und jährlich aktualisieren.

**Welche Rolle spielt das menschliche Verhalten selbst, wenn es um Cyber-Security geht?**

Der menschliche Faktor ist und bleibt das größte Problem. Sicherheit ist ja auch als Modell einer Kette darstellbar: Das schwächste Glied entscheidet, wann die Kette bei Zug reißt, und nicht das stärkste. Demzufolge sollten auch Ihre Sicherheitsmaßnahmen verhältnismäßig und aufeinander abgestimmt sein. Eine Panzertür in der Strohhütte nützt beispielsweise niemandem. So genannte Social-Engineering-Angriffe sind daher nicht zu unterschätzen.
Und so sind es oft die Menschen und ihre Motivation, anderen zu helfen, die ausgenutzt werden. Wie etwa beim so genannten „CEO Fraud“, in dem Mitarbeitende der Finanzbuchhaltung angeblich Mails von ihrem obersten Chef erhalten haben, doch dringend und sofort eine wichtige Überweisung zu tätigen. Hier wurde kein Hackertool eingesetzt, sondern nur eine täuschend echte Mail geschrieben.
Awareness ist also genau so wichtig wie das Einrichten technischer Maßnahmen – auch wenn sie viel schwieriger zu erreichen und auch zu quantifizieren ist.

**Hatten Sie selbst bei Ihrem Unternehmen auch schon Probleme mit Cyber-Attacken?**

Wir haben schon öfter mal Mails und auch Telefonanrufe erhalten, die zumindest sehr verdächtig waren und Social-Engineering-Angriffe gewesen sein könnten. Man kann die andere Seite ja leider nicht fragen, ob es wirklich so gemeint war. In allen von mir beobachteten Fällen wurde aber von den Betroffenen richtig gehandelt und Warnmails an alle Angestellten verschickt, dass verdächtige Anfragen beobachtet wurden.
Was härtere Angriffe wie Ransomware oder ein bewusstes Lahmlegen unserer IT angeht, so waren wir noch nie betroffen.

**Die renommierte Security-Studies Forscherin Dr. Myriam Dunn Cavelty sprach unlängst davon[1], dass wir uns bereits jetzt in einem „Cyberwar“ befänden. Was halten Sie von dieser Behauptung und wie bewerten Sie Gefahr eines „Cyber-Krieges“?**

Es ist naheliegend, dass die Staaten dieser Erde nun Cyber-Aktivitäten als kostengünstigere und lautlosere, vielleicht auch nicht mehr so eindeutig zuordenbare Möglichkeit für sich entdeckt haben, Konflikte mit verfeindeten Nationen oder Konfliktparteien auszutragen. Folgerichtig beobachten wir bei vielen Streitkräften dieser Erde die Herausbildung eigener Waffengattungen „Cyber“ neben den traditionellen Gattungen zu Land, zu Wasser und in der Luft. Bei einigen Streitkräften wurde diese Cyberfähigkeit auch vorher unter dem Mantel einer anderen Waffengattung (etwa Air and Space) hochgezogen.
Ich kann mir auch gut vorstellen, dass die Hemmschwelle beim Einsatz solcher Cyberwaffen sehr viel niedriger liegt, als einen konventionellen Waffengang zu starten. Dafür spricht ja auch, dass die Nachvollziehbarkeit (auch als attribution bezeichnet) solcher Angriffe zumeist schwierig ist. Und dass so etwas gemacht wird, sieht man ja nicht zuletzt am Stuxnet-Angriff auf die iranischen Atomanlagen.

**Und wie „real“ ist diese Gefahr eines „Cyber-Krieges“?**

Nicht nur in gut recherchierten Romanen wie Blackout von Marc Elsberg, sondern auch in realen Stromausfällen in Teilen Deutschlands als Folge von Unfällen oder Katastrophenlagen, sieht man, wie essenziell unsere Gesellschaft auf die Versorgung mit Strom angewiesen ist – sogar mehr als auf die Versorgung durch Trinkwasser. Strom ermöglicht alles, etwa das Betreiben eines Ölbrenners für die Zentralheizung, das Aufrechterhalten von Kommunikationsinfrastruktur, das Kühlen von Lebensmitteln in Lagerhallen oder im heimischen Kühlschrank.
Ein Cyberangriff auf vitale Teile der Stromversorgung hätte somit sicher katastrophale Folgen für die Gesellschaft. Und genau deshalb liegt der Gedanke nahe, dass sich die großen Mächte dieser Erde eine hohe Motivation haben, sich schon mal in Friedenszeiten guten Zugriff zu allen wichtigen solchen Stellen in anderen Ländern zu sichern – auch in befreundeten Staaten. Einfach, um im Ernstfall dann Hebel zu haben. Ob dies Irrsinn ist, bleibt dahin gestellt. Diese Frage würde sich ja auch bei der Aufrüstung mit nuklearen Waffen stellen, und trotzdem wird und wurde die nukleare Fähigkeit von vielen Staaten dieser Erde als wichtiger Bestandteil ihrer Sicherheitsdoktrin verfolgt.

**Wir sind durch die zunehmende Vernetzung und Verlagerung ins Digitale alle noch mehr miteinander verbunden. Das produziert zugleich eine größere Menge an Daten. Je mehr Daten ein Unternehmen etwa hat, umso größer**

**„Die meisten Angriffe gelingen nicht deshalb, weil die Angreifer über hoch spezialisiertes Wissen verfügen, das beste Skillset aufbieten können oder völlig überraschende Taktiken anwenden. Sondern die meisten Angriffe gelingen, weil die Angreifer auf jahrelang ungepatchte und auch ansonsten schlecht gewartete IT-Systeme treffen.“**

Fotos: genua

[1] https://www.zukunftsinstitut.de/artikel/der-cyberkrieg-ist-laengst-hier-interview/

**das Risiko für Cyber-Attacken. Warum? Wie hängen Big Data und Cyber-Security zusammen?**

Hier geht es meistens um lohnenswerte Datensätze wie Kundendaten, Login- und Passwortkombinationen oder Kreditkarten-Zahlungsdaten. Je größer der Kundenstamm eines Unternehmens, um so mehr solche wertvollen Daten sammeln sich zwangsläufig also an – und um so lohnender ist auch ein Angriff.

Den Begriff „Big Data" halte ich an dieser Stelle aber nicht für zutreffend. Unter Big Data verstehe ich nicht nur die Existenz einer erheblichen Menge von Daten, sondern auch ihre Nutzbarmachung durch Methoden der Data Science, gewissermaßen als manuelle Vorstufe für die Verarbeitung eben dieser Daten mit Mitteln des maschinellen Lernens. Der Klau von Kreditkartendaten erfordert dies aber gar nicht. Hier reicht der schlichte Verkauf der Daten auf dem Schwarzmarkt, oder aber das eigenhändige Benutzen dieser geklauten Daten.

**Glauben Sie an eine weitere Forcierung der Thematik Cyber-Security? Und welche Rolle wird fortan der Staat einnehmen, um für die IT-Sicherheit seiner Mitbürger zu sorgen?**

Auf dem Gebiet der Gesetzgebung passiert hier inzwischen eine Menge, und das Thema ist nicht nur international, sondern auch in Deutschland weit oben auf der Agenda. Denken Sie an die nicht unumstrittene Neuauflage des IT-Sicherheitsgesetzes oder an die ebenso heftig diskutierte Cybersicherheitsstrategie des Bundes 2021, die noch eben schnell vor Ende der Legislaturperiode durch die Organe forciert wurde.

Es wird auf jeden Fall der Zusammenhang zwischen einer sicheren und vertrauenswürdigen Infrastruktur auf der einen Seite und wirtschaftlichem Erfolg im digitalen Raum auf der anderen Seite gesehen. Ohne Vertrauen wird die digitale Transformation nicht stattfinden können.

Dummerweise befindet sich der Staat – nicht nur in Deutschland – aber in einem Zwiespalt: Auf der einen Seite ist es ein wichtiges Interesse, die gerade erwähnte Digitalisierung durch vertrauenswürdige Infrastruktur zu ermöglichen. Dazu ist eine Stärkung der digitalen Souveränität des Individuums nötig, was etwa mit einschließt, dass Produkte frei von Backdoors sein müssen oder dass es Kryptographie ohne hinterlegte Schlüssel für den Zugriff Dritter (so genanntem „Key Escrow") geben muss.

Dem entgegen steht das ebenfalls legitime Interesse eines Gemeinwesens, auf dem Gebiet der Gefahrenabwehr und der Strafverfolgung nicht ganz abgehängt zu werden. Was mache ich jetzt aber, wenn die Kriminellen genau die gerade erwähnte vertrauenswürdige Infrastruktur zu illegalen Zwecken benutzen? Man kann Backdoors ja nicht nur für die Bösen einbauen. Wenn sie aber überall drin wären, ist es nur eine Frage der Zeit, bis auch Dienste anderer Nationen, oder gar das organisierte Verbrechen solche Backdoors nutzen. Einfach deshalb, weil das Wissen darüber inzwischen genug diffundiert ist.

Das Dilemma beschäftigt die Gesellschaft schon eine Weile und geht bereits zurück bis auf die so genannten „Crypto Wars" der amerikanischen Bürgerrechtsbewegung. Es wird uns auch noch sehr lange begleiten, nehme ich an, da es keine einfache Lösung des Problems gibt.

**Zuletzt: Wie sieht Ihre Zukunftsvision einer sicheren digitalen Infrastruktur aus?**

Hierzu sollten wir über die Verschiebung von Diensten hin zu den großen Plattformen reden. Und zwar gar nicht so sehr wegen der oft kritisierten Quasi-Monopolstellung und der Plattform-Logik des „Winner takes it all". Ich glaube aber daran, dass ein funktionierender IT-Markt und das Ringen um die beste technische Lösung nur mit offenen Standards funktionieren kann. Wenn große Unternehmen standardisierte Schnittstellen anbieten müssten, so dass Amazon, Facebook, Google und Konsorten auch kleinere Anbieter mit an den Kuchen ranlassen müssten, dann könnte das ebenso wie das Wirken unserer Regulierungsbehörde (jetzt Bundesnetzagentur) in den Bereichen Strom oder Eisenbahn die Monopole ein Stück weit aufbrechen und echten Wettbewerb wieder ermöglichen.

**„Es wird auf jeden Fall der Zusammenhang zwischen einer sicheren und vertrauenswürdigen Infrastruktur auf der einen Seite und wirtschaftlichem Erfolg im digitalen Raum auf der anderen Seite gesehen. Ohne Vertrauen wird die digitale Transformation nicht stattfinden können."**

Und das würde auch nationalen Anbietern erlauben, hier mitzumischen. Denn in der digitalen Welt der Zukunft geht es nicht mehr so sehr darum, dass OpenSource-Software eingesetzt wird, sondern dass Sie derjenigen Partei vertrauen können, die einen Dienst für Sie anbietet. Wenn das Vertrauen weg ist, dann hilft es auch nichts, wenn der Dienstanbieter seinen Dienst auf OpenSource realisiert. Aber vielleicht trauen Sie ja einer deutschen Firma, die nach DSGVO handeln muss und von deutschen Datenschutzbeauftragten kontrolliert wird mehr als etwa einem US- oder einem chinesischen Anbieter. Und damit das geht, brauchen wir – wieder – die Orientierung an offenen Standards.

Interview: Hannes Mittermaier

## Alexander von Gernler

Alexander von Gernler leitet bei genua die Abteilung Research and Innovation. Frühere Stationen seiner beruflichen Laufbahn führten ihn vom Software-Entwickler über den Scrum Master hin zum Technischen Botschafter von genau sowie zum Leiter der Forschung.

Alexander von Gernler ist ehemaliger Junior Fellow sowie Vizepräsident der Gesellschaft für Informatik e.V. (GI). Er ist außerdem in der Studiengruppe Digitalisierung der Vereinigung Deutscher Wissenschaftler e.V. (VDW) engagiert. Er leistet regelmäßig Debattenbeiträge zum Thema, wie etwa in der Süddeutschen Zeitung, im Redaktionsnetzwerk Deutschland oder in Veröffentlichungen der Nationalen Akademie der Technikwissenschaften acatech.

Fotos: genua

# MULTITASKING ERFORDERLICH FÜR AGILES ARBEITEN?

Kürzlich rief mich eine Freundin an. Sie wirkte aufgeregt, es rauschte und knatterte in der Leitung. Bevor sie zum Grund ihres Anrufs kam, zwitscherte sie drauflos: „Ich trainiere jetzt multitasking: Gerade radle ich in mein Büro und telefoniere gleichzeitig über Kopfhörer mit meinen Kunden. Ist das nicht toll!“ Ich war gar nicht begeistert. Erstens mag ich keinen ohrenbetäubenden Krach im Kopf. Zweitens finde ich, dass der Straßenverkehr in München vor allem für Radler höchste Konzentration erfordert. Und drittens braucht unser Gehirn dafür kein Training. Denn es ist ständig im Multitasking-Modus. Viele Prozesse laufen gleichzeitig ab, die allermeisten automatisch und unbewusst.

Vielleicht kennen Sie das: Sie sitzen in einem Meeting, sind voll konzentriert auf die Teilnehmer, hören auf das, was der Moderator gerade sagt, und plötzlich richten Sie Ihren Blick auf etwas Schwarzes am rechten Rand Ihres Gesichtsfelds – eine dicke Hummel am Fenster. Ihr Gehirn scannt ständig mit seinen Sinnesorganen die Umgebung ab, allerdings erreichen die verarbeiteten Informationen nur dann das Bewusstsein, wenn etwas Ungewöhnliches aufgenommen wird. Wenn es nicht nur ungewöhnlich, sondern bedrohlich zu sein scheint, übernimmt das Stammhirn und sichert mit dem Autopiloten unser Überleben. Dabei schaltet es das Frontalhirn ab, das für genaue Analyse und Planung verantwortlich ist, und deshalb im Überlebensmodus nicht schnell genug wäre.

Vielleicht kennen Sie auch diese Situation? Sie fahren mit Ihrem Auto nach Hause. Ihre Gedanken drehen sich um ein bestimmtes Problem des Tages und die Frage, was es zum Abendessen geben soll. Wenn die Rücklichter vor Ihnen plötzlich rot werden, richtet sich die bewusste Aufmerksamkeit genau darauf, und unterbewusst treten wir voll auf die Bremse ... dem Multitasking und Autopiloten im Gehirn sei Dank.

Und sicherlich kann man in einem Telefonat zuhören und gleichzeitig einen Film sehen. Ob man dann wirklich alles „mitkriegt“ – sei es im Telefonat oder im Film – ist die Frage, hier funktioniert Multitasking also nur bedingt.

Bei parallelen Prozessen, in die jeweils das Frontalhirn einbezogen ist, funktioniert Multitasking nicht wirklich. Ein Beispiel: Sie versuchen telefonisch mit einem Kollegen ein Drucker-Problem zu lösen und stimmen gleichzeitig im Chat mit Kunden Termine ab. Wenn man versucht, diese beiden Fontalhirn-Aufgaben gleichzeitig zu erledigen, dauern sie insgesamt länger, der Stresspegel steigt, die Fehlerquote ebenso. Sehr wahrscheinlich merkt Ihr Telefonpartner auch, dass Sie unkonzentriert sind. Wenn Multitasking also die gleichzeitige Bearbeitung von mehreren unabhängigen bewussten Aufgaben leisten soll, funktioniert es nicht. Dafür ist unser Frontalhirn nicht ausgelegt, es arbeitet am effektivsten seriell, mit regelmäßigen kurzen Pausen, damit die Energieversorgung im gesamten Gehirn stimmt.

Effektive Pausen sind Achtsamkeitsrituale, eine Atemübung, ein mentales Entspannungsbild. In solchen kurzen Momenten sind wir mit einer besonderen Qualität des Seins im Kontakt. Andere Dinge versinken, die Welt dreht sich nur noch um diesen unseren aktuellen Fokus.

Mit Übungen dieser Art verändert sich die Struktur des Gehirns, über ein MRT messbar. Die Dichte der grauen Substanz nimmt zu, das führt zu einer Funktionsverbesserung in den Gehirnarealen, besonders dem Hippocampus – der u.a. für Informationsverarbeitung und Lernen verantwortlich ist. In diesem Bewusstsein für den Moment entsteht die kleine Pause, die das Hamsterrad stoppt, den Arbeitsspeicher unseres Gehirns vor Overflow schützt und unseren Stoffwechsel für weitere Phasen der Höchstleistung elastisch hält. Positive Momente dieser Art im „Hier und Jetzt“ – mal intensiver, mal weniger intensiv – sind wie Perlen an der Schnur verantwortlich für unser Wohlbefinden, damit für unsere psychische Gesundheit und unsere Leistungsfähigkeit.

**Weitere Tipps finden Sie unter www.mentaleintelligenz.de und in meinem gerade erschienenen Buch! Herzlichst Ihre Petra Bernatzeder,**
**Diplom-Psychologin, Coach, Expertin für mentale Intelligenz, www.upgrade-hr.com**

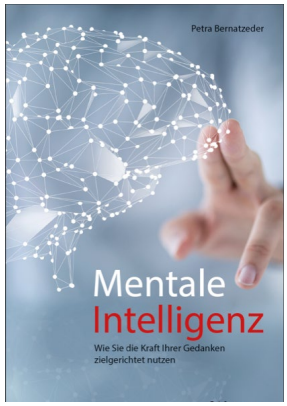



Foto: Privat

# Die Crux mit den Daten

## Ein Gespräch mit Nikolaus Angster

Sie nehmen in rasanter Manier zu: unsere Daten. Gerade das, was die digitale Transformation produziert, ist ein gewaltiger Haufen an Daten, der zur beruflichen Aktivität am Arbeitsplatz, zum Kommunizieren von Großunternehmen, aber auch zum privaten Austausch unter Freunden genutzt wird. Dass die Datenmenge nicht kleiner wird, ist zweifellos annehmbar; dass die Sensibilität um unsere Daten ob ihrer enormen Menge aber leiden könnte, ist eine berechtigte Befürchtung. Es geht also um die Sicherheit, um das Vertrauen und um die Verschlüsselung sensibler Daten, die eben nicht öffentlich im digitalen Äther herumschwirren sollen. DataGuard hat sich auf diese Aspekte fokussiert. Nikolaus Angster, Wirtschaftswissenschaftler und Privacy Tech Consultant, berichtet über die aktuellen Herausforderungen.

**Eine simple Frage mit womöglich weitreichenderen Folgen wird im Zusammenhang mit IT-Sicherheit immer wieder gestellt. Wie antworten Sie auf diese Frage: „Was passiert eigentlich mit meinen Daten?“**

Um diese Frage zu beantworten, ist eine Analyse und Bewertung der zugehörigen Datenverarbeitungsprozesse notwendig. Als regulatorisches Rahmenwerk kann die Datenschutzgrundverordnung (DSGVO) hier als Orientierungshilfe dienen. Gemäß Art. 13 Abs. 1 DSGVO hat die von der Datenverarbeitung betroffene Person jederzeit das Recht, Informationen zu den verarbeiteten Daten zu erlangen. Konkret bedeutet dies, dass Sie als Betroffener einer Datenverarbeitung sowohl die Kategorien der Daten und die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, als auch die Rechtsgrundlagen für die Verarbeitung und die Empfänger der Daten erfragen können. DataGuard ermöglicht Unternehmen die Analyse, eine effiziente Dokumentation und transparente Kommunikation der eigenen Datenverarbeitungsprozesse.

**Welche Mission verfolgen Sie, wenn es um dieses Thema Datenschutz geht?**

Als Technologie-Unternehmen verfolgt DataGuard eine klare Mission: „Protect the people behind the data“ – wir schützen die Menschen, die von Datenverarbeitungsprozessen betroffen sind. In der Praxis finden sich Unternehmen im Wettbewerb oft großen Herausforderungen ausgesetzt. Als externer Datenschutzbeauftragter ermöglicht DataGuard diesen Unternehmen, die regulatorischen Anforderungen des Datenschutzes zu meistern und den Unternehmenserfolg durch eine systematische, risikoorientierte und dokumentierte Datenverarbeitung abzusichern.

Welche konkreten Lösungen bieten Sie Ihren Kunden an, um ein Unternehmen IT-sicher zu machen?

Bei DataGuard bieten wir unseren Kunden mit „Datenschutz-as-a-Service“ eine Kombination aus Expertenberatung und einer digitalen Plattform zur Digitalisierung und effizienten Umsetzung von Datenschutzthematiken. Kernbestandteil dieser Leistung ist der Bereich IT & Sicherheit. Im Zusammenspiel mit dem Kundenunternehmen führen unsere zertifizierten Branchenexperten eine Lückenanalyse in Bezug auf das vorhandene Datenschutzniveau durch. Hier werden unter anderem die physische Infrastruktur (wie Zutrittskontrollen), IT-Infrastruktur (etwa eingesetzte Serversysteme und Tools) und organisatorische Prozesse (wie Richtlinien und Berechtigungskonzepte) geprüft, um auf ein angemessenes Datenschutzniveau gemäß DSGVO hinzuarbeiten. Unsere Handlungsempfehlungen hinsichtlich der technischen und organisatorischen Maßnahmen orientieren sich zudem an Best Practices anderer Normen, wie der ISO 27001. Seit 2021 bieten wir mit unserer „Informationssicherheit-as-a-Service“-Lösung eine zusätzliche Leistung, die Unternehmen auf dem Weg hin zur Implementierung eines eigenen Informationssicherheits-Managementsystems (ISMS) unterstützt.

**Wie bewerten Sie die Differenz zwischen einem Unternehmen, also einem Kollektiv, und der Rolle der einzelnen Individuen eines Unternehmens?**

Sowohl für den Datenschutz als auch die Informationssicherheit ist es besonders wichtig, dass die Unternehmensführung klare Ziele und Werte, aber auch konkrete Hilfen und Handlungsanweisungen an die Beschäftigten kommuniziert. Denn: Sicherheit kann in Unternehmen nur dann ganzheitlich funktionieren, wenn ein gemeinsames Bewusstsein für datenschutzrechtliche und informationssicherheitsrelevante Thematiken geschaffen und dieses auch gelebt wird. Nur wenn ein Unternehmen beispielsweise im Zusammenspiel mit einem externen Datenschutzbeauftragten seinen Beschäftigten das notwendige Know-how und die Ressourcen zur Verfügung stellt, können die einzelnen Mitarbeitenden am Ende des Tages erfolgreich zur Einhaltung der regulatorischen Anforderungen beitragen.

**„Sicherheit kann in Unternehmen nur dann ganzheitlich funktionieren, wenn ein gemeinsames Bewusstsein für datenschutzrechtliche und informationssicherheitsrelevante Thematiken geschaffen und dieses auch gelebt wird.“**

**Gewährleistet das Maximum an IT-Sicherheit eine tatsächliche Sicherheit oder lediglich eine hohe Wahrscheinlichkeit? Welche Bedrohungen stufen Sie derzeit als die am gefährlichsten ein?**

Datenschutz und Informationssicherheit sind die Voraussetzungen für eine erfolgreiche und nachhaltige Digitalisierung. Doch: Je mehr Assets, also Unternehmenswerte, im digitalen Raum angesiedelt sind, desto wichtiger wird auch die IT-Sicherheit dieser Werte. Das heißt jedoch nicht zwangsläufig, dass durch bestimmte Maßnahmen hundertprozentige Sicherheit gewährleistet werden kann. Ziel sollte immer eine Analyse der Risiken im konkreten Kontext des Unternehmens sowie eine Bewertung und Entwicklung einer Behandlungsstrategie sein. Im Datenschutz werden die Risiken von Datenverarbeitungsprozessen aus der Sicht der betroffenen Personen betrachtet und bewertet.

Gleichzeitig bietet die Informationssicherheit eine Übersicht zu allen Risiken, die für Organisationen kritische Informationswerte (wie Geschäftsgeheimnisse) darstellen.
Neben den weiterhin relevanten Bedrohungen wie Ransomware- und Distributed-Denial-of-Service (DDoS)-Attacken ist im Jahr 2021 außerdem die stark wachsende Menge an Schadprogrammen zu beachten. Das Bundesamt für Sicherheit in der Informationstechnik verzeichnet im Lagebericht für 2021 beispielsweise eine Steigerung von 22 Prozent an neuen Schadprogrammen gegenüber dem Vorjahr.

**Wie bewerten Sie die Kategorie „Vertrauen“ im digitalen Umgang unseres Alltags? Was heißt in diesem Zusammenhang „Vertrauen“ für Sie?**
Vertrauen spielt eine sehr zentrale Rolle, denn es ist gleichzeitig für den Erfolg von Kunden- und Geschäftspartnerbeziehungen relevant. Wer die Sicherheits- und Datenschutzbedenken potenzieller Kunden und Partner ernst nimmt und in seiner Unternehmensstrategie berücksichtigt, legt den Grundstein für eine erfolgreiche Dienstleistungserbringung im digitalen Zeitalter. Die Implementierung angemessener Sicherheitsmaßnahmen sowie die transparente Information und Kommunikation zu diesen bilden hier die Basis für das Vertrauen, welches am Ende über die Nutzung und den Erfolg von Produkten und Dienstleistungen entscheidend sein kann. Zum Beispiel können leicht zugängliche und vor allem verständliche Datenschutzhinweise nachweislich zur Reduzierung der Komplexität und Unsicherheit bei möglichen Interessenten beitragen.

**„Häufig bilden individuelle Fehler und mangelnde Sensibilisierung für Sicherheitsthematiken die Einfallstore für kriminelle Machenschaften.“**

**Was ist die größte Herausforderung der nächsten Jahre, wenn es um unsere IT-Sicherheit geht?**
Problematisch ist die Vernetzung von digitalen Assets in unserem Alltag, die allerdings für Endnutzer praktisch ist. Denn immer öfter sind ganze Lieferketten im Fokus von Angriffen und dadurch nicht nur die Unternehmen, sondern auch deren Kunden oder unbeteiligte Dritte betroffen.
Bei solchen Angriffen suchen die Angreifer aktiv nach Schwachstellen, um Quellcodes abzuändern und Schadprogramme unerkannt in Patch- und Updateprozesse einzubinden. So kann schädlicher Code, oftmals signiert und zertifiziert von vertrauenswürdigen Anbietern, in fremde Systeme eingespielt werden. Bei Lieferkettenangriffen besteht die Schwierigkeit für die betroffenen Unternehmen darin, rechtzeitig zu erkennen, dass ihre Software mit Schadprogrammen infiziert ist, bevor diese für die Nutzung freigegeben werden. Je nach Vernetzungsgrad und Nutzerzahlen einzelner Dienste ist die Anzahl an potenziellen Betroffenen solcher Attacken erheblich.

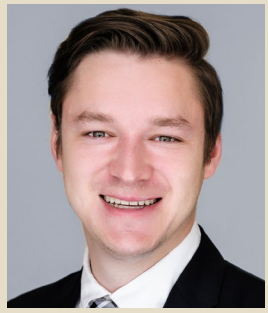
**Welche Rolle spielt die Komponente „Mensch“ im Bereich IT-Sicherheit? Oder umgekehrt: Wie gehen Sie mit dem Faktor Mensch um neben der Implementierung von Software-Lösungen?**
Die Komponente „Mensch“ spielt im Bereich IT-Sicherheit eine sehr zentrale Rolle. Denn nicht nur die Verantwortlichen für die Sicherheitsprozesse innerhalb der Unternehmen müssen von geschulten Experten besetzt werden. Häufig bilden individuelle Fehler und mangelnde Sensibilisierung für Sicherheitsthematiken die Einfallstore für kriminelle Machenschaften. Zum Beispiel können Angreifer über eine einfache Phishing-E-Mail genau an diejenigen Informationen der Zugriffsrechte gelangen, die für die Ausführung weiterer kritischer Angriffe (wie einem Lieferkettenangriff) notwendig sind. Dementsprechend stellen die Sensibilisierung der Mitarbeiter und Gestaltung von Awareness-Maßnahmen zentrale Kerngebiete des Datenschutzes und der Informationssicherheit dar.

**Was ist die „Datenschutz-Plattform“, die Sie für Ihre Kundschaft anbieten?**
Unsere webbasierte Plattform ist der Dreh- und Angelpunkt unserer Lösung. Kunden finden darin priorisierte To-dos, rollenspezifische Mitarbeiterschulungen, eine organisierte Dokumentation ihrer Prozesse sowie zeitsparende Tools, die ihnen bei der langfristigen Umsetzung ihrer Compliance helfen. Das Ergebnis ist eine „Single Source of Truth“ für das gesamte Unternehmen. In Kombination mit der persönlichen Betreuung durch unsere Datenschutz- und Informationssicherheitsexperten können also jegliche regulatorische, Partner- oder Kundenanforderungen mit nur minimaler Beeinträchtigung des Tagesgeschäfts umgesetzt werden. Zusätzlich dient die Plattform als schneller Kommunikationskanal zu den betreuenden Experten oder zur Zusammenarbeit mit Partnern, die in bestimmte Bereiche der Plattform eingeladen werden können.

**Zuletzt: Wie sieht Ihre Zukunftsvision einer sicheren digitalen Infrastruktur aus?**
Das Ziel für Anbieter muss sein, über Transparenz und Kommunikation die Komplexität und Unsicherheit auf Nutzerseite zu reduzieren. Regulatorische Rahmenwerke wie die DSGVO bieten eine Grundlage dafür, technische Funktionen und Datenverarbeitungsprozesse für die betroffenen Personen verständlich zu machen. Für Unternehmen geht es hier einerseits um die Erfüllung der erwarteten und geforderten Sicherheitsmindeststandards, andererseits um eine erfolgreiche Dokumentation und Aufklärungsarbeit, um das Vertrauen in die bereitgestellten Dienste zu erhöhen. Die Zukunftsvision einer sicheren digitalen Infrastruktur stellt hier gleichzeitig den ausschlaggebenden Differentiator für zukunftsorientierte Unternehmen dar: Technologien und Infrastrukturen sollten durch die Implementierung technischer und organisatorischer Maßnahmen ausreichend Vertrauen für eine Akzeptanz und Nutzung schaffen, die für Anbieter und Nutzer gleichermaßen wertschaffend ist.

Interview: Hannes Mittermaier


**Nikolaus Angster**



Nikolaus Angster ist Wirtschaftswissenschaftler und Privacy Tech Consultant bei DataGuard. Im Rahmen verschiedener Compliance-Projekte beschäftigt er sich seit 2016 mit den vielfältigen Herausforderungen der Cyber Security. Dabei hat er insbesondere in der Unternehmensberatung internationale Logistik- und Finanzdienstleistungskonzerne zu komplexen Problemstellungen der Informationssicherheit und des Datenschutzes begleitet. Als Schlüssel für ein wirksames Management von Sicherheitsrisiken verfolgt er in seiner Arbeit einen risikoorientierten Ansatz – mit dem Ziel, den Unternehmenserfolg durch eine systematische und nachhaltige Datenverarbeitung abzusichern.


Foto: DataGuard

# Ein Angriff aus Nullen und Einsen.

## Über den Cyberspace als Kriegsschauplatz von heute. Ein Gespräch mit Myriam Dunn Cavelty

Die zunehmende Digitalisierung unserer Informationssysteme ist ein Paradies für böswillige Machenschaften, weil es das ideale Terrain bietet, um selbst staatsinterne Prozesse auszukundschaften oder gar lahmzulegen. Was also vermehrt in die Diskussion kommt, ist die Frage um unsere digitale Sicherheit. Blickt man auf den Spezialfall eines militärischen Konflikts zwischen zwei Staaten, so ist das World Wide Web und alles, was mit ihm zusammenhängt, längst zum entscheidenden Operator in der Kriegsführung geworden. Der Sammelbegriff „Cyberwar" umschreibt die Machenschaften des „digitalen" Kriegführens. Myriam Dunn Cavelty, Dozentin für Security Studies und stellvertretende Leiterin des Center for Security Studies (CSS) der ETH Zürich, beschäftigt sich ausgiebig mit dem Thema und wagt die pessimistische Voraussicht: Einen absolut sicheren digitalen Raum wird es nicht geben.

**„Cyberwar", also zu Deutsch „Cyberkrieg", ist ein verhältnismäßig junges Wort. Es taucht zum ersten Mal 1993 bei den Wissenschaftlern John Arquilla und David Ronfeldt auf. Was ist aus Ihrer Sicht der erste historisch datierbare Krieg, der als „Cyberwar" gelten kann?**

Die Frage kann man nur beantworten, wenn man den Begriff klar definiert: Für eine differenziertere Sicht ist es hilfreich, zwei Arten des Cyberkriegs zu unterscheiden, nicht zuletzt, weil der „Krieg" eine sehr spezifische und relativ seltene Form der Gewaltanwendung ist.

Zum einen gibt es den strategischen Cyberkrieg. Er bezeichnet eine Form der Kriegführung zwischen Staaten, bei denen ein Cyberangriff aus dem Nichts kritische Infrastrukturen lahmlegt oder zerstört, mit sehr gravierenden Konsequenzen. Die Form der politischen Auseinandersetzung würde fast ausschließlich digital stattfinden. Diese Art des „Kriegs", die wir aus gewissen Hollywoodfilmen kennen, wurde vor allem in den Anfängen der Debatte häufig dazu verwendet, um schwarzmalerische Zukunftsszenarien an die Wand zu malen, in denen die technologisierte Gesellschaft als dem Untergang geweiht dargestellt wird, wenn nicht sofort Maßnahmen im sicherheitspolitischen Bereich ergriffen. Diese Art des Cyberkriegs gab es noch nie – und wird es ziemlich sicher nie geben.

**„Ganz wichtig ist aber, dass es nicht möglich ist, einen Krieg durch Cybermittel zu gewinnen."**

Die zweite Form ist der operationelle Cyberkrieg. Diese Form ist „unterstützend", d.h. anderen Formen der kriegerischen Auseinandersetzung untergeordnet. Sie ist im Gegensatz zu der eben besprochenen Form längst Realität: Jede politische Auseinandersetzung hat heutzutage eine Cyberkomponente. Schon im Kosovokonflikt 1998 gab es ausgehend vom US-Militär Konzepte, wie der Informationsraum strategisch und politisch eingesetzt werden sollte, damals meisten unter dem Schlagwort „Information Operations".

**Gäbe es heutzutage wieder Krieg zwischen Industrienationen, wäre dieser Krieg nicht immer ein operationeller Cyberwar? Heißt das, dass potenziell jeder Krieg von nun an auch teils ein Cyberwar sein wird?**

So ist es. Je stärker computerisiert und digitalisiert die Streitkräfte und die Gesellschaft sind, desto mehr „Cyber"-elemente finden sie in einer Auseinandersetzung. Dabei sind viele der zugrundeliegenden Konzepte „alt" – denken Sie z.B. an die Elektronische Kriegführung oder was in der Militärstrategie „Enthauptungsschlag" genannt wird, also ein Angriff auf die politischen und militärischen Führungsstrukturen eines Gegners. Die Ziele sind die gleichen, nur die Mittel haben sich verändert. Ganz wichtig ist aber, dass es nicht möglich ist, einen Krieg durch Cybermittel zu gewinnen. Nicht nur weiß man aus Erfahrung, dass es kaum möglich ist, die Effekte so zu kontrollieren, dass sich Cybermittel für strategische, gezielte Einsätze à la „Bomben" eignen, auch ist es längst klar, dass sich kein Staatsterritorium durch Cybermittel kontrollieren lässt. Cyberoperationen werden daher immer nur ein begleitendes Phänomen sein.

**„Es zeichnet sich nämlich ab, dass die unliebsamen, destabilisierenden Effekte vor allem über den eigenen politischen Diskurs und die Medien generiert werden."**

**Welche Methoden der Kriegsführung kann dann ein von Ihnen beschriebener Cyberwar umfassen?**

Ich denke, nun sollten wir uns um die Frage kümmern, wofür sich Cybermittel denn am besten eigenen, wenn nicht für Einsätze im klassisch militärischen Sinn. Seit rund zehn Jahren sieht man, dass staatliche Akteure Cyberkapazitäten aufbauen, im offensiven und im defensiven Bereich. Häufig werden dafür Organisationseinheiten geschaffen, die als „Cyber-Kommandos" bezeichnet werden. Diese Einheiten bereiten sich auf Kriege im Cyberspace vor, wobei der Schutz der eigenen militärischen Netzwerke oftmals im Zentrum steht.
Um aber die sicherheitspolitischen Entwicklungen und digitale Vorfälle der letzten Jahre einordnen zu können, müssen wir den Fokus darauf richten, wie Staaten unter der Kriegsschwelle, im hybriden, „grauen" Bereich, operieren – dafür ist nicht das Militär, sondern der Nachrichtendienst zuständig. Militärische Auseinandersetzungen sind u.a. durch das Völkerrecht stark reglementiert. Nachrichtendienste hingegen nutzen den Cyberspace im Namen der Informationsbeschaffung seit Jahren ohne klare Regeln. Dieses andauernde „Austesten" von roten Linien hat Lucas Kello treffend als „Un-peace" (also Nicht-Frieden) bezeichnet.

**Beschreiben Sie ein Szenario konkreter: In unserem Gedankenspiel wird ein führender Industriestaat durch einen Cyberangriff belagert. Wie könnte dieser aussehen? Ab wann könnte ein Staat kollabieren? Wie schlägt der virtuelle Angriff um auf die tatsächlichen, materialen Infrastrukturen eines Staats?**

Schauen wir uns die Realität an: Staatliche Akteure dringen hauptsächlich in die Netzwerke anderer Staaten ein, um geheime und strategisch wertvolle Daten zu stehlen. Normalerweise vergehen zwischen dem ersten Eindringen in ein Netzwerk und der Entdeckung des „Angriffs" viele Monate. Das liegt in der Natur der Sache. Das Hacken eines Netzwerks läuft nicht ab, wie wir es in Hollywoodfilmen kennen: Knopfdruck, Code rast über einen Bildschirm, ein physischer Effekt wird erzielt. Häufig weiß der Angreifer nicht, ob er im gehackten Netzwerk überhaupt interessante Daten findet oder auch, was er sonst noch anrichten könnte. Kleinere Sabotageakte, für die z.B. „Stuxnet" berühmt ist (eine Malware, durch die Zentrifugen in einer iranischen Atomanlage verbogen wurden), sind möglich. Gleichzeitig eintausend wichtige Ziele lahmzulegen ist nicht möglich – bzw. wäre der Aufwand bei gleichzeitig großen Unsicherheiten viel zu hoch.

**Immer wieder hört man Nachrichten von Hacker-Attacken, die beispielsweise demokratische Verfahren wie Wahlen gefährden können. Was ist auf staatspolitischer Ebene schon getan worden, um das zu vermeiden? Was muss noch getan werden?**

Aus Sicht der Wissenschaft sind die Kausalitäten bei „Disinformationskampagnen" bisher nicht geklärt. Es scheint so, als ob sie die Meinungen von Menschen nicht zu ändern vermögen, sondern vielmehr „nur" bestätigen und ggf. verstärken. Wir sollten also eher nach Innen auf unsere eigene Gesellschaft und nicht nach außen, auf einen „Feind" schauen. Es zeichnet sich nämlich ab, dass die unliebsamen, destabilisierenden Effekte vor allem über den eigenen politischen Diskurs und die Medien generiert werden. Überreaktionen in der Politik sind deshalb absolut zu vermeiden! Sehr gefährlich ist z.B. die Idee, dass die Definition von Wahrheit in einer Demokratie staatlich gesteuert werden kann. Die Medien sollten generell versuchen, Hacker-Attacken nicht aufzubauschen und im richtigen Kontext darzustellen. Und ganz generell sollten wir uns als Gesellschaft überlegen, was wir digitalisieren wollen und was nicht. Die Digitalisierung bringt sehr viele Vorteile, aber auch Nachteile. In Zukunft müssen wir vermehr Risikoabschätzungen vornehmen.

**Durch die Virtualität eines Cyberwars ist seine Undurchschaubarkeit begründet. Ganz früher war es noch so, dass die Kriegserklärung den Beginn eines Krieges markiert hat. Wie ist das in Zeiten von Cyberwar-Bedrohungen? Wann beginnt eigentlich ein Cyberwar? Wann endet er?**

In Zeiten des „Un-Peace" im Cyberraum sind wir ständig im „Krieg" – oder eben nicht, wie ich finde. Es gibt keinen Anfang und kein Ende, Cyber-operationen oder Cyber-kampagnen sind ständige Begleiterscheinungen staatliches Mit- und Gegeneinander.

**Nach außen sieht es so aus, als seien Regierungen „gut gerüstet" gegen mögliche Gefahren aus dem Internet. Wie schätzen Sie aktuell beispielsweise die sicherheitspolitische Lage der deutschen Bundesregierung ein? Gibt es auch hier Vorreiternationen in der Welt?**

Die meisten Staaten sind nicht sonderlich gut gerüstet, aber das liegt in der Natur der Dinge: Es gilt, dass über 90% aller Netzwerke und kritische Infrastrukturen von privaten Firmen verwaltet werden. Der Staat hat die Aufgabe, seine eigenen Netzwerke zu schützen (was er nicht immer gut macht). Die Netzwerke Privater hingegen kann er nicht schützen: Weder gibt es dafür gesetzliche Grundlagen noch hat er die Leute dazu.
Wie viele andere Staaten widmet sich die deutsche Bundesregierung dem Aufbau von Kapazitäten und vor allem der

Konsolidierung von Rollen und Verantwortlichkeiten intern und mit Partnern in der Wirtschaft und der Gesellschaft. In einer Vorreiterrolle sieht man z.B. Estland und Israel, aber nicht aus den gleichen Gründen. In Estland ist es die sogenannte „Estonian Defence League“ oder „Kaitseliit“ im Cyberbereich, ein militärischer Freiwilligenverband, der schnell mobilisiert werden könnte. In Israel die „Start-Up“ Politik, bei der nachrichtendienstlich geschulten Bürgern die Etablierung einer Firma im Cybersicherheitsbereich vereinfacht wird.

**„Generell gilt: Kriminelle haben sich professionalisiert, und die Cyberkriminalität wird weiter zunehmen.“**

**Cyber-Security ist ein Thema, das nicht nur das Großunternehmen betreffen kann, sondern auch auf individueller Ebene großen Schaden anrichten kann. Man denke an das Risiko des gehackten Passworts für Online-Banking oder andere sensible Daten. Wie bewerten Sie die Auswirkungen eines Cyber-Wars? Wird er von Nationen geführt, von Unternehmen oder gar von Individuen?**

Hier sind wir nun im kriminellen Bereich angekommen! Kriminell motivierte Vorfälle haben nichts mit Krieg zu tun, sind aber sehr häufig und generieren hohe Kosten. Generell gilt: Kriminelle haben sich professionalisiert, und die Cyberkriminalität wird weiter zunehmen, denn die Risiken sind im Vergleich zu der herkömmlichen Kriminalität einiges kleiner, während der „Grundschutz“ bei viel zu vielen Firmen und Einzelpersonen sehr tief bleibt. Im kriminellen Bereich finden wir Einzeltäter, lose Gruppen und organisierte Kriminalität. Nordkorea sagt man als einzigem Staat nach, dass er cyberkriminelle Mittel nutzt, um zu Geld zu kommen.

**Was sind Ihre aktuellen Forschungsfragen? Hat die Corona-Pandemie und die damit im Zusammenhang stehende Verlagerung ins Digitale eine Zuspitzung der Thematik Cyberwar evoziert?**

Die Corona-Pandemie hat nichts verändert an der strategisch-politischen Wichtigkeit des Cyberraums, aber viele Beobachtungen bestätigt. Zum Beispiel ist noch klarer geworden, wie wichtig es ist, technische Aspekte von Cybersicherheit mit sozio-politischen zu verknüpfen. Denn nur so können wir erklären, warum die Nutzung von digitalen Technologien unterschiedliche politische Reaktionen auslöst. Was in unserer Forschung vermehrt ins Zentrum rückt, ist die Rolle von spezialisierten Cybersicherheitsfirmen im politischen Bereich.

**Was ist Ihre Vision eines absolut Internet-sicheren Lebens? Wie könnte das aussehen?**

Ich muss Sie leider enttäuschen, das wird es nie geben! Digitale Technologien werden nie sicher werden. Erwarten wir den nächsten Cybervorfall – wir können ihn nicht verhindern. Aber wir können uns darauf vorbereiten und uns fragen, wie wir ihn optimal bewältigen können.

Interview: Hannes Mittermaier

## Myriam Dunn Cavelty

Myriam Dunn Cavelty ist Dozentin für Security Studies und stellvertretende Leiterin des Center for Security Studies (CSS) der ETH Zürich. Sie studierte Internationale Beziehungen, Geschichte und Internationales Recht an der Universität Zürich. 2007 war sie Visiting Fellow am Watson Institute for International Studies (Brown University) und 2010–2011 Fellow der stiftung neue verantwortung in Berlin. Sie publiziert regelmäßig in internationalen Fachzeitschriften und ist Autorin und Herausgeberin mehrerer Bücher zu Themen rund um Sicherheit im Informationszeitalter. Neben ihrer Forschungs-, Lehr- und Publikationstätigkeit berät sie Regierungen, internationale Institutionen und Unternehmen in den Bereichen Cybersecurity, Cyberwar, Schutz kritischer Infrastrukturen, Risikoanalyse und strategische Früherkennung.

Foto: Privat

# Die Tücken der digitalen Kommunikation

## Ein Gespräch mit Yvonne Bernard

Cyber-Angriffe lauern meistens dort, wo man sich selbst am häufigsten aufhält, sprich, auf Seiten, Apps oder Programmen, die unseren digitalen Alltag mitbestimmen. Da sticht sofort unser E-Mail-Verkehr ins Auge: Das digitale Postfach ist unser alltäglicher Begleiter im Kommunizieren am Arbeitsplatz, aber auch im Privaten. Deshalb sind gerade E-Mail-Programme ein lukratives Mittel für Cyber-Attacken. Hornetsecurity hat sich hierauf spezialisiert und sorgt für eine möglichst sichere Nutzung. Welche Gefahren aber dennoch zu bedenken sind und wie man sich davor in Acht nimmt, verrät Dr. Yvonne Bernard, Chief Technical Officer bei Hornetsecurity.

**Können Sie kurz Ihre beruflichen Aktivitäten bei Hornetsecurity ausführen?**

Ich habe 2014 aus der Forschung zur Hornetsecurity Group gewechselt. Zunächst habe ich als Personal Assistant alle Abteilungen und Abläufe kennengelernt. Anschließend habe ich mehrere Jahre als Head of Product Management das Produktportfolio laufend erweitert, dabei u.a. Advanced Threat Protection und die Total Protection Suite Entwicklung betreut und die Produkte live gebracht. Seit bin ich als 2021 Chief Technical Officer bei Hornetsecurity verantwortlich für Produktmanagement, Product Development, Innovation and Research, Security Lab und unsere globale Cloud Infrastructure.

**Hornetsecurity ist Europas führender Cloud-Security-Provider für E-Mail. Wie gewährleisten Sie den Schutz Ihrer Kunden?**

Wir entwickeln unsere Security-Services laufend weiter, reagieren auf neue Trends und Angriffe mit leichtgewichtigen Releaseprozessen. Insbesondere unser eigenes Security-Lab-Team sorgt dafür, dass wir den Angreifern immer mindestens einen Schritt voraus sind. Hierbei wird der Verkehr 24/7 beobachtet und abgeleitet, welche Arten von Angriffen sich künftig entwickeln könnten, um proaktiv unsere Mechanismen bereits vor der ersten Schad-E-Mail zu härten.

**Was sind die größten Cyber-Gefahren für ein Unternehmen? Welche für ein Individuum?**

Für Unternehmen sind die größten Cyber-Gefahren:

- Datenverlust und -Diebstahl;
- Spionage;
- CEO-Fraud;
- Diebstahl von Zugangsdaten;
- Betriebs- und Produktionsstillstand aufgrund bspw. Stilllegung der IT-Infrastruktur durch zum Beispiel Ransomware.

**„Microsoft 365 hat sich gegenüber Konkurrenten, weil Google Gmail ganz klar im Business-Umfeld ist, durchgesetzt."**

Ransomware stellt eine der größten Bedrohungen für Unternehmen dar, besonders beobachten wir hier seit den letzten paar Jahren die Entwicklung zu sogenannter „Ranshameware", wie wir es intern bezeichnen: Hierbei kopieren Cyberkriminelle einige sensible interne Daten und Dateien eines Unternehmens, bevor sie diese verschlüsseln. Danach werden die Opfer damit erpresst, ein Lösegeld für die Entschlüsselung der Daten zu zahlen, da die zuvor gestohlenen Dateien und Informationen auf einer „Leak-Seite" veröffentlicht werden.

Für Individuen:

Auch hier ist die Nr. 1 Ransomware, doch ist das meist nicht

so „profitabel“ für Cyberkriminelle, da sie von Unternehmen deutlich höhere Summen erhalten könnten. In den meisten Fällen haben Hacker es hier auf Zugangsdaten abgesehen: Paypal, Amazon und Co. und vor allem Kreditkarten-Daten. Zuletzt beobachtete das Hornetsecurity Security Lab eine hohe Anzahl an „Impersonation Attacks“ der Sparkasse und Volksbanken Raiffeisenbanken. In diesen Schad-E-Mails werden die Empfänger dazu aufgefordert, einem Link zu folgen und dort die Zugangsdaten zu ihren privaten Konten einzugeben.

**„Ransomware stellt eine der größten Bedrohungen für Unternehmen dar, besonders beobachten wir hier seit den letzten paar Jahren die Entwicklung zu sogenannter ‚Ranshameware‘.“**

**Warum sind gerade E-Mails ein probates Mittel für Online-Kriminalität? Gibt es bestimmte Basisregeln, mit denen man grundsätzlich die Vertrauenswürdigkeit von E-Mails auf den ersten Blick einschätzen kann?**

Die E-Mail gilt auch in Zeiten von WhatsApp, Teams und Co. weiterhin als das seriöse, schnelle sowie meistgenutzte Kommunikationsmittel weltweit. Ein Großteil der Unternehmen weltweit stellt für seine Mitarbeiter zur internen als auch externen Kommunikation E-Mail-Adressen bereit, teilweise sind diese auch öffentlich einsehbar. Eine vermeintliche E-Mail vom Chef, der sich gerade im Urlaub befindet, mit der Bitte um eine schnelle Überweisung an ein bestimmtes Konto, um ein wichtiges Geschäft abzuschließen, oder eine E-Mail eines „Geschäftspartners“ mit einer angehängten PDF zur Freigabe, kann bei einem unwissenden Empfänger schnell dazu führen, dass sich Malware im internen IT-System verbreitet oder Transaktionen in Millionenhöhe unwissentlich auf das Konto von Hackern getätigt werden. Kurz gesagt: Bei ungenügendem Schutz sind Cyberkriminellen kaum Grenzen gesetzt, ins E-Mail-Postfach und damit ins System von Unternehmen zu gelangen.

Warum gerade E-Mail der Angriffsvektor Nr. 1 ist hat einige Gründe:

- E-Mail-Adressen sind einfach zu ermitteln;
- Es ist keine Authentifizierung durch den Angreifer notwendig;
- E-Mails sind keinen unternehmensspezifischen Zugangskontrollen ausgesetzt;
- E-Mails stellen die den meistgenutzten Service für die Geschäftskommunikation dar;
- Mitarbeiter sind via E-Mail direkt kontaktierbar;
- sensible Informationen werden oft per E-Mail ausgetauscht.

Jedoch gibt es tatsächlich einige Anhaltspunkte, an der man eine potenzielle Schad-E-Mail erkennen kann. Zuerst einmal gilt es, den Inhalt der E-Mail zu checken: Sind viele Rechtschreibfehler vorhanden? Ist die Ansprache persönlich an Sie gerichtet oder eher allgemein gehalten? Dann ist es noch wichtig, die Absender-Adresse zu kontrollieren: Kommt die E-Mail tatsächlich von John Smith, mit der Ihnen bekannten E-Mail Adresse john.smith@company.com oder einer völlig anderen? Sollten Sie sich weiterhin unsicher sein, kontaktieren Sie Ihren Kollegen oder Geschäftspartner einfach per Telefon und fragen nach, ob diese E-Mail auch tatsächlich von ihm stammt.

**Warum wird es trotzdem nie 100% Schutz im digitalen Äther geben?**

Solange es Angreifer gibt und die Angriffe sich für sie rentieren, wird es auch Angriffe geben. Das ist ein Katz- und Maus-Spiel.

**Umfragen zeigen, dass von fünf Unternehmen eines bereits Opfer eines Ransomware-Angriffs war. Ganz grob: Was verbirgt sich überhaupt hinter „Ransomware“ und was machen Sie, um solche Attacken in Zukunft zu minimieren?**

Ransomware ist ein Schadprogramm, welches gezielt Dateien auf einem befallenen Rechner verschlüsselt. Die Hacker hinter diesem Programm verlangen in der Regel ein Lösegeld von dem Opfer, um diese Dateien wieder zu entschlüsseln. Eine Entschlüsselung ist jedoch nicht immer garantiert.

Wir beobachten bei der Entwicklung unserer Services vor allem die aktuellen Trends der Vorgehensweisen der Cyberkriminellen und passen unsere Filter dahingehend an. Zum Beispiel beobachteten wir vor einigen Jahren Schad-E-Mails, in denen das infizierte, angehängte Dokument durch ein Passwort verschlüsselt wird, wodurch die Filtermechanismen von Antivirenprogrammen das dahinterliegende Schadprogramm nicht entdecken können. Wir entwickelten daraufhin das Feature „Malicious Document Decryption“, welches Teil unserer Advanced Threat Protection Services ist. Den Cyberkriminellen immer einen Schritt voraus sein, dass ist es, worauf es bei der Entwicklung von Security-Lösungen ankommt.

**Aktuell ist die Rede von „MalKamak“. Was ist das? Wie stufen Sie die potenzielle Gefahr, die von MalKamak ausgeht?**

Die angeblich vom Iran unterstützte Gruppe „MalKamak“ attackiert große Unternehmen aus den Branchen Luft- und Raumfahrt sowie Telekommunikation. Man vermutet, dass sie bereits seit 2019 unbemerkt aktiv war und in Verbindung mit anderen Hackergruppen wie APT (APT39) and Agrius APT steht.

Solche Cyberkriminellen Gruppen sind nie zu unterschätzen, vor allem wenn ihnen viele finanzielle und damit auch zahlreiche gute technische Mittel zur Verfügung stehen. Derzeit wurden insbesondere Luft- und Raumfahrt sowie Telekommunikationsunternehmen ins Visier genommen, ich gehe aber davon aus, dass es in weiteren Industriebereichen Opfer geben wird.

MalKamak ist aber nur eine Gruppe von vielen. Letztlich bestimmen die Medien, welche ins Scheinwerferlicht geraten und welche weiterhin still im Hintergrund agieren, die Berichterstattung muss letztlich selektiv erfolgen aufgrund der Vielzahl der Angreifer.

**Warum spezialisiert sich Hornetsecurity vor allem auf die Sicherheit von Microsoft? Leiden andere Betriebssysteme weniger unter Cyber-Attacken? Warum ist das so?**

Je verbreiteter ein Betriebssystem, desto lukrativer ist es, Angriffe darauf zu fahren und speziell dafür zu entwickeln. Ne-

ben dem Betriebssystem ist aber Microsoft 365 der spannende Aspekt, auf den ich eingehen möchte.

Microsoft 365 hat sich gegenüber Konkurrenten, weil Google Gmail ganz klar im Business-Umfeld ist, durchgesetzt. U.a. wird dies aufgrund der vielfach ohnehin genutzten Office-Lizenzen gewesen sein, aber insbesondere Teams, Sharepoint und weitere Add-On Services haben Microsoft zum künftigen Cloudanbieter auch für E-Mail gemacht. In den kommenden Jahren werden auch in Deutschland viele Kunden in die Microsoft Cloud migrieren, der Exchange im eigenen Rechenzentrum ist ein Auslaufmodell, das hat die Entwicklung in Ländern mit früherer Cloud Adoption gezeigt.

**„Jedoch gibt es tatsächlich einige Anhaltspunkte, an der man eine potenzielle Schad-E-Mail erkennen kann."**

Aber: Bei Microsoft 365 ist es einfach für Cyberkriminelle, die Sicherheitsmechanismen zu testen, einen Tenant kann man sich sogar kostenlos besorgen, und über die MX Records kann ich sogar sehen, ob ein Kunde bei Microsoft 365 ist. Die Build-in Security von Microsoft ist damit obsolet, damit testen Angreifer zuerst, wie sie sie umgehen. Außerdem gibt es keine Firewall, wer den Microsoft 365-Benutzer hackt, hat schließlich direkten Zugriff auf alle seine Daten.

Und da kommt Hornetsecurity ins Spiel: Unsere Produkte verbinden sich innerhalb von 30 Sekunden mit Microsoft und sichern den Angriffsvektor E-Mail umfassend ab.

**Wie bewerten Sie insgesamt die Situation unserer Cyber-Security in den letzten 24 Monaten? Sehen Sie eine Zunahme der Gefahren durch die zunehmende Digitalisierung unseres Alltags? Welche Rolle nimmt hier die Corona-Pandemie ein?**

Die Corona-Pandemie hat mit Sicherheit die Digitalisierung beschleunigt, was zunächst einmal ein durchaus positiver Effekt ist. Angst vor Digitalisierung ist ein schlechter Berater, Bewusstsein für IT-Sicherheit sollte jedoch unbedingt vorhanden sein.

Es wird vielfach behauptet, dass die Anzahl der Angriffe zugenommen habe, ich sehe aber vielmehr, dass die Qualität der Angriffe gestiegen ist. Viele können nicht mehr vom bloßen Auge erkannt werden und tauchen in dutzenden Varianten innerhalb eines Tages auf.

**Wurden Sie persönlich oder Ihr Unternehmen schon Opfer eines Cyber-Angriffs?**

Als Sicherheitsanbieter werden wir täglich (vermutlich sogar minütlich) angegriffen. Ich habe z.B. schon Spearphishing-Versuche unter Verwendung meiner Signatur gesehen. Allerdings hat glücklicherweise keine Attacke zum Erfolg geführt. Hier griffen unsere eigenen Engines, beispielsweise Targeted Fraud Forensics Filter, absolut zuverlässig. Ich bin absoluter Verfechter davon, seine eigenen Produkte auch selbst zu verwenden, somit bekommt man auch die Administrator- und Endbenutzer-Perspektive direkt mit.

Interview: Hannes Mittermaier

### Dr.-Ing. Yvonne Bernard

Dr.-Ing. Yvonne Bernard studierte an der Leibniz Universität Informatik (B.Sc., M.Sc.) und promovierte anschließend dort im Bereich Sicherheit in offenen verteilten Systemen in der DFG-Forschergruppe OC-Trust. Sie arbeitete parallel über 5 Jahre an der Leibniz Universität Hannover als wissenschaftliche Mitarbeiterin im Gebiet System- und Rechnerarchitektur. Während dieser Zeit veröffentlichte sie über 20 wissenschaftliche Publikationen in den Bereichen Vertrauen, Sicherheit, offene Systeme, Verteilte Systeme, Multiagentensysteme sowie Machine Learning.

Sie war zwei Jahre bei Hornetsecurity als Personal Assistant tätig, anschließend 5 Jahre lang Head of Product Management. Seit 2021 treibt sie als Chief Technical Officer in den Bereichen Produktmanagement, Softwareentwicklung, Innovation and Research, Security Lab und Cloud Infrastruktur die strategische und technische Weiterentwicklung des Cloud Security Pioniers voran.

Foto: Privat

# 1. CYBER SECURITY

Cyber Security ist eines der meist behandelten Themen im Geschäftsumfeld; und das seit Jahren. Diese Attraktion ist leicht zu begründen, schließlich geht es bei dem Thema Sicherheit um nicht weniger als Angst, Vertrauen und eben auch um Geld. Bei einem solchen Thema wird der Mensch schnell aufmerksam. Auch wenn viel von Cyber Security geredet wird, so ist es schwierig, dieses Thema scharf abzugrenzen. Wie ist Cyber Security definiert, wie Internetsicherheit, Informationssicherheit oder Datenschutz?

Cyber Security ist ein so kompliziertes und eben auch interessantes Thema, weil es auf so vielen unterschiedlichen Ebenen behandelt werden kann. So ist Cyber Security selbstverständlich technischer Natur, aber ebenso hat es eine organisatorische Dimension: Nur wenn eine Maßnahme auch wirklich in einen Prozess integriert werden kann, wird diese verwendet. Darüber hinaus gibt es eine politische Ebene („wessen" Datenschutzgesetze werden beispielsweise beim Surfen im Internet angewendet) und eben auch eine menschlich-soziale: Der Anwender muss die Maßnahmen wollen, keine Berührungsängste haben und sie insbesondere auch verstehen.

Selbst innerhalb der beispielhaft vorgestellten Ebenen gibt es stets einen schwierigen Kompromiss zu lösen, der mit „Wähle zwei: Sicherheit, Nutzbarkeit, Kosten" umschrieben werden kann. Eine sichere und einfach zu bedienende Lösung ist oft teuer, eine einfach zu bedienende und günstige Lösung oft nicht sicher und schließlich eine günstige und sichere Lösung oft nur schwer zu verwenden. Sowohl für Unternehmen als auch für Privatanwender gilt es nun, einen möglichst passenden Weg zu beschreiten.

Ebenso facettenreich wie das Thema Cyber Sicherheit sind die einzelnen Beiträge dieser Ausgabe selbst. Sie enthalten unter anderem allgemein aufzufassende Themen wie die Sensibilisierung der Gesellschaft, technische Themen wie zukünftige digitale Identitäten, aber auch die Behandlung konkreter Anwendungsfälle wie den mobilen Zugriff auf Unternehmensdaten.

## MEIST GEKLICKT – Unsere erfolgreichsten Blog-Beiträge

Unsere Beiträge wurden insgesamt über **2.810.000 Mal** geklickt*

Beiträge zum Thema **CYBER SECURITY** erhielten **560.000** Klicks.

| | Autor I Thema |
|---|---|
| #1 | **Timmi Hopf I** Warum ein ganzheitlicher IT-/OT-Security-Ansatz wichtig ist **Seite 68** |
| #2 | **Ben Kröger I** Weckruf Cybersicherheit: Wie viele Vorfälle braucht es noch? **Seite 65** |
| #3 | **Tim Bloomer I** Ransomware automatisch abwehren **Seite 47** |
| #4 | **Dr. Torben Guelstorff I** Status quo bei verhaltensbiometrischen Authentifizierungsverfahren **Seite 83** |
| #5 | **Tanja Hofmann I** Viel zu komplex? Wie Unternehmen Multi-Cloud-Umgebungen effektiv absichern können **Seite 61** |

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 15. November 2021.**

# INHALT

## FACHBEITRÄGE



## BLOGBEITRÄGE

### 1.1 RANSOMWARE



### 1.2 SOCIAL ENGENEERING



### 1.3 CLOUD



### 1.4 ARBEITSWELT



### 1.5 REAKTIONEN



### 1.6 AUTH



### 1.7 USE CASES

# Eine starke Unternehmenskultur minimiert Cyberrisiken

**Ulrich Pfeiffer**
ADVIA GmbH

Die Zahl der Cyberangriffe wächst seit Jahren kontinuierlich. Besonders dramatisch ist seit Ausbruch der Corona-Pandemie der weltweite Anstieg der Social-Engineering-Attacken, bei denen Cyberkriminelle Mitarbeitende manipulieren, um Zugang zu IT-Systemen und Daten von Unternehmen zu erhalten. Es ist davon auszugehen, dass dieser Trend sich noch verstärken wird. Informationssicherheits-Strategien von Unternehmen berücksichtigen den Hauptrisikofaktor Mensch jedoch nur ungenügend. Insbesondere ist vielen Unternehmen nicht klar, dass ein erfolgreiches Sicherheitskonzept auch die Etablierung einer Informationssicherheits-Kultur beinhalten muss. Angesichts des technischen Fokus eines Großteils der Informationen zu Cybersecurity und Informationssicherheit in Fachmedien und im Internet wollen wir hier einen Ausblick darauf geben, wie die Organisationsentwicklung in die Informationssicherheits-Strategie einfließen kann und wie eine Informationssicherheits-Kultur mit Hilfe agiler Vorgehensweisen im Unternehmen entwickelt werden kann.

## 1) Die Bedrohung durch Cyberkriminalität wächst rasant

Im Juli 2021 hat die Bitkom eine alarmierende Studie zum Thema Vertrauen und IT-Sicherheit veröffentlicht.[1] Den Ergebnissen zufolge hat sich der Schaden durch Cyberangriffe binnen eines Jahres auf 223 Milliarden Euro verdoppelt. Waren früher vor allem Großkonzerne und staatliche Institutionen betroffen, ziehen sich Cyberangriffe heute durch die gesamte deutsche Industrie: Insgesamt gaben 9 von 10 Firmen an, im vergangenen Jahr Opfer von Cyberangriffen geworden zu sein. 10 % der Unternehmen waren durch Cyberangriffe sogar in ihrer geschäftlichen Existenz bedroht. Den größten Beitrag zu dieser besorgniserregenden Entwicklung leisten Ransomware-Attacken, bei denen der Zugang der Nutzer*innen zu den infizierten Systemen durch Verschlüsselung blockiert und nur gegen Zahlung von Lösegeldern in teilweise erheblicher Höhe wieder entsperrt wird (Abbildung 1). Der Anstieg dieser Art von Attacken stieg binnen eines Jahres um gigantische 350%. Neben finanziellen Schäden kann es bei Attacken auf kritische Infrastrukturen sogar um Leben und Tod gehen: Im Herbst 2020 ging durch die Medien, dass eine Frau im Krankenwagen gestorben ist, weil die Notaufnahme der Uniklinik Düsseldorf durch Ransomware lahmgelegt war und die Patientin nicht aufnehmen konnte. Auch wenn sich dieser Begründung für den Tod der Frau im Nachhinein als unwahrscheinlich herausgestellt hat[2], gehen Experten davon aus, dass es nur eine Frage der Zeit ist, bis es die ersten Toten durch Cyberangriffe gibt.[3]

Die Ausweitung der Tätigkeit im Homeoffice im Rahmen der Corona-Pandemie leistet einen substanziellen Beitrag zum Anstieg der Cyberkriminalität. Bedenklich ist dabei vor allem, dass die Erfolgsquote der Attacken, die mit dem Homeoffice in Verbindung stehen bei über 50 % liegt. Einen Hauptgrund dafür sieht die Bitkom in der gemischten Nutzung von Privat- und Firmengeräten. Auch die unbefugte Nutzung von Firmengeräten – z.B. durch Familienmitglieder – und sonstige Verletzungen von Compliance-Regeln begünstigen Attacken. Auch der ungenügende Schutz der Kommunikationskanälen, die für die virtuelle Zusammenarbeit genutzt werden, stellt ein erhebliches Risiko dar. Manchmal ist es jedoch auch schlicht der mangelnde Digitalisierungsgrad von Arbeitsabläufen und Prozessen, der die Mitarbeitenden zu unsicheren Workarounds zwingt. Angesichts der hybriden Zukunft der Arbeitswelt ist davon auszugehen, dass die Anzahl der Cyberangriffe weiterhin rasant steigen wird. Oft wird in diesem Zusammenhang verkürzt von Cybersecurity gesprochen, die jedoch nur ein Teilgebiet der Informationssicherheit ist. Während sich Cybersecurity auf die Absicherung des Cyberraums beschränkt, umfasst die Informationssicherheit den Schutz von Informationen und Informationssystemen zur Sicherstellung von deren Integrität, Vertraulichkeit und Verfügbarkeit. Im Folgenden zeigen wir auf, welche Rolle der Faktor Mensch dabei spielt.

## 2) Social Engineering: Attacken zielen auf den Menschen als schwächstes Glied der Kette

Die Zunahme der Cyberkriminalität im Homeoffice verdeutlicht, was bereits vor der Pandemie zu erahnen war: Der Mensch ist das größte Sicherheitsrisiko und damit das schwächste Glied der Informationssicherheitskette (Abbildung 2)! Dies haben auch Cyberkriminelle erkannt und zielen bei ihren Attacken vermehrt auf Menschen, ein Vorgehen, das auch als Social Engineering bezeichnet wird. Im Kern geht es dabei laut BSI um die geschickte Täuschung über die Identität und die Absicht des Täters. Es wäre zu leicht, dabei einfach nur auf Gutgläubigkeit als Grund für erfolgreiche Angriffe zu verweisen. Laut der Agentur der EU für Cybersicherheit ENISA ist alleine die Anzahl der Phishing-Mails im letzten Jahr um 600% gestiegen![4] Verizon hebt Phishing auf den ersten Platz unter allen Aktionen, die in 2020 zu einer Datenpanne in Unternehmen geführt haben.[5] Konnte man sich früher halbwegs in Sicherheit wiegen, wenn man unbekannte *.exe-Dateien in E-Mails nicht geöffnet hat, ist das Vorgehen der Cyberkriminellen heute deutlich perfider und lässt selbst Menschen mit hoher digitaler Affinität in die Falle tappen: Die Attacken werden durch das Sammeln von Informationen und Ausspionieren von Mitarbeitenden minutiös vorbereitet. Websites

**Abbildung 1. Ransomware-Attacken sind in den vergangenen Jahren zur größten Bedrohung geworden.**

**Abbildung 2. Social-Engineering-Attacken zielen auf den Menschen als schwächstes Glied der Sicherheitskette.**

und Mail-Designs werden perfekt nachgebaut. Die Angreifer können sich so glaubhaft als Mitarbeiter des IT-Service einer Firma ausgeben, da sie Interna kennen und Informationen über ihre Opfer und deren berufliches Umfeld haben. Das betrifft auch Führungskräfte: Ein McAfee-Report aus dem Jahr 2020 verweist explizit auf eine gestiegene Anzahl an sogenannten CEO Frauds, deren Kosten schnell im Millionen-Bereich liegen, da es neben Datenverlusten und Ausfallzeiten auch zu Marken- und Reputationsschäden kommt. [6] Doch was können Unternehmen tun?

## 3) Der Faktor Mensch als Kern der Informationssicherheits-Strategie

Angesichts der wachsenden Bedrohungen investieren immer mehr Unternehmen in eine Informationssicherheits-Strategie. Laut dem Digital Trust Report 2021 von PwC ist die Corona-Pandemie für 98% der Unternehmen ein Auslöser gewesen, ihre Sicherheitsmaßnahmen zu überdenken und neu auszurichten.[7] Mehr als die Hälfte davon hat ihr Budget für 2021 erhöht. Allerdings beobachten wir im Kontext dieser Entwicklung, dass die meisten Informationssicherheits-Strategien auf technologische Vorkehrungen fokussieren und den Faktor Mensch außer Acht lassen. Natürlich sind technologische Abwehrmaßnahmen das Fundament jeder Strategie. Fatalerweise kann jedoch bereits ein einziger Fehler einer einzelnen Person die technologischen Sicherheitsvorkehrungen eines Unternehmens aushebeln: Wird ein unsicheres Passwort gewählt, ein Passwort verraten, eine Datei angeklickt oder ein Remote-Zugriff gewährt, ist es zu spät. Der Mensch muss also auch in einer Informationssicherheits-Strategie im Mittelpunkt stehen. Ein Mindeststandard jeder Strategie sollte sein, dass die Informationssicherheits-Awareness durch individuelle Trainings- und Weiterbildungsmaßnahmen etabliert und kontinuierlich ausgebaut und an neue Bedrohungen angepasst wird. Die trockenen Datenschutz-Schulungen im Frontalunterricht, die in vielen Unternehmen noch zum Standard gehören, reichen dazu aber nicht mehr aus. Stattdessen muss der Faktor Mensch nicht nur sicherheitstechnisch, sondern auch lernpsychologisch berücksichtigt werden: z.B. durch interaktive E-Learning-Elemente, Malware- und Phishing-Simulationen und Angebote für Peer-to-Peer-Lernformate. Gerade der soziale Austausch scheint von großer Bedeutung zu sein: In dezentralen Unternehmen und Unternehmen mit hoher Homeoffice-Quote ist die Erfolgsrate von Social-Engineering-Attacken deutlich höher als in zentralisiert organisierten Unternehmen: Der Flurfunk spielt demnach eine Rolle für die gemeinsame Sensibilisierung für das Thema. Welche Rolle spielt also die Organisation?

## 4) Die Organisation in der Strategie mitdenken!

Nicht das Individuum, sondern der Mensch als Teil der Organisation mit ihrer gelebten Kultur, spielt die eigentliche Hauptrolle in der Informationssicherheit. Während sich in anderen Bereich der IT die Erkenntnis durchgesetzt hat, dass Digitalisierung ebenso sehr ein Organisations- wie ein Technologiethema ist, wird die Organisation in der Informationssicherheit noch sträflich vernachlässigt. Dies ist insofern überraschend, da der Erfolg einer Informationssicherheits-Strategie davon abhängt, dass Menschen sich korrekt verhalten. Bis zu einem gewissen Grad kann dies durch individuelle Trainings beeinflusst werden. Das Verhalten von Menschen im Job wird jedoch maßgeblich von der vorherrschenden Organisationskultur beeinflusst. Die Kultur führt dazu, dass bestimmte Dinge auf eine bestimmte Art und Weise getan werden, ohne dass dies irgendwo geschrieben steht: Teams kommunizieren zu sensiblen Themen über WhatsApp, große Dateien werden auf Grund limitierter E-Mail-Quotas über unautorisierte Filetransfer-Dienste versendet, in der Schublade der Sekretärin liegt eine Passwortliste, falls der Chef mal dringend an einen Rechner muss… Der Einfluss der Organisationskultur kann sich auf vielen Ebenen zeigen und zu Sicherheitsrisiken führen, in manchen Fällen entwickelt sich über Jahre hinweg eine Schatten-IT, die komplett unter dem Radar der Sicherheitsbeauftragten genutzt wird. Weder Technologien noch individuelle Vorkehrungen können dies letztlich zu 100% verhindern. Unternehmen wird dies zunehmend bewusst. Nur 5% bewerten ihre Informationssicherheits-Kultur laut einer Studie der Information System Audit and Control Association ISACA als zufriedenstellend.[8] Gleichzeitig zeigt die Studie, dass die wenigsten Unternehmen wissen, wie sie vorgehen sollen, um die Kultur zu entwickeln. Als wesentliche Ursachen werden in erster Linie kulturell-organisationale Gründe genannt, u.a. die fehlende Akzeptanz der Mitarbeitenden (41%), mangelhaftes Alignement der Geschäftsbereiche (39%) und fehlendes Engagement des Top-Managements (27%) genannt. Was also tun?

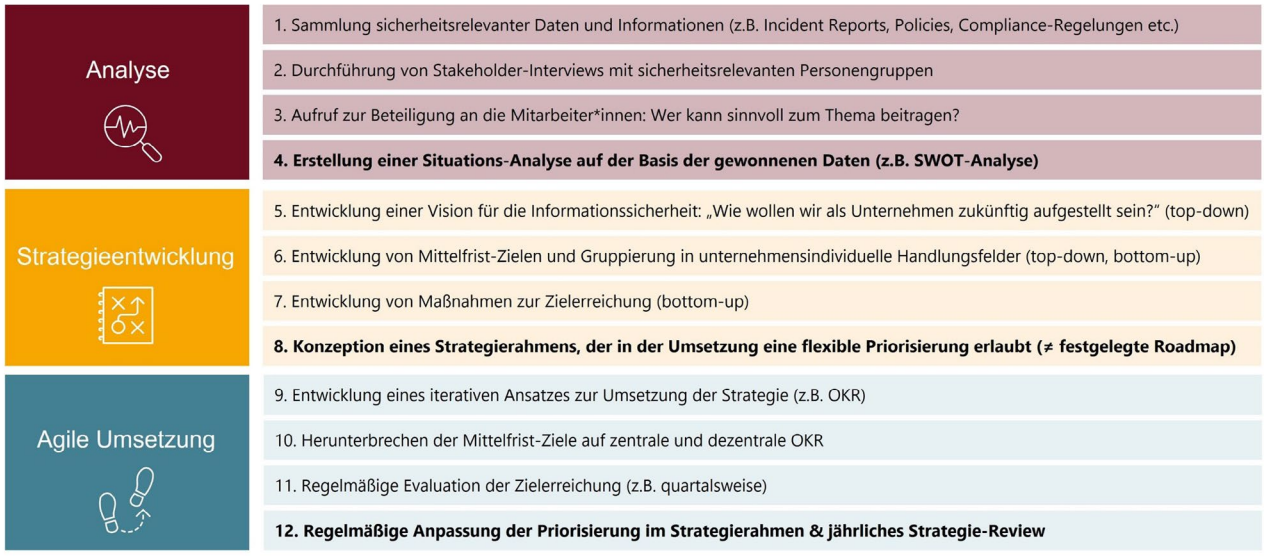



**Abbildung 3. Phasen und Schritte zur Entwicklung einer Informationssicherheits-Strategie, die auch die Organisation mitdenkt.**

## 5) Merkmale einer Informations-sicherheits-Kultur

Die Informationssicherheits-Kultur wurde schon vor 15 Jahren wissenschaftlich aufgegriffen[9] – Praktikern war ihre Bedeutung wohl schon deutlich länger bewusst. Da akademische Perspektiven auf das Thema leicht als wirklichkeitsfern wahrgenommen werden, ist seitdem jedoch wenig passiert. In einem spannenden Artikel haben die beiden MIT-Forscher*innen Keman Huang und Keri Pearlson 2019 ein Modell zur Entwicklung einer Cybersecurity-Kultur in Unternehmen vorgestellt.[10] Das Modell basiert auf dem Kulturebenen-Modell von Ed Schein[11], das drei Ebenen von Kulturphänomenen beschreibt und ist allgemein für Informationssicherheits-Kulturen anwendbar: 1) Artefakte: Auf der obersten Ebene sind die sichtbaren Auswüchse einer Kultur, wie beispielsweise das gelebte Verhalten, der Umgang miteinander, die Kleiderordnung etc., 2) Werte und Normen: Die zweite Ebene bilden Leitbilder, Führungsprinzipien und Strategien, in denen bekundet wird, wie die Organisation sein soll, 3) Grundannahmen: Die dritte Ebene befindet sich unter der sichtbaren Oberfläche. Hier befinden sich für selbstverständlich gehaltene Bewertungen, Lösungen und Grundgedanken, die die Organisation prägen. Eine Informationssicherheits-Kultur entsteht, wenn auf allen drei Ebenen sicherheitsrelevantes Verhalten gefördert wird. Dazu ist es laut Huang und Pearlson notwendig, dass unterschiedliche Gruppen im Unternehmen unterschiedliche Verhaltensweisen entwickeln:

1) Management: Führungskräfte spielen eine Schlüsselrolle in der Informationssicherheit. Einerseits können sie durch die richtigen Entscheidungen externe Bedrohungen reduzieren, andererseits propagieren sie durch konsequentes Vorleben die Kultur. Damit dies gelingt, müssen Führungskräfte zunächst das notwendige Wissen und Skill-Set erwerben, um Informationssicherheit zu verstehen und Risiken im eigenen Unternehmen zu erkennen. Auf der Basis dieses Wissens müssen Führungskräfte Informationssicherheit als strategisches Thema priorisieren. Schließlich müssen sie sichtbar an sicherheitsrelevanten Aktivitäten teilnehmen.
2) Teams: Gemeinsame Überzeugungen und die damit einhergehenden Verhaltensweise entstehen in erster Linie durch die Zusammenarbeit im Unternehmen. In der Zusammenarbeit im Team muss daher offen über Informationssicherheit gesprochen und diese priorisiert werden. Zudem muss sie in die tägliche Kollaboration integriert werden. Dabei helfen Checklisten und die konsequente Einbindung des Themas in Prozesse und Regeltermine. Darüber hinaus muss die bereichsübergreifende Zusammenarbeit zwischen IT/Informationssicherheit und Business intensiviert werden. Sitzt die IT oder gar ein Informationssicherheitsbeauftragter (ISB/CISO) immer mit am Tisch, um für sicherheitsrelevante Themen zu sensibilisieren, erleben auch neue Teammitgliedern den Stellenwert der Informationssicherheit ganz direkt.
3) Individuen: Jede*r Einzelne kann zur Informationssicherheits-Kultur beitragen, wenn bestimmte Bedingungen erfüllt sind. Vor allem müssen die Mitarbeitenden Selbstwirksamkeit wahrnehmen, d.h. wissen und erleben, dass ihre individuellen Handlungen einen Impact auf die Sicherheit haben. Dazu ist es notwendig, dass sie die -Vorgaben und Prozesse zur Informationssicherheit des Unternehmens kennen (Was ist zu tun? Was ist falsch/richtig? Wie ist es zu tun?) und verstehen (Warum ist das wichtig?). Dazu müssen Mitarbeitende eine generelle Awareness für Informationssicherheit entwickeln, um Bedrohungen zu erkennen. Die individuellen Komponenten einer Informationssicherheits-Kultur lassen sich z.B. durch Simulationen und interaktive Übungen schulen.

Spricht man über Unternehmenskultur im Zusammenhang mit Informationssicherheit, kommt schnell ein Eindruck von ausschließlichem „müssen" und „sollen" auf. Auch wenn regelhaftes Verhalten ein wichtiges Element einer Informationssicherheits-Kultur ist, lässt sich mit erhobenem Zeigefinger nur selten etwas erreichen. Im Strategieprozess sollte man stattdessen betonen, wie eine solche Kultur Mitarbeitende, Teams und Führungskräfte ermutigt, die richtigen Entscheidungen zu treffen und ihren Arbeitsalltag im Einklang mit den Sicherheitsrichtlinien zu gestalten.[12] Ähnlich verhält es sich mit wissenschaftlichen Empfehlungen. Huang und Pearlman empfehlen verschiedene Maßnahmen zur Kulturentwicklung. Während einige davon generisch und damit in allen Unternehmen sinnvoll sind (z.B. dezidierte Informationskanäle, Cybersecurity-Trainings

etc.), kann nicht jede Maßnahme in jeder Unternehmenskultur umgesetzt werden – die Informationssicherheits-Kultur ist letztlich eine Untermenge der allgemeinen Unternehmenskultur. Wir plädieren deshalb dafür, dass Unternehmen ihre individuelle Strategie unter breiter Partizipation aller Ebenen entwickeln.

## 6) Die Strategie partizipativ entwickeln und iterativ umsetzen

Die Organisation in der Strategie mitdenken – hinter dieser Aufforderung verbergen sich gleich zwei Aussagen: Zum einen muss die Strategie die Organisationsentwicklung hin zu einer Informationssicherheits-Kultur beinhalten, wie beschrieben. Zum anderen muss die Organisation bei der Entwicklung und Umsetzung eingebunden werden. Geschieht dies nicht, so scheitern laut Studien von McKinsey ca. 70% aller Strategieprojekte. Das liegt selten am Konzept oder an Technologien, sondern an ungünstigen kulturellen und organisatorischen Rahmenbedingungen.[13] Es ist daher wichtig, die Mitarbeitenden schon früh in den Prozess einzubinden. Wir meinen hier nicht das klassische Change-Management, wo Veränderungsprozesse von oben angeordnet und dann mit Hochglanz-Newslettern begleitet werden, sondern echte Partizipation: Wenn der Mensch in der Organisation der kritische Faktor ist, dann ist er zugleich auch eine wesentliche Informationsquelle für Sicherheitsrisiken und potenzieller Ideengeber für Lösungen. Strategische Leitlinien können dabei selbstverständlich vom CIO oder ISB/CISO kommen – bewährt hat sich in Strategieprozessen jedoch die Entwicklung von Zielen und Maßnahmen im Zusammenspiel von strategischen Erwägungen des Managements (top-down) und konkreten Prozesskenntnissen sowie Ideen aus dem gesamten Unternehmen (bottom-up). Eine Strategie, die auf diese Weise entwickelt wurde, wird automatisch von einer breiten Mehrheit im Unternehmen getragen.

Um nachhaltigen Erfolg zu erreichen, sollte die Informationssicherheits-Strategie schrittweise und flexibel umgesetzt werden. Dazu eignen sich Vorgehensmodelle aus der agilen Welt. Diese finden im Bereich der Informationssicherheit, wo entsprechende Managementsysteme (ISMS) im top-down Verfahren eingeführt werden, häufig keine umfassende Anwendung – wohl weil Agilität (fälschlicherweise!) mit vollkommener Autonomie assoziiert wird. Dabei haben agile Methoden einen entscheidenden Vorteil: Sie bieten einen geregelten Rahmen für die iterative und kontrollierte Umsetzung von Vorhaben und erlauben die kontinuierliche Anpassung an neue Entwicklungen. Für die nachhaltige Umsetzung einer Informationssicherheits-Strategie empfehlen sich insbesondere Objectives and Key Results (OKR) – ein agiles Strategie-Framework das v.a. durch seine Anwendung bei Google berühmt wurde.[14] Dabei werden die mittelfristigen Ziele einer Strategie in einem vierteljährlichen Review auf qualitative Objectives heruntergebrochen („Unsere Mitarbeitenden werden besser im Erkennen von Gefahren“), die durch quantitative Key Results („Der Anteil der erfolgreichen Phishing-Attacken ist um 10% gesunken“) messbar gemacht werden. Die OKR können dann auf Business Units oder Teams heruntergebrochen werden, wo dann zentrale Maßnahmen zum Erreichen der Ziele (z.B. Schulungen) um dezentrale Maßnahmen (z.B. Einführung von Informationssicherheits-Weeklys) ergänzt werden können. Im Review wird das Erreichte evaluiert und die Priorisierung angepasst, z.B. wenn neue Bedrohungen auftauchen, die in der Strategie nicht berücksichtigt wurden. Ganz nebenbei unterstützen OKR so übrigens auch die Kulturentwicklung: Das Thema ist ständig präsent, wird offen diskutiert wird und alle sind ihren Aufgaben und Rollen entsprechend involviert. Abbildung 3 skizziert die wesentlichen Schritte der Strategieentwicklung von der Analyse, über die Strategieentwicklung hin zur agilen Umsetzung der Strategie.

OKR sind nur eine von mehreren möglichen Methoden, um eine Informationssicherheits-Strategie im Unternehmen auszurollen und alle transparent an der Umsetzung zu beteiligen. Auch mit Elementen aus der agilen Projektmanagement-Methodik SCRUM oder mittels Portfolio-Kanban lässt sich erreichen, dass die Organisation Informationssicherheit wirklich lebt. Die konkrete Methode ist aber eigentlich zweitrangig. Es geht angesichts der wachsenden Bedrohungen und der Komplexität des Themas Informationssicherheit in erster Linie darum, dass die gesamte Organisation neue, sicherheitsrelevante Verhaltensweisen verinnerlicht. Agile Methoden dienen hier als Unterstützung auf dem Weg zum Ziel, da ihr Regelwerk erfordert, dass sich Menschen auf eine bestimmte Art und Weise verhalten, etwa indem sie die transparente Zielerreichung in kleinen Schritten, den regelmäßigen Austausch, und den offenen Umgang mit Fehlern fördern. Diese Art von Kulturentwicklung ist notwendig, um auf die Bedrohungen der Zukunft schnell reagieren zu können.

## Fazit

Menschen sind der Hauptangriffspunkt von Cyberkriminellen. Die zunehmende Tätigkeit im Homeoffice und die damit verbundene Dezentralisierung werden diesen Trend weiter unterstützen. Um dieser Entwicklung strategisch zu begegnen reichen technologische Schutzmechanismen und individuelle Schulungen nicht aus, da das Verhalten von Menschen im Job maßgeblich durch die Kultur beeinflusst wird. Die Entwicklung einer Informationssicherheits-Kultur ist ein langfristiges Unterfangen. Das Investment lohnt sich jedoch, da nachhaltige Cyberresilienz nur erreicht werden kann, wenn die notwendigen technologischen Vorkehrungen auf eine Organisation treffen, die sicherheitsrelevantes Verhalten auf allen Ebenen verinnerlicht hat. Denn eines sollten Unternehmen im Kopf behalten: Eine Informationssicherheits-Strategie ist nie „fertig“, der Job ist nicht erledigt, sobald sie umgesetzt ist. Wer gewappnet sein will, investiert in eine agile Sicherheitskultur, in der das Thema kontinuierlich präsent ist.

Referenzen: **[1]** Vertrauen & IT-Sicherheit 2021 | Bitkom Research (bitkom-research.de) **[2]** https://www.heise.de/hintergrund/Staatsanwalt-macht-Rueckzieher-Krankenhaus-Hacker-nicht-fuer-Tote-verantwortlich-4961183.html **[3]** Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Suc-cessfully Harm or Kill Humans **[4]** Phishing most common Cyber Incident faced by SMEs — ENISA (europa.eu) **[5]** Verizon 2020 Data Breach Report **[6]** New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion | McAfee, Inc. **[7]** Digital Trust Insights 2021 – PwC **[8]** https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html **[9]** Organisational security culture: Extending the end-user perspective - ScienceDirect **[10]** http://web.mit.edu/smadnick/www/wp/2019-02.pdf **[11]** Organizational Culture and Leadership (vnbrims.org) **[12]** Tipps für eine echte Cyber-Security-Kultur im Unternehmen (computerweekly.com) **[13]** How to beat the transformation odds | McKinsey **[14]** re:Work - Guide: Set goals with OKRs (rework.withgoogle.com)

**Ulrich Pfeiffer**

Ulrich Pfeiffer verantwortet bei der ADVIA den Themenbereich Agile Transformation & New Work und berät Unternehmen zur Organisationsentwicklung im digitalen Kontext. Zuvor war der promovierte Psychologe in diversen Führungspositionen für Strategisches Management und Digitalisierung zuständig.

Foto: Privat

# Verhaltensbasierte Container-Sicherheit: Reduktion auf das Wesentliche

**Bernd Mährlein**
Lacework

Im Vergleich zu monolithischen Anwendungen beschleunigen containerisierte Applikationen die Entwicklung, bieten mehr Flexibilität bei der Bereitstellung und reduzieren die Ressourcenbelastung. Container-Technologien sind daher auf dem Vormarsch: Forrester[1] prognostiziert, dass 60 Prozent der globalen Unternehmen bis Ende dieses Jahres Container einsetzen werden. Laut einer IDC Studie[2] plant mehr als die Hälfte der deutschen Unternehmen, bis 2022 die überwiegende Zahl ihrer Workloads mittels Container und nicht mehr über herkömmliche Umgebungen bereitzustellen.

Neben unbestreitbaren Vorteilen bringt der Einsatz von Containern aber insbesondere für die IT-Sicherheit auch eine Reihe von spezifischen Herausforderungen mit sich. Container bedeuten einen weiteren Komplexitätssprung und durch agile Entwicklungsmethoden wie DevOps vervielfacht sich die Zahl der Code-Iterationen, für deren Sicherheitsbewertung immer weniger Zeit zur Verfügung steht. Die IT-Sicherheit wird so zum Bremsklotz, den frustrierte Entwickler mit Workarounds zu umgehen versuchen. Eine unkontrollierte Schatten-IT mit ganz eigenen Problemen entsteht.

## Vorhandene Werkzeuge meist nicht Cloud-nativ

Als weitere Herausforderung kommt hinzu, dass traditionelle Sicherheitskontrollpunkte wie Betriebssysteme oder virtuelle Maschinen bei Containern und Serverless-Funktionen verschwinden. Vorhandene Sicherheitswerkzeuge und -ansätze sind zudem meist nicht Cloud-nativ. Die Konzepte lassen sich nicht unbegrenzt auf hochkomplexe Cloud- und Container-Umgebungen ausdehnen. Ein zu enger Aufgabenfokus führt zu Informationssilos und einer Alarmschwemme. Cloud- und Container-Umgebungen benötigen eine übergreifende Perspektive und Kontextsensitivität, ansonsten ist die Komplexität nicht mehr zu bewältigen.

Darüber hinaus erschwert die Dynamik von Container-Umgebungen die Definition von Sicherheitsregeln für Firewall / Networking. Container werden beispielsweise oft mit Regeln gebaut, die nur bestimmten Anwendertypen den Zugriff erlauben. Über die Zeit werden sich aber wahrscheinlich die Anwenderdefinitionen und Gruppenzugehörigkeiten ändern, was zu unerwünscht weitreichenden Berechtigungen führen kann. Es liegt nicht in der Verantwortung von DevOps-Teams, dies zu berücksichtigen, sodass Risiken entstehen.

Weitere Investitionen in zusätzliche Punktlösungen und mehr Fachpersonal (das kaum verfügbar ist) können diese Situation nicht dauerhaft entschärfen. Es ist absehbar, dass sich die Komplexitätsspirale weiterdreht und Container aufgrund ihrer Popularität noch stärker ins Fadenkreuz von Angreifern rücken. Vor diesem Hintergrund wächst das Interesse an KI-gestützten Ansätzen, die Sicherheit im Takt der Cloud bei reduziertem Aufwand versprechen.

## Sicherheit erlernt Normalzustand

Verhaltensbasierte Cloud- und Container-Sicherheit nutzt Machine Learning, um den Normalzustand (die Baseline) der Aktivitäten in der Umgebung zu erlernen und vor diesem Hintergrund dann Anomalien zu identifizieren. Voraussetzung dafür ist, dass tatsächlich alle Aktivitäten von Containern, Applikationen, Anwendern und anderen Cloud-Entitäten lückenlos aufgezeichnet und analysiert werden können. Um das zu erreichen, werden die Prozesse in der Infrastruktur beobachtet. Aus folgenden Gründen eignen sich Prozesse als Analyseeinheit:

- Prozesse sind verantwortlich für die gesamte Kommunikation untereinander und mit externen Hosts.
- Startumstände können nachverfolgt werden.
- Jeder Prozess ist mit einer bestimmten Binärdatei und einem SHA-256 Hash verbunden.
- Prozesse haben bestimmte Command Lines, Zwecke und Lebenszyklen.

Durch den Vergleich des aus der Baseline bekannten Container-Verhaltens mit dem aktuellen Verhalten können Anomalien zuverlässig identifiziert werden, auch ohne vorher definierte Regel. Zudem wird das aktuelle Verhalten des Containers mit seiner Peer-Gruppe abgeglichen, in der sich ähnliche Container befinden. So lassen sich nicht nur bekannte, sondern auch unbekannte Bedrohungen

erkennen, wenn zum Beispiel eine containerisierte Applikation unerwartet viele Aufrufe neuer APIs startet. Dieser neue Ansatz adressiert wichtige Herausforderungen der Container-Sicherheit:

## Images und Registry kontrollieren

Container-Images beinhalten Betriebssysteme, Applikationen und Konfigurationsdateien. Die Bereitstellung der Images erfolgt zentral über die Registry. Bei der Entwicklung wird häufig auf öffentlich verfügbaren Images aufgebaut, die Malware enthalten können. Probleme entstehen auch durch die Übernahme von Standardkonfigurationen oder nicht aktuellen Patch-Ständen. Die Bereitstellung ungeprüfter Images muss daher ebenso verhindert werden wie der unbefugte Zugriff auf die Registry.

Prozess-Monitoring erfasst alle neu eingeführten Dateien, Hash-Werte und alle Änderungen an Images. Zur Malware-Identifikation werden Hash-Werte mit einer kuratierten Datenbank abgeglichen. Da alle Änderungsinformationen im Zeitverlauf bereitstehen, können bei einer Bedrohung nicht nur ein bestimmter, sondern alle betroffenen Container identifiziert werden.

## Orchestratoren schützen

Für das zentrale Management von Containern werden Orchestratoren wie Kubernetes oder Docker Swarm eingesetzt, die komplexe Konfigurationen erfordern. Häufig werden die Web-Interfaces dieser Werkzeuge nicht ausreichend geschützt oder Anwender-Accounts erhalten zu weitreichende Berechtigungen.

Durch Prozess-Monitoring erhalten Sicherheitsverantwortliche Einblick in Kubernetes-Cluster sowie in die Kommunikation zwischen Clustern. Visualisierungen gehen bis auf Namespace- und Pod-Level. Der Verhaltensabgleich mit der Baseline bringt ungeschützte API-Server oder Management-Konsolen ans Licht, zu denen ungewöhnliche Verbindungen gestartet werden sollen.

## Umfassende Sichtbarkeit gewährleisten

Container und Microservices werden on-demand gestartet und genauso schnell wieder gelöscht. Alle sicherheitsrelevanten Informationen, die nicht innerhalb weniger Minuten erfasst wurden, gehen verloren. Bestimmte Bereiche der Container-Kommunikation sind für herkömmliche Architekturen unsichtbar, wie zum Beispiel der Datenverkehr zwischen Containern auf derselben EC2-Instanz.

Prozess-Monitoring erfasst die gesamte Kommunikation im Zeitverlauf, auch innerhalb einer Datei oder zwischen Containern auf demselben Host. Log-Aufzeichnungen bleiben verfügbar, auch wenn der Container bereits wieder gelöscht wurde. Das ist ein wesentlicher Unterschied zum bekannten Traffic-Monitoring auf Networking-Ebene.

## Sicherheit automatisieren

Strategien für zukunftssichere Cloud- und Container-Sicherheit müssen von einer weiter wachsenden Komplexität ausgehen, die nicht mehr manuell beherrschbar ist. Jede weitere Punktlösung senkt die Sichtbarkeit. Stattdessen muss ausnahmslos jede Komponente und Aktivität in der Container-Umgebung zentral überwacht werden, damit Angreifer kein Schlupfloch finden und eine konsolidierte Reaktion auf akute Bedrohungen möglich ist. Bei dieser umfassenden Überwachung fallen gigantische Datenmengen an, die nur automatisiert ausgewertet werden können. Menschliche Eingriffe in Form von Regeln und Log-Auswertungen müssen daher eliminiert werden. Nur auf diesem Weg kann die IT-Sicherheit den Schutz von Cloud und Containern gewährleisten, ohne die Flexibilitäts- und Geschwindigkeitsvorteile zu gefährden.

Referenzen: **[1]** ForresterNow Predictions 2021: Cloud Computing **[2]** IDC, DevOps in Deutschland, 2020

**Bernd Mährlein**

Bernd Mährlein hat langjährige Erfahrung im Technologiesektor und ist seit Anfang 2021 als Area Director bei Lacework für den Aufbau der Region Central Europe zuständig. Zuvor war er bereits in verschiedenen Rollen bei Unternehmen wie Cybereason, MongoDB, Intralinks und SAP tätig.

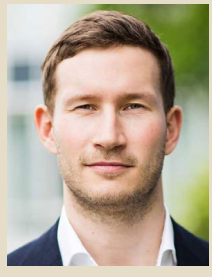


Foto: Privat

# Social Engineering: Das mächtige Werkzeug der Hacker

**Paul Arndt**
Ginkgo Cybersecurity GmbH

Social Engineering ist ein Konzept, dessen Ursprünge weit vor das Computerzeitalter zurückreichen. Gemeint ist damit gemeinhin die Erreichung eines Ziels mit Hilfe zwischenmenschlicher Beeinflussung. Doch wie genau funktioniert Social Engineering und was für mögliche Auswirkungen kann es haben? Warum ist es eines der effizientesten Werkzeuge für Hacker und was sind mögliche Gegenmaßnahmen?

## 1. Formen von Social Engineering

**Phishing**
Unter Phishing versteht man die ungezielte digitale Variante des Social Engineering.

Phishing wird analog zu einem Fischernetz angewendet. Das heißt, es werden sehr viele Nutzer mit wenig spezifischen Angriffen attackiert. Die Angreifer setzen darauf, dass zumindest einige der Angegriffenen auf diesen Phishing-Angriff reinfallen.

In der nebenstehenden Abbildung ist ein beispielhafter Phishing-Angriff dargestellt. Der Angreifer stellt sich als Zahlungsdienstleister PayPal dar und versucht die Anmeldedaten des Angegriffenen abzufangen. Falls dieser den Anhang öffnet, wird er oder sie zum Opfer des Phishing-Angriffs.

**Spear Phishing**
Eine Variante des Phishings ist das Spear Phishing. Für diese spezialisierte Form werden vor dem Angriff Daten über das Opfer gesammelt und dann für den Angriff verwendet. Diese Attacken zeichnen sich dadurch aus, dass sie bedeutend erfolgreicher sind als das klassische Phishing. Verwendet werden sie meistens im kommerziellen oder sogar militärischen Umfeld.

**Whaling**
Whaling ist eine weitere Spielart des Phishings, die sich vom Spear Phishing nur durch die Art der Ziele unterscheidet. Angriffsflächen des Whalings sind CEOs und andere Führungspersonen.

**Vishing**
Vishing wiederum bezeichnet Phishing über das Telefon. Angreifer versuchen mit Hilfe von Telefonie Personen zur Herausgabe von persönlichen Informationen wie Zugangsdaten zu bewegen.

**Baiting**
Baiting ist eine weitere Form des Phishings, die den Angegriffenen zur physischen Interaktion zwingt. Dabei wird zum Beispiel versucht, Personen mit einem USB-Stick als Werbegeschenk zu ködern. Sobald dieser Stick in dem Zielsystem eingeführt wird, wird eine Malware ausgeführt.

Da das Einführen von fremden USB-Sticks mittlerweile hohe Aufmerksamkeit erhalten hat, müssen Hacker diese Form des Angriffs weiterentwickeln. Eine sehr kreative und wirkungsstarke Form ist das manipulierte USB-Kabel. Dieses Kabel führt beim Einstecken in ein USB-Gerät einen Angriff aus. [1]

**Pretexting**
Diese Form des Social-Engineering-Angriffs charakterisiert sich durch das Verwenden eines zumeist erfundenen Vorwands (engl. pretext). Diese Vorwände können sehr komplex und präzise auf den Angegriffenen zugeschnitten sein. Pretexting findet für gewöhnlich in Zusammenarbeit mit anderen Formen des Social Engineerings statt. Beispiele für Pretexting sind zum Beispiel der sogenannte Enkeltrick, das Ausgeben als Servicetechniker, oder ähnlich gelagerte Vorgehensweisen.

**Contact Spamming**
Contact Spamming ist eine sehr effiziente Form des Angriffs, da hier Nachrichten von einer vertrauenswürdigen Quelle gesendet werden. Angreifer senden hierfür an alle Kontakte eines Opfers Phishing-Nachrichten. Da die Quelle vertrauenswürdig ist, wird der Inhalt seltener hinterfragt oder verifiziert.

## 2. Warum ist Social Engineering so effizient?

Die Effizienz von Social Engineering beruht im Wesentlichen auf drei Faktoren.

1. In den meisten Kulturen und Gesellschaftsformen werden Menschen zu einer allgemeinen Offenheit erzogen. Die meis-

ten von ihnen sind anderen gegenüber offen und hilfsbereit, solange bestimmte Regeln eingehalten werden. Dies ist ein wichtiger Faktor für das harmonische Zusammenleben in einer Gemeinschaft. Leider lässt sich dieses positive Verhalten durch böswillige Angreifer ausnutzten. Zu der grundsätzlichen Bereitschaft zu helfen kommt im geschäftlichen Umfeld oft auch noch das Thema Hierarchien hinzu.[2] Kann ein Angreifer glaubhaft machen, z.B. durch Kleidung, Auftreten und seine Sprache, einer höheren Hierarchie-Ebene anzugehören, öffnet dies oft Tür und Tor.

2. Zusätzlich zu dieser Offenheit werden bestimmten Rollenbildern gewisse Pflichten, aber auch Rechte zugesprochen. Wenn eine Reinigungsfachkraft sich in einem Unternehmensgebäude mit einer Reinigungsausrüstug bewegt, stellt dies normalerweise niemand in Frage, denn mit dieser Rolle wird die Aufgabe der Reinigung assoziiert. Damit geht aber natürlicherweise auch das Recht einher, sich relativ frei zu bewegen. Angreifer können diese Einschätzung nutzen und ein bekanntes Rollenbild erfüllen. Mit Hilfe von simplen Mitteln können hier oft erstaunliche Ergebnisse erzielt werden. Allein das entsprechende Auftreten und die passende Kleidung qualifiziert in vielen Fällen zur Managerin oder zum Manager. Eine Warnweste und ein Helm legitimieren einen Straßenarbeiter, der den Verkehr aufhält. Entsprechende Kleidung und Ausrüstung tarnen einen Angreifer als Sanitäter oder Handwerker, dem Zugang zu sensiblen Bereichen gewährt wird.
3. Zuletzt sind alle Menschen Individuen mit eigenen Interessen und persönlichen Schwächen. Diese lassen sich gezielt sammeln und für Social Engineering ausnutzen. Das Wissen über Vorlieben kann in Gesprächen gezielt genutzt werden, um Menschen zu beeinflussen. Ähnliche Interessen erwecken zum Beispiel in der Regel Sympathie. Wissen um Konflikte oder Ängste kann ähnlich verwendet werden.

Nach einer Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht fühlen sich lediglich 16 % der befragten Unternehmen von Social Engineering gefährdet.[3] Dies zeigt, dass trotz der Wirksamkeit und der im nächsten Abschnitt vorgestellten Auswirkungen dem Social Engineering nicht der notwendige Respekt entgegengebracht wird.

## 3. Auswirkungen von Social Engineering

Social Engineering wird häufig als Türöffner für technische Hackerangriffe verwendet. Insbesondere Ransomware-Angriffe und Datendiebstahl beginnen oft mit Social Engineering-Angriffen. Das Ponemon-Institut hat für das Jahr 2017 genauere Zahlen über Hackerangriffe erhoben. Danach wurden mindestens 69% der befragten Unternehmen Opfer von Social-Engineering-Angriffen. [4]

Erfolgreiche Social-Engineering-Angriffe können Schäden in enormer Höhe nach sich ziehen. Ein Beleg hierfür ist zum Beispiel die Attacke auf Twitter im Jahr 2020. Die Angreifer nutzten hierfür Spear Vishing, um Zugang zu internen Tools zu erhalten. Nachdem die Hacker Zugriff auf diese internen Tools hatten, konnten sie ohne technisches Know-how Passwörter von Twitter-Konten verändern und die Zwei-Faktor-Authentifizierung deaktivieren. Über die so gekaperten Accounts verfassten die Angreifer Tweets, die Nutzer dazu aufforderten Geld an


**Abbildung 1: Beispielhafte Phishing-Mail**

sie zu überweisen. Über diese stumpfe Methode konnten die Angreifer über 120.000$ erbeuten.[5] Zusätzlich zu dem direkten finanziellen Schaden der Nutzer nahm der Börsenwert von Twitter um über eine Milliarde US-Dollar ab.[6] Neben diesen messbaren Auswirkungen musste das Unternehmen Glaubwürdigkeit und Vertrauen einbüßen. Außerdem wurden von ausgewählten Nutzern die Direktnachrichten eingesehen und in deren Namen Nachrichten versendet. Dieses Beispiel zeigt, dass Social-Engineering-Angriffe finanzielle Schäden in Milliardenhöhe verursachen können. Darüber hinaus zeigt dieses Beispiel, dass Datendiebstahl mit Social-Engineering-Angriffen leicht durchgeführt werden kann.

## 4. Welche Gegenmaßnahmen gibt es?

Wie können Unternehmen sich vor Angriffen durch Social Engineering schützen? Tatsächlich gibt es kein Allheilmittel gegen Social-Engineering-Angriffe, ein gut geplanter Angriff hat immer große Chancen erfolgreich zu sein. Allerdings können präventive Maßnahmen ergriffen werden, um die Wahrscheinlichkeit von erfolgreichen Attacken zu verringern. Zudem können die Auswirkungen von erfolgreichen Angriffen durch gestaffelte und redundante Sicherheitsmechanismen begrenzt werden.

Basis jeder Strategie gegen Social-Engineering-Angriffe sollte das Training der Mitarbeiter darstellen. Mit Hilfe von Mitarbeiterschulungen kann die Sensibilität gegenüber Social Engineering deutlich gesteigert werden. Alle Mitarbeiter müssen ein gesundes Misstrauen gegenüber externen Quellen erlernen. Jede Nachricht von einem nicht vertrauenswürdigen Absender ist potenziell ein Angriff, der im schlimmsten Fall zu einem ernsten IT-Sicherheitsvorfall führen kann. Auf Grundlage


**Abbildung 2: getarnter Link**

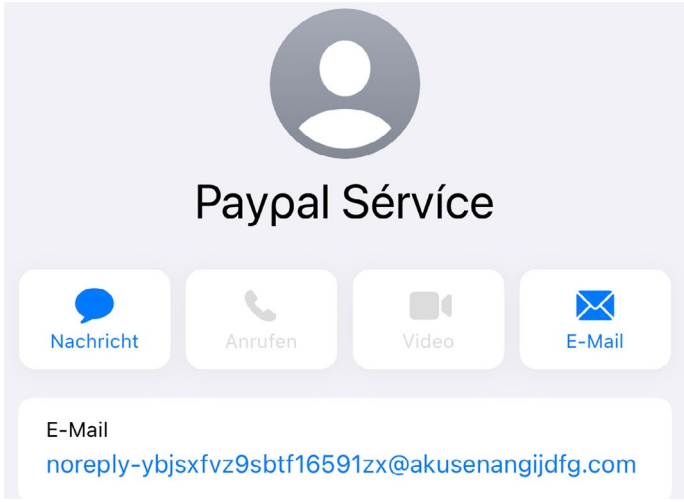



**Abbildung 3: nicht vertrauenswürdiger Absender**

dieses Misstrauens dürfen in keinem Fall Informationen, selbst die trivial wirkendsten, an Fremde gegeben werden. Jede noch so kleine Information kann einem Social-Engineering-Angriff dienen. Außerdem müssen Mitarbeiter im Erkennen solcher Attacken geschult werden. Zusätzlich zur Vorsicht gegenüber externen Quellen sollte der gesamten digitalen Kommunikation ein gesundes Maß an Misstrauen entgegengebracht werden, denn selbst wenn eine Quelle vertrauenswürdig erscheint, könnte es sich um einen Angreifer handeln. Selbst wenn nur geringe Zweifel an der Echtheit der empfangenen Nachricht bestehen, sollten Mitarbeiter telefonisch, oder am besten persönlich die Nachricht verifizieren.

Des Weiteren ist es möglich, technisch zu beschränken welche Links aus E-Mails verwendet werden dürfen. So kann zum Beispiel das Öffnen von Links von externen Absendern gesperrt werden. Außerdem ist es möglich bei allen E-Mails über einen Link zu hovern, um dessen Inhalt zu sehen. Im nebenstehenden Beispiel führt der Link nicht auf Google, sondern auf eine vermutlich bösartige Quelle.

Um das Misstrauen der eigenen Mitarbeiter gegenüber externen Quellen zu sensibilisieren, können diese automatisch als ausdrücklich nicht vertrauenswürdig markiert werden. Zusätzlich sollten alle internen Mails mit Hilfe von Zertifikaten signiert werden. Wenn ein Absender nicht bekannt ist, kann die Absenderadresse genauer betrachtet werden. In der nachfolgenden Abbildung ist ein Beispiel für eine solche definitiv nicht vertrauenswürdige Absenderadresse zu sehen.

Das Least-Privilege-Prinzip ist eine wichtige Gegenmaßnahme, die sich dadurch charakterisiert, dass Nutzer nur die Berechtigungen haben, die zur Bearbeitung ihrer Aufgaben tatsächlich benötigt werden. Somit werden viele Nutzer uninteressant als Ziel für Social Engineering-Angriffe, oder es müssen verschiedene Mitarbeiter identifiziert und manipuliert werden, wodurch erfolgreiche Angriffe deutlich unwahrscheinlicher werden.

Eine weitere effektive Maßnahme ist es, Befugnisse für kritische Prozesse auf mehrere Personen aufzuteilen, sodass in kritische Prozesse mehrere Personen involviert werden müssen. Ein klassisches Beispiel hierfür ist, dass niemals dieselben Personen einen neuen Zulieferer anlegen und gleichzeitig Rechnungen von diesem freigeben können sollte.

KI-basierte E-Mail-Überprüfung wiederum kann zur präventiven Erkennung von bösartigen E-Mails verwendet werden. Diese Erweiterung zu standardmäßigen Spamfiltern kann sehr hohe Erfolgsquoten bei der Abwehr von E-Mail basierten Social-Engineering-Angriffen erreichen. Jedoch darf der Einsatz eines solchen Tools nicht zu einem Gefühl der Sicherheit führen, denn gezielte Angriffe können auch diese KI-basierten Ansätze überwinden.

Im Allgemeinen ist ein „Defense in Depth"-Konzept wichtig, denn jede Gegenmaßnahme für sich kann von versierten Angreifern umgangen werden. Das Verknüpfen und Zusammenschließen einer Vielzahl von Gegenmaßnahmen führt zu einer weniger anfälligen IT-Umgebung.

Zuletzt ist es möglich die eingeführten Gegenmaßnahmen durch externe Dienstleister überprüfen zu lassen. Diese Experten versuchen, mittels Social-Engineering-Penetration-Testing Zugriff auf das Unternehmen zu bekommen. Der Vorteil hiervon ist es, dass Mitarbeiter hierdurch geschult werden und technische Maßnahmen geprüft werden können.

## Fazit

Social Engineering ist eines der – wenn nicht sogar das mächtigste Werkzeug von erfolgreichen Hackern. Da sich Unternehmen auf technischer Ebene immer besser gegen Cyber-Bedrohungen schützen, wird Social Engineering in Zukunft eine noch bedeutendere Rolle bei gezielten Attacken spielen. Auch wenn Unternehmen dieses Angriffs-Konzept nicht vollständig abwehren können, sollten entsprechende Schutzmaßnahmen auf keinen Fall vernachlässigt werden. Hier ist ein „Defense in Depth"-Konzept unabdingbar.

Referenzen: **[1]** https://www.futurezone.de/digital-life/article233239937/manipuliertes-usb-kabel-fuer-iphone-co-wer-es-anschliesst-wird-opfer-von-angriffen-ueber-wlan.html **[2]** https://mobil-krankenkasse.de/wissen-gesundheit/magazin/01-2018/helfen-macht-gluecklich.html **[3]** https://wiskos.de/files/pdf4/M3_Komplett_Online_neu_doi.pdf (Seite 43) **[4]** https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf (Seite 29) **[5]** https://www.businessinsider.com/twitter-reels-from-colossal-hack-as-new-details-surface-2020-7?r=DE&IR=T **[6]** https://www.businessinsider.com/twitter-market-value-losses-after-massive-hack-2020-7 **[7]** https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ **[8]** https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html **[9]** https://www.helpnetsecurity.com/2016/01/26/belgian-bank-crelan-loses-e70-million-to-bec-scammers/ **[10]** https://www.forbes.com/sites/leemathews/2019/09/06/toyota-parts-supplier-hit-by-37-million-email-scam/?sh=151ff5795856 **[11]** https://www.fnp.de/hessen/telefonbetrueger-setzen-auf-panik-bei-opfern-zr-91025310.html

# Aktuelle Beispiele für Social Engineering

## Angriff auf Mat Honan (2012)

Der Journalist Mat Honan und sein Twitteraccount wurden erfolgreich Ziel eines Hackerangriffs. In Folge dessen wurden über Mat Honans Account homophobe und rassistische Nachrichten verbreitet. [7]

Die Angreifer konnten mit Hilfe des Amazon Supports 4 Ziffern von Mat Honan's Kreditkarte bekommen. Dem Support von Apple genügten diese 4 Ziffern zur Verifikation von Mat Honans Identität.

Mit Hilfe der Apple Zugangsdaten konnte auf den iCloud Schlüsselbund zugegriffen werden, in dem die Zugangsdaten zu Twitter abgelegt waren.

## Angriff Google und Facebook (2016)

Im Jahr 2016 wurden Google und Facebook Opfer eines gezielten Social Engineering-Angriff. Hierfür wurden von den Angreifern tatsächliche Dienstleister der beiden Tech-Giganten nachgeahmt. In deren Namen sendeten die Angreifer Rechnungen an Mitarbeiter mit Finanzverantwortung. [8]

Dieser Angriff erfuhr eine positive Wendung, da der Kopf des Angriffs identifiziert und gefasst werden konnte.

## Angriff auf Crelan Bank in Belgien (2016)

Die Bank wurde Opfer eines Social Engineering Angriffs, bei dem sie über 70 Millionen Euro verloren hatte. Durchgeführt wurde dieser Angriff, indem die Angreifer sich als hochgradigen Manager der Bank ausgaben und Mitarbeiter zu Überweisungen angewiesen hatten. [9]

## Toyota-Teilezulieferer E-Mail-Betrug (2019)

Im August 2019 überzeugten Angreifer einen Angestellten der Toyota Boshoku Corporation, welcher über finanzielle Befugnisse verfügte, die Kontodaten einer elektronischen Überweisung zu ändern. Das Unternehmen verlor so über 4 Milliarden ¥ (37 Millionen $). [10]

## Telefonbetrug durch angebliche Polizei (2021)

Die Angreifer, die sich telefonisch als Polizisten ausgaben, behaupteten, dass ein Kind der Angegriffenen einen Unfall verursacht habe. Das Kind wurde angeblich in Untersuchungshaft gehalten und nur gegen Zahlung einer hohen Kaution freigelassen. Wie viel Geld mit dieser Methode bisher erbeutet worden ist, steht noch nicht fest. Die Angreifer forderten ca. 80.000€ Kaution. [11]

**Paul Arndt**

Paul Arndt (40) ist Managing Director der 2020 gegründeten Ginkgo Cybersecurity GmbH, ein Beratungshaus und Tochterunternehmen der Ginkgo Management GmbH. In dieser Funktion berät er Kunden unterschiedlichster Branchen national und international zu den Themen Cybersecurity.

Foto: Privat

# Trügerische Sicherheit: Aus diesen Gründen bleibt Ransomware weiterhin eine Gefahr

**Sebastian Evers**
Attingo Datenrettung Gmbh

## Nach Emotet ist vor Emotet

Die Zerschlagung der Verbreitungswege und Netzwerke von Emotet, Anfang 2021, wird als Meilenstein in der Bekämpfung von Cyber-Kriminalität gefeiert. Fast jede größere Ransomware-Kampagne hatte Emotet dazu verwendet, um Netzwerke zu infiltrieren und Malware nachzuladen. Darunter waren diverse Unternehmen (Konzerne, KMUs), Behörden und staatliche Einrichtungen sowie Krankenhäuser. Emotet war auch bei dem Ransomware-Angriff auf den Heise Verlag sowie die Funke Mediengruppe ein Schlüsselelement für die Täter. Alleine in Deutschland soll sich der durch Emotet und Begleitschadsoftware verursachte Schaden auf etwa 14,5 Millionen Euro belaufen. [1]

Emotet galt lange Zeit als die weltweit gefährlichste Schadsoftware. In Anbetracht dieser Einstufung hat die Abschaltung der Netzwerke rund um Emotet sowie die durch die Ermittlungsbehörden initiierte Selbstdeinstallation der Malware den Cyber-Kriminellen einen schwerwiegenden Schlag versetzt. Die Bekämpfung und Beseitigung von Emotet ist nur eine gewonnene Schlacht unter unzähligen – in einem Krieg von ungeahntem Ausmaß. Es ist ein stetiges Wettrüsten, und die Methoden der Täter werden zunehmend perfider. Der Sieg über Emotet ist nur ein abgeschlagener Kopf der Hydra. Mit der Stilllegung des gefürchteten „Downloaders“ werden Ransomware-Angriffe nicht einfach aufhören. Das Geschäft mit „Malware-as-a-service“ boomt dennoch weiterhin. Es ist also nur eine Frage der Zeit, bevor ein „Emotet 2.0“ auf der Bildfläche erscheint – weitaus besser und effektiver als sein berüchtigter Vorgänger.

Doch auch ohne Emotet gibt es mehr als genug Angriffe und ein Ende ist leider nicht in Sicht. Begünstigt durch verschiedene Gründe zieht es mehr und mehr Kriminelle in den Sumpf der Ransomware-Erpressung.

## Krypto-Währung begünstigt Ransomware-Erpressungen

„Follow the money“ lautet eine der kriminalistischen Faustregeln. Folgt man der Spur des Geldes, gelangt man auf diesem Weg früher oder später auch zu den Strippenziehern – so die grundlegende Idee. Allerdings sind die Täter bei Ransomware-Erpressung durch die schwierige – nahezu unmögliche – Nachverfolgung gezahlter Kryptowährungen quasi nicht ausfindig zu machen. Wo früher bei Erpressungen die Geldübergabe der größte Schwachpunkt des Verbrechens gewesen ist, ist dieses Risiko heute nahezu null. Auch pseudonyme Krypto-Währungen lassen sich über dezentrale Exchanges anonymisieren, von allen Anhaltspunkten kriminellen Ursprungs reinwaschen und in sauberes Geld umwandeln. Somit lässt sich der Wechsel von Krypto in Bargeld, ohne Hinweise auf kriminellen Ursprung, durchführen.

## Erpresser agieren in der Regel global

Die Zuständigkeit der jeweiligen Ermittlungsbehörden endet an den Landesgrenzen. Das wissen auch die Täter. Man kann also davon ausgehen, dass die Ransomware-Erpresser stets länderübergreifend agieren. Oftmals werden die personellen Strukturen in Osteuropa und Asien vermutet. Durch entsprechende OPSEC Maßnahmen ist eine Identifizierung der Täter fast unmöglich. Mit der Koordination der Angriffe aus einem anderen Land – oder mehreren anderen Ländern – ist es für lokale Ermittlungsbehörden nicht möglich effektiv gegen Täter vorzugehen. Die Verständigung der Polizei ist in vielen Fällen nur ein Placebo. Der Umstand schreckt die Täter nicht ab, ihre Verbrechen zu begehen. Sie wissen, dass sie geschützt durch mehrere Landesgrenzen beinahe nichts zu befürchten haben. Denn es kommt nicht immer zu einer landesübergreifenden Zusammenarbeit von Ermittlungsbehörden, wie im Falle von Emotet.

## Verbrechen auf Vertrauensbasis

Die Kriminellen haben sich den Ruf erarbeitet, dass sie die Daten nach Bezahlung der Lösegelder tatsächlich zur Verfügung stellen. Eine gewisse Romantisierung hat sich dadurch eingeschlichen. Es wird von einer „Ganovenehre“ gesprochen. Allerdings verfolgt die stringente Einhaltung der getroffenen Vereinbarungen gegenüber den Opfern ein klares Ziel: Es geht nur darum, die Zahlungsbereitschaft der Betroffenen nicht zu gefährden. Alles daran ist geschäftliches Kalkül. Es geht ausschließlich darum, dass die geforderten Lösegelder gezahlt werden. Solange jedem klar ist, dass die Erpresser die Daten gegen Zahlung freigeben, werden Betroffene auch dafür bezahlen, wenn ihnen keine Alternative zur Verfügung steht. Würden die Täter nach erfolgter Zahlung keine Daten herausgeben, würden sie sich damit zukünftige Geschäfte kaputt machen. Es ist eine Art perverser Symbiose zwischen Tätern und den Opfern entstanden.

## Zahlungsbereitschaft ist ein Problem

In der Situation des Opfers erscheint der Ausweg meist alternativlos: Wenn die Angreifer die digitale Infrastruktur lahm gelegt haben, dann stellt die Zahlung des geforderten Lösegelds in den meisten Fällen die schnellste und effektivste Methode dar, um zeitnah wieder handlungsfähig zu sein. Stillstand kostet in jeder einzelnen Minute große Summen. Die Erpresser wissen das genauso gut wie ihre Opfer. Und das beständige Ticken der Uhr ist auf krimineller Seite, denn in den meisten Fällen zahlen die Betroffenen. Das Lösegeld ist in der Regel geringer als der finanzielle Aufwand, der erforderlich wäre, um alles von Grund auf neu aufzusetzen. Ganz zu schweigen vom durch den Stillstand bedingten Verlust. Einziger Ausweg bleibt die Datenrettung von etwaigen gelöschten aber nicht verschlüsselten Backup-Systemen.

## Lösegeld-Versicherungen wecken Begehrlichkeiten

Vor Cyber-Angriffen ist niemand sicher, es wird im Laufe der Zeit jeden treffen – die Frage ist nur wann. Das haben die vergangenen Jahre immer wieder gezeigt. Viele Versicherungen bieten seit Längerem umfassenden Schutz gegen Hacker- und Cyber-Angriffe. Unternehmen schließen diese Versicherungen zunehmend mit immer höheren Abdeckungssummen ab, sodass die hohen Lösegeldforderungen übernommen sind, sollte man trotz allem einem Angriff durch Ransomware-Erpresser zum Opfer fallen. Doch diese vermeintliche Sicherheit ist ein großes Problem. Sie ist der Tropfen Blut im Piranha-Becken. Die Erpresser wissen über die hohen Abdeckungssummen Bescheid. Sie können sich sehr sicher sein, dass ein Angriff sich auch rentiert und dass das Opfer schnell bereitwillig zahlen wird, wenn eine Versicherung involviert ist. Sie können ebenso davon ausgehen, dass das Lösegeld in beliebiger Höhe angesetzt werden kann. Dieser Umstand führt dazu, dass sich immer mehr Kriminelle dazu berufen fühlen, mit Ransomware-Angriffen auf zahlungskräftige Klientel abzuzielen. Und wenn eine Versicherung wie Axa für Lösegelder künftig nicht mehr zahlt, wird sie selbst zum Ziel einer Attacke.

## Schutz vor Ransomware-Angriffen, Vermeidungs-Strategien [2] Erster Schritt: Vorbereitung

**Kontrolle ausüben: Updates und Patches aktuell halten**

Da bekanntermaßen die Ausnutzung von Sicherheitslücken die Infektion mit Malware begünstigt, ist der erste Schritt zur Prävention von Ransomware-Angriffen eine aggressive Patch- und Update-Strategie zur Absicherung der potenziellen Zielsysteme. Dazu zählt auch die Vermeidung des Einsatzes von Hardware, über die man zu wenig eigene Kontrolle hat.

**Besonders geschützte Sicherheitskopien**

Sicherheitskopien und deren Schutz sind ebenfalls von sehr großer Bedeutung. Das hohe Risiko von Ransomware bei groß angelegten Cyber-Angriffen auf Firmen resultiert daraus, dass die Angreifer Backup-Dateien und Datensicherungssysteme zerstören und die tagtäglich genutzten Dateien und Systeme verschlüsselt werden. Im Hinblick auf diese Gefahr sollten entsprechende Dokumente, Datenbankensysteme etc. in eng getakteter Abfolge offline an Orte kopiert werden, die für die Eindringlinge schwer bis gar nicht zu erreichen sind (z.B. Tapes, externe Festplatten oder Offline-Storage-Backups). Dabei sollte auch überprüft und getestet werden, ob sich die Daten ohne großen Aufwand aus den Backups wiederherstellen lassen. Permanent verbundene Netzwerklaufwerke (NAS) und auch Cloud-Speicher sind nicht komplett sicher, denn das Risiko, dass verschlüsselte Dateien automatisch dorthin gesichert werden und dadurch bestehende Backups überschreiben, ist immens.

**Vorfallreaktionspläne**

Es sollten spezifische Vorfallsreaktionspläne (Incident-Response-Plan, auch: IRP) für Ransomware-Attacken entwickelt werden, um sich auf gezielte Angriffe mit Krypto-Trojanern vorzubereiten, welche große Teile von Unternehmen lahmlegen könnten. Der Reaktionsplan sollte detailliert beschreiben, welche Personen was zu tun haben, sobald der Verdacht einer Netzwerk-Infiltration oder einer Ransomware-Attacke vorliegt. Nur auf diese Weise ist eine schnelle Reaktion umsetzbar – gleichzeitig aber auch eine mahnende Bewusstseinbildung im Vorhinein möglich. Für die Abwehr von Ransomware ist jede Sekunde entscheidend, welche dem IT-Security-Team bleibt, um die Verschlüsselung durch Krypto-Programme zu unterbinden oder zu unterbrechen.

**Umfassende Mitarbeiter-„Awareness“**

Diesem Aspekt gebührt besonders hohe – wenn nicht die höchste – Priorität: Umfassende Sensibilisierungsmaßnahmen und Schulungen („Awareness“-Training) für die Anwender sind eine unumgängliche wie auch sehr effektive Schutzmaßnahme, um sich gegen potenzielle Angriffe zu wappnen. Dadurch wird das Risiko reduziert, dass Angestellte auf Phishing-Mails – insbesondere Spear-Phishing-Mails – hereinfallen und damit die Malware ins firmeninterne Netzwerk holen. Viele Cyber-Angriffe setzen dabei auf Social-Engineering-Taktiken. Die Mitarbeiter sollten sich der Gefahr bewusst sein und lernen, wie eine verdächtige Nachricht enttarnt werden kann, um einer Infektion entgegen wirken zu können.

**Sicherheit durch „Security by Design“**
So banal es vielleicht auch klingen mag, eine durchdachte Netzwerktopologie, bei der Anwender nur soweit Zugriffe haben als sie es für den Arbeitsalltag benötigen, hilft in vielen Fällen vor einer massenhaften Ausbreitung und weitreichenden Vernichtungen. Ebenso verringern sich die Einfallsverktoren wenn nicht zwingend benötige Dienste – beispielsweise von NAS und IoT – nicht direkt über offene Ports im Internet zur Verfügung stehen, sondern sich hinter dem Schutz einer VPN-Firewall verstecken können. Ausreichend starke Passwörter für Logins auf Samba-Shares oder Administrationskonten setzen wir in diesem Umfeld selbstredend voraus.

## Zweiter Schritt: Entdecken und Feststellen

Organisationen können den potenziellen Schaden, welchen ein Angriff mit Ransomware verursachen könnte, minimieren, wenn die Malware früh genug entdeckt werden kann. Network-Intrusion-Detection-Systeme (NIDS) haben während der Infektions- und Exploitphase die Möglichkeit Signaturen sowie IOCs (Indicators of compromise) auszumachen. Mithilfe von Threat Intelligence hat IDS die Möglichkeit, um die Aktivität von Ransomware im Netzwerk aufzuspüren, zu stoppen oder zumindest eine Warnung an die IT-Sicherheitsbeauftragten zu senden.

Namhafte IDS-Anbieter haben zahlreiche Erkennungsmuster in ihre Systeme integriert, mit deren Hilfe Netzwerk-Anomalien aufgedeckt werden können. Diese Aktivitäts-Muster können sich je nach Ransomware und Ransomware-Version unterscheiden. Aus dem Grund ist es notwendig mehrere Verteidigungslinien aufzubauen. Trotzdem sind die Signaturen ein guter Ansatz, da somit die in den meisten Unternehmen eingesetzten Systeme zur Abwehr mit einbezogen werden.

**Das Stoppen ausführbarer E-Mail-Anhänge**
Generell sind alle Tools hilfreich, welche Attachments und Executables in Phishing-E-Mails ausfindig machen können, um Ransomware den Zugang zum Unternehmens-Netzwerk zu verwehren. Mit derartigen Schutzmaßnahmen existiert schon einmal eine grundlegende und automatisierte Verteidigung.

**Überwachung temporärer Dateien sowie Anwendungsdaten**
Mit der Tatsache, dass Ransomware zumeist aus den Verzeichnisordnern %appdata% oder %temp% startet, liefert einen weiteren Hebelpunkt: Die Überwachung dieser Ordner sowie darin ausgeführter Anwendungen und Programme ermöglicht es Ransomware zu entdecken, bevor diese die Gelegenheit hat Dateien zu verschlüsseln. Wie schon in der Exploit-Phase kann man über Netzwerk-Regeln die Ausführung sowie Verbreitung von Malware wie Ransomware visualisieren. Oder man transferiert seine Workstations auf Linux-Systeme, denn dort gibt es besagte Ordner in dieser Form erst gar nicht.

**Vssadmin-Befehle beaufsichtigen**
Angriffe auf Backups und der Versuch die Datensicherungen zu zerstören erlauben es, ebenfalls die Ransomware-Aktivitäten aufzudecken, bevor die Verschlüsselung gestartet werden kann. Die Ausführung von „vssadmin“-Kommandos sollte dabei besondere Beachtung finden und nach Möglichkeit mit einem Alarm verknüpft werden. So haben Verantwortliche eine reelle Chance, rechtzeitig einzugreifen und gefährdete Computer und Netzwerklaufwerke vor der Ransomware-Verschlüsselung zu schützen.

**Kontrolle von Registry-Einträgen und Dateiendungen**
Auch die Überwachung der Kommunikation des Command-and-Control Servers (C&C) ist eine Möglichkeit, um anhand von Netzwerk-Signaturen, der Vergabe von Dateinamen und Änderungen in der Registry zu erkennen, dass beispielsweise der zu Beginn der Verschlüsselungsphase erforderliche Schlüsselaustausch erfolgt. Die Ransomware Locky fiel dadurch auf, dass immer mehr Dateien mit der Dateierweiterung .locky auftauchten. So konnte der Befall mit dem Krypto-Trojaner bemerkt werden.

Leider benutzen viele Krypto-Trojaner mittlerweile einzigartige Dateierweiterungen, die von Befall zu Befall unterschiedlich sind. Zudem ist die Umbenennung der verschlüsselten Dateien durch die Ransomware in der Regel ein recht später Schritt, der ziemlich zum Ende des Krypto-Angriffs erfolgt. Dennoch können die Indikatoren bereits ausreichen, um das Ausmaß des Angriffs eingrenzen zu können – wenn der Angriff schon nicht verhindert werden kann.

## Dritter Schritt: Eindämmung und Quarantäne

Ist bereits ein Gerät der Ransomware zum Opfer gefallen, so gibt es nach wie vor die Möglichkeit den Angriff auf dieses Umfeld zu beschränken, um den Angriff auf Dateien im Netzwerk zu verhindern.

Endpoint-Security-Systeme, die ausführbare Dateien erkennen und die Prozesse stoppen können, sind ein guter Ansatz für eine Eingrenzung von Ransomware-Attacken. Wird schadhafte Malware entdeckt, so wird die Netzwerk-Verbindung unmittelbar getrennt und die Schadsoftware ist auf dem jeweiligen System isoliert, sodass sie keine Dateien im Netzwerk verschlüsseln kann.

## Vierter Schritt: Systembereinigung und Entfernung von Ransomware / Malware

Ist der Ransomware-Angriff identifiziert und eingedämmt worden, ist es unabdingbar, die Malware sowie etwaige Spuren zu entfernen. Es empfiehlt sich betroffene Systeme zu ersetzten, anstatt diese nur zu „säubern", da sich diverse Malware überaus gut in den Tiefen der Hardware zu verstecken weiß. Möglicherweise wurden bereits Router oder Drucker infiziert, in dem sich die Dateien verstecken, um für den Fall einer Entdeckung vor einer effektiven Bereinigung sicher zu sein und im Anschluss das Netzwerk erneut zu infizieren.

Wann immer man sich für eine Säuberungsaktion entschließt, anstatt für das Ersetzen kompletter Hardware, sollte im Nachhinein eine penible Überwachung auf IOC und Signaturen erfolgen, um ein wiederholtes Aufkommen der Ransomware-Infektion schnellstmöglich zu unterbinden.

## Fünfter Schritt: Wiederherstellung von Netzwerken, Systemen und Daten

Die Wiederherstellung umfasst zunächst einmal das Wiedereinspielen von Datensicherungen und Backups der zerstörten und verschlüsselten Dateien. Für ein Unternehmen, das auf umfassende und geprüfte Sicherheitskopien zurückgreifen kann, kann ein Krypto-Angriff mit Ransomware nahezu folgenlos bleiben. Es ersetzt die befallenen Geräte oder säubert sie und rekonstruiert den Datenbestand aus den Backups – ratsamerweise aber zumindest auf neuen Datenträgern, um die infizierten Originale für spätere Ermittlungstätigkeiten oder noch benötigte Datenwiederherstellungen zur Verfügung stehen. Dabei wird man eine kurzzeitige Unterbrechung bei den IT-Anwendungen in Kauf nehmen müssen. Es ist recht unwahrscheinlich, dass die Attacke unter derartigen Voraussetzungen zu einem tagelangen Problemzustand wird – auch wenn es in dieser Hinsicht bereits Fälle gegeben hat, bei denen z.B. NotPetya einen internationalen Logistikkonzern beinahe vollständig lahm gelegt hat. Zehn Tage lang arbeitete das Unternehmen vollkommen analog, bis die IT-Infrastruktur wieder online war.

## Wie kam es zu dem Ransomware-Befall?

Bei jedem Cyber-Angriff lohnt sich eine genauere Beleuchtung, wie die Infektion stattgefunden hat. Waren es Phishing-E-Mails oder web-basierte Angriffs-Kits? Wenn es ein web-basierter Angriff gewesen ist, wie wurde der verantwortliche Anwender auf die Internetseite gelockt? Wenn man herausfinden kann, wie Ransomware in die Systeme und ins Netzwerk gelangen konnte, dann lassen sich mit diesen Erkenntnissen Abwehr- und Erkennungsmethoden maßgeblich optimieren und Schwachstellen für die Zukunft minimieren.

## Die Bedrohung durch Ransomware wird nicht verschwinden

Ransomware-Angriffe gegen KMUs, Konzerne, Behörden und öffentliche Einrichtungen sowie Krankenhäuser stellen eine Gefahr dar, welche trotz ihrer Häufigkeit erst die Spitze des Eisbergs des potenziell Möglichen bildet. Aufgrund der Attraktivität solcher Angriffe und der damit erzielten Erfolge werden Täter zunehmend häufiger darauf setzen. Und die Angriffe werden sukzessive an Schlagkräftigkeit und Gefährlichkeit dazu gewinnen, sodass noch gewaltigere Schäden, mit noch höheren Kosten die Folge sein werden.

Die Wenigsten sind auf Datenverlust durch derartige Ransomware-Angriffe vorbereitet – egal, ob groß oder klein. Die kaum absehbaren Folgen stellen einen weitaus kritischeren Verlust dar, als die Bezahlung der geforderten Lösegeldsumme: Imageverlust, Produktivitätseinbußen, eingeschränkte Geschäftsfähigkeit, beeinträchtigte Kundeninteraktion, Datendiebstahl oder die Veröffentlichung brisanter Daten. Die erfolgreiche Abwehr eines Ransomware-Angriffs hängt davon ab, wie gut man darauf vorbereitet ist, die Indizien für das Treiben von Krypto-Trojanern oder anderer Malware zu erkennen und verdächtige Aktivitäten zeitnahe zu stoppen.

## Besser auf Ransomware vorbereitet sein

Es ist stets besser, auf den Extremfall vorbereitet zu sein, der niemals eintritt – und das wird er mit an Sicherheit grenzender Wahrscheinlichkeit dennoch irgendwann -, anstatt beim Eintreten des Extremfalls schutzlos ausgeliefert zu sein. Mit einfacheren Worten: Vorsicht ist besser als Nachsicht.

Quellen: **[1]** https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210127_pmEmotet.html **[2]** https://www.attingo.de/blog/so-schuetzen-sie-sich-effektiv-gegen-ransomware-angriffe/

**Sebastian Evers**

Sebastian Evers ist seit 2010 als Kundenbetreuer bei der für ganz Deutschland zuständigen Attingo Datenrettung GmbH in Hamburg tätig. Regelmäßig bloggt er zu spezifischen Themenfeldern aus dem Bereich der professionellen Datenrettung und informiert über die „Dos and Dont's".

Foto: Privat

# Cyberangriffe bei Unternehmensfusionen: Bedrohungslage und Abwehr

**Kai Lucks**
MMI Merger Management Institut

Cyberattacken auf Unternehmen sind zunehmend verbreitet und ein lukratives Geschäft für die Angreifer. Im Schatten der aktuellen Cyber-Diskussion und weit unterschätzt von den Unternehmern sind Angriffe, die im Zuge von M&A stattfinden.

Rund 60.000 Cyber-Angriffe richten russische Hacker täglich auf deutsche Ziele. Die weltweit zu zählenden Attacken, die aus allen Regionen kommen, gehen hochgerechnet in den zweistelligen Millionenbereich. Mit stark steigender Tendenz. Denn dieses Geschäft ist für die Angreifer höchst lukrativ – und mit relativ geringen Risiken behaftet, denn sie greifen geschützt aus dem Darknet an und lassen sich mit Kryptowährungen bezahlen. Mittlerweile hat sich eine ganze Cyber-Industrie gebildet. Das „Marktvolumen", d.h. die Summe der Zahlungen durch Cyber-Erpressung, liegt bei 6 Mrd. US-Dollar. Die Angreifer kommen aus allen Weltregionen, aus den Industrieländern, aus Schwellenländern, aus dem Inland – und gelegentlich auch aus dem eigenen Unternehmen. Große Angriffe lassen sich grob zurückverfolgen. Eine deutlich konzentrierte Angreifer-Gemeinschaft ist ansässig in Russland, in China und in Nordkorea. Diese Regionen sind sogar geprägt von speziellen Industriestrukturen, teils staatlicherseits betrieben, etwa aus Devisenmangel, zur Finanzierung besonderer Programme (etwa der Nuklearaufrüstung Nordkoreas) oder in Verbindung mit Industriespionage und gezielten Angriffen auf sensible Branchen der Industrieländer.

## Organisierte Cyber-Kriminalität

Die „Gemeinschaften" sind hochprofessionell organisiert, etwa in Form von Franchising-Strukturen mit einem zentralen Treiber, der die Ziele auskundschaftet, also quasi Marktforschung, Kandidatenscreening, Priorisierung, Angriffe und Verfahren vorgibt. Dieser ist vernetzt mit externen „Methodikern", den eigentlichen Hackern, sofern er sie nicht schon an Bord hat: IT-Freaks, IT-Spezialisten, und High-Tech-Angreifern aus Spezialinstituten, die sich im Dunstkreis von Regierungen, Ministerien und Geheimdiensten befinden. Spitzenangriffe waren spektakulär, etwa die Ausschaltung der Zentrifugen-Steuerungen für die nukleare Brennstoffanreicherung im Iran. Die Angreifer kamen aus dem Geheimdienst der USA. Zuvor wurden die Ziele genau evaluiert: nämlich die Siemens-SPS-Steuerungen. Deren Architekturen und Sicherheitslücken musste man sich beschaffen. Es liegt nahe, auf welchen Wegen und unter wessen Druck auf wen.

## Der Cyber-Krieg

Dies sind keine Verschwörungstheorien. Die Bedrohung ist real. Vorstände aus der IT-Branche der USA sprechen zunehmend von einem Cyber-Krieg, der immer weiter eskaliert. Dabei wird auch systematisch ausgetestet, inwieweit Industrienationen durch Angriffe auf ihre systemrelevanten Branchen geschwächt werden können. Die Spitzen-Angriffe auf Konzerne erfordern Spitzenkenntnisse und breit gefächerte Kompetenzen, also Teams und Ressourcen, wie sie nur von Geheimdiensten und Fachministerien unter Initiative und Finanzierung von Regierungen bereitgestellt werden können. Die großen Konzerne stellen ihrerseits große Ressourcen zur Cyber-Abwehr bereit. Selbst Grundlagenforschung, etwa zur Weiterentwicklung von Instrumenten, die der sogenannten Künstlichen Intelligenz zuzurechnen sind, wird zur Entwicklung von Cyber-Angriffs-Verfahren betrieben. Mittlerweile hat sich ein Wettbewerb zwischen „guter KI" und „böser

KI“ entwickelt, der die Leistungen immer weiter in die Höhe schraubt – aus dem Wissen der „guten Verteidiger“, dass sie nur gewinnen können, wenn sie die Nase vorn haben. Vielleicht mit nur einem Jahr Vorsprung.

## Häufigste Angriffsformen

Die Angriffsformen sind äußerst vielfältig. Am verbreitetsten sind Attacken mithilfe von Betrugs-Software (Betrug, engl.: Ransom). Ransomware-Angriffe können äußerst unangenehme Folgen für Unternehmen haben. Bei Ransomware handelt es sich um polymorphe Viren wie Locky, Tesla oder Petya, die den Rechner oder ein ganzes Netzwerk durch Verschlüsselung der lokal gespeicherten Dateien lahmlegen. Bekannteste Spezies davon sind Kryptotrojaner, die bereits Firmen in ihrer Existenz bedrohen oder sogar in die Insolvenz getrieben haben. Ein „Worst-Case-Szenario“ eines Ransomware-Angriffs beginnt typischerweise bei einem Mitarbeiter eines Unternehmens, der sich auf dem Dienstrechner einen Kryptotrojaner einfängt. Anschließend dauert es nicht lange, bis sich der Schädling über das gesamte Firmennetzwerk ausgebreitet hat. Ransom-Schäden können den Unternehmer vor unlösbare Probleme stellen. So ist er bereit, den Erpressern für die Freigabe der blockierten IT-Bereiche hohe Geldsummen zu bezahlen: „Easy money“ für die Angreifer.

## Enormer Schaden bei der Reederei Maersk

Mit einem solchen Fall hatte die weltweit größte Reederei A. P. Møller Maersk zu kämpfen. Das Unternehmen musste im Juni 2017 einen massiven und globalen Ausfall der IT-Systeme hinnehmen. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) handelte es sich bei der eingesetzten Schadsoftware hier um den Kryptotrojaner Petya. A. P. Møller Maersk reagierte prompt mit der Teilabschaltung von ganzen Systemen. Somit konnte zwar ein Worst-Case wie die Gefährdung der Steuerungssysteme der Container-Schiffe unterbunden werden, jedoch kam es noch wochenlang zu Unterbrechungen in ihrer Flotte. Nicht ohne finanzielle Folgen für A. P. Møller Maersk. Man geht davon aus, dass der Hackerangriff dem Unternehmen insgesamt 200 bis 300 Millionen Euro gekostet hat.

## Zahlreiche Angriffe kamen den Opfern teuer zu stehen

Der französische Baumaterialhändler Saint Gobain musste 2017 nach einem Cyber-Angriff seine Computer vollkommen vom Netz nehmen, um Daten zu retten. Der US-Pharmariese Merck hatte nach einem Angriff Probleme, seine Daten zu retten. Der britische Konsumguthersteller Benckiser berichtete, dass er nach einem Cyber-Angriff Mühe hatte, seine Fertigung wieder hochzufahren und die Distribution wieder zu aktivieren. Das kostete dem Unternehmen 130 Millionen US-Dollar an Umsatz.

Die vorgenannten Fälle gingen auf das Konto der NotPetya-Malware, die zehntausende von Systemen in mehr als 65 Ländern traf. Neben den genannten Unternehmen waren darunter Großorganisationen wie Rosneft, FedEx, Mondelez International und Nuance Communication. Viele der weiteren Opfer befanden sich in der Ukraine, der Heimat einer Steuersoftwarefirma, deren Produkt zu den Attacken verwendet wurde.

## Hohe durchschnittliche Schäden

Experten beziffern die durchschnittliche Ausfallzeit, die mit einem Angriff durch Kryptotrojaner einhergeht, mit 9 bis 16 Stunden. Typischerweise laufen Kosten aus mehreren Einzelschäden auf, die bei der Wiederherstellung des Betriebs und der Entfernung des Kryptotrojaners zusammenspielen. Dazu zählt auch der Verlust von Datensätzen, der entsteht, wenn das betroffene Unternehmen in der Vergangenheit nicht regelmäßig oder gar keine Backups durchgeführt hat. Für jeden verlorenen Datensatz rechnen die Herausgeber der Studie „Cost of Data Breach” mit umgerechnet durchschnittlich 325 Euro. Wenn man bedenkt, dass hier schnell einige tausend verlorene Datensätze zusammenkommen, dann kann man den Kostenumfang leicht hochrechnen, den ein Datenverlust mit sich ziehen kann. Hinzu kommen Kosten für die Analyse über das Ausmaß des Angriffs. Hierbei ist insbesondere zu überprüfen, welche Geräte und Daten verschlüsselt wurden und um welche Art von Kryptotrojaner es sich handelt. Nicht selten ziehen Unternehmen hierzu IT-Expertenteams zurate, die durchaus mehrere Tage für solch eine aufwendige Untersuchung benötigen können. Kosten, die hierfür entstehen, können dann schnell in den fünfstelligen Bereich schießen. Zudem können weitere Aufwendungen hinzukommen – so etwa für Anwälte und Gerichte, die Benachrichtigung der Öffentlichkeit, die Datenrettung, zu zahlende Strafen an Regulierungsinstitutionen sowie Überstunden für Angestellte.

## Große Angriffe führen häufig zu Insolvenzen

Ein Fünftel aller Unternehmen meldet bereits nach einer ersten großen Kryptotrojaner-Attacke Insolvenz an. Ein Angriff durch Ransomware kann für Unternehmen die unterschiedlichsten Konsequenzen haben. Die meisten Firmen folgen den Tipps von Experten, das geforderte Lösegeld nicht zu bezahlen. Allerdings treten auch bei Nichtzahlung erhebliche negative Konsequenzen ein. Nach Expertenschätzungen müssen insgesamt 20 Prozent aller Unternehmen, die Opfer eines Kryptotrojaners wurden, den Betrieb vorläufig komplett einstellen. Weitere 15 Prozent mussten erhebliche Umsatzverluste hinnehmen. Auch waren 25 Prozent der Unternehmen nicht in der Lage, das Einfallstor zu identifizieren. Dies führte dazu, dass sich der Schädling ungehindert im Netzwerk ausbreitet. Sind Schädlinge wie Kryptotrojaner erst einmal in das Firmennetzwerk eingedrungen, wird es nicht nur aufwändig, sondern auch teuer, die verseuchten Systeme wiederherzurichten. Nur mit den richtigen Präventivmaßnahmen lassen sich negative Folgen eines Ransomware-Befalls abwenden.

## Der Mittelstand wird zum wichtigsten Angriffsziel

Angesichts hoher Verteidigungsmauern der Großkonzerne hat sich die „Masse" der Cyber-Angreifer auf die darunter liegende Schicht größerer mittelständischer Unternehmen konzentriert. Hier sind die Hürden nicht ganz so hoch, die Aufmerksamkeit geringer. Und die Potenziale, um ertragreiche Erpressungen durchzuführen, sind größer. Denn der Aufwand für groß angelegte Angriffe ist nicht unbeträchtlich. Deshalb müssen die Angriffsziele gut gewählt sein. Kleinere Mittelständler sind (noch?) nicht das Ziel, denn sie verfügen nicht um die Geldmittel, die man erpressen kann und mit denen sich ein Angriff lohnt.

Deshalb richtet sich die Breite der Angriffe in zunehmendem Maße auf große Mittelständler – und davon hat Deutschland mehr als alle anderen Länder der Welt: allein 6.000 Unternehmen mit einem Umsatz von über 50 Millionen Euro sowie 1.000 Weltmarktführer.

## Geringes Cyber-Risikobewusstsein gefährdet M&A

Obwohl die Aufmerksamkeit bei Konzernen und dem größeren Mittelstand auf die Beherrschung und Abwehr von Cyber-Angriffen durchaus gegeben ist, bleibt das Feld der Cyber-Sicherheit vor, während und nach M&A-Transaktionen auf merkwürdige Weise weitgehend unbeachtet. Nur wenige Unternehmen haben dies auf ihrem Radar. Konkrete Nachfragen wurden von unserer Seite wurden meist nicht oder ausweichend beantwortet – teilweise verständlich, um potenziellen Angreifern keine Lücken im Verteidigungsring anzubieten, wie beschrieben.

Angreifer haben M&A bereits als besonders günstige Gelegenheiten für Cyber-Attacken ausgemacht, insbesondere weil der Zeitdruck im Projekt, die Kommunikation, die Übergänge und Überführungen von unternehmerischen Aktivitäten viele Angriffsmöglichkeiten bieten – die sich bei genauerer Analyse von außen auch gut lokalisieren lassen.

## Deutliche Schwächen bei M&A werden sichtbar

Die faktische Schwäche und das Übersehen von Risiken werden aber im Zuge von konkreten Verhandlungen über M&A-Beratungen und die Vergabepraxis überdeutlich, etwa zur IT Due Diligence im Allgemeinen und speziell zu einer Cyber Security Due Diligence. Dabei ist die Bewältigung und die Abwehr von Cyber-Angriffen im Zuge von M&A nicht nur in der Prüfungsphase relevant, sondern über den gesamten M&A-Prozess, beginnend mit ersten Vorsignalen des Vorstandes in der Presse zu M&A-Absichten und mehr noch wenn ein Deal bzw. die namentliche Nennung von Kandidaten angekündigt werden. Das Thema Cyber-Management bei M&A endet auch nicht mit dem Closing oder mit dem Abschluss der formalen Implementierung, sei es im Stand-alone-Fall – bei reinen Übernahmen ohne Integrationen, etwa für Private Equity – oder bei Integrationen des operativen Geschäfts.

## Zeitwahl und Angriffspunkte bei M&A identifizieren

Die Praxis hat gezeigt, dass die Angreifer ein potenzielles Ziel, das im Zuge von M&A angegriffen werden soll, sehr frühzeitig identifizieren und dann systematisch durchleuchten, mit den Fragen (a) ob sich ein Angriff lohnen könnte und (b) wann der optimale Zeitpunkt für einen Angriff gegeben ist. Das kann, wie Beispiele zeigen, auch Jahre nach der Übernahme sein. Dies bezeugt, dass die Angreifer zunächst strategische und operative Untersuchungen anstellen, bevor sie ihre teuren und fachlich herausfordernden Angriffe starten. Da geht es knallhart um die Maximierung von Erträgen, Risikobewertungen und Investitionsentscheidungen. Der finanzielle, der personelle und organisatorische Aufwand für die Einsätze der treibenden Einheit und der einzuschaltenden Subunternehmer muss vorab analysiert werden – vor allem der technischen Erforschung und Durchführung der Angriffe. Eine große Einzelaktion bindet alle Ressourcen und schließt damit andere Ziele für die Zeit der Angriffe weitgehend aus.

## Selbstverständnis und Selbstbewusstsein der Angreifer nutzen

Wie aus Verhandlungen mit Angreifern deutlich wurde, sehen und betreiben sie ihr Geschäft professionell und mit der Überzeugung, einer Branche anzugehören, die in dem Ökosystem einer offenen Wirtschaftswelt eine Daseinsberechtigung hat. Die meist jungen Hacker und auch die IT-geschulten älteren Profis sind überzeugt oder glauben, einer Elite anzugehören, die den unterlegenen Targets in einem ungleichen Kampf das Management ihres Geschäftes bzw. ihrer (M&A-) Prozesse aus der Hand nehmen darf, frei nach dem Motto „das Recht des Stärkeren ist immer das bessere". Die Kriminalität ihres Handelns blenden sie aus. Das Darknet verleiht ihnen Sicherheit. Selbst die Geldübergabe ist, dank virtueller Währungen, kein Risiko. Neben der finanziellen Attraktivität des Cyber-Geschäftes sind Angriffe auch ein sportliches Erlebnis. Die öffentliche Aufmerksamkeit der Fälle, ohne dass die Angreifer sich zu erkennen geben, ist dabei ein besonderer Kick.

## Daraus ergeben sich Schlüsse zur Verhandlungsführung

Erkenntnisse über die Motivationslagen der Angreifer geben Hinweise, wie Verhandlungen zwischen Verteidigern und Angreifern psychologisch geführt werden müssen. Erfahrungen aus solchen Fällen und ein gewisser neutraler Anstrich externer Gesprächspartner implizieren, dass ein angegriffenes Unternehmen erfahrene externe Verhandler einsetzen sollte. Die Angreifer vermuten zurecht, dass ein Externer am ehesten eine Brücke zwischen den ungleichen „Partnern" in diesem aufgezwungenen „Deal" bauen kann.

## Wie ist bei Cyber-M&A-Projekten vorzugehen, nach Standards oder „Kür"?

Als Grundlage sind die nationalstaatlichen Regularien zu beachten,

etwa die Datenschutz-Grundverordnung in Deutschland und die EU-weit gültigen Regeln der General Data Protection Regulation. Darauf baut der deutsche BSI-Standard auf, als Methodik zur Herstellung eines soliden Informationssicherheitsmanagements, kurz ISMS. Die BSI-Standards sind ein elementarer Bestandteil der IT-Grundschutz-Methodik. Sie enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit. BSI ist aber ein reiner Sicherheitsstandard und kein Projektleitfaden. Wichtiger für die Projektarbeit auch hierzulande sind die internationalen NIS-(Network and Information Security-) Standards, die als ein Rahmenwerk zum prozeduralen Vorgehen in Cyber-Risiko-Projekten zu verstehen sind. Dieser „Rahmen" gibt nur die zu bearbeitenden Felder vor und die prozedurale Einbindung.

## Geschäftsspezifische Vorgehensweisen sind zu entwickeln

Konkret heißt dies, dass für den speziellen M&A-Fall die jeweils probaten Mittel und Pfade gesucht und angewendet werden müssen. Dies setzt natürlich die fachlichen IT-Kenntnisse voraus sowie Erfahrungswissen über Cyber-Angriffe und -Verteidigung. Wichtigste Weichenstellung für die Projektführung ist die Definition des Geschäftes, um das es geht, insbesondere die Branchen, die bearbeiteten Wertschöpfungsstufen und die Regionalitäten der Beteiligten. Die besondere Herausforderung bei einem Cyber-M&A-Projekt liegt darin, die Vorgehensweisen bei komplementär angesiedelten Geschäften festzulegen, etwa unterschiedliche Geschäftsdefinitionen und verschiedene Länder.

## Cyber Due Diligence bei M&A sollte zur Regel werden

Eine zentrale Rolle bei M&A spielt die Unternehmensprüfung, also die Due Diligence, die der Verkäufer im Vorfeld zur Absicherung von Daten und Fakten über das zur Disposition stehende Unternehmen oder Unternehmensteile durchführen kann („Vendor Due Diligence"), um damit Informationsproblemen bei den späteren Verhandlungen zuvor zu kommen. Breite Verwendung spielt die vom Käufer zu fordernde „Purchaser Due Diligence". Beide sollten nach heutiger Erkenntnis eine IT Due Diligence und insbesondere Einsätze zum Thema Cyber-Risiko-Management beinhalten. Der Ansatz der Cyber Due Diligence sollte genau der strategischen Positionierung und der zukünftigen Ausrichtung der kombinierten bzw. integrierten Geschäfte folgen. Präventive und defensive Aspekte des Cyber-Schutzes sind herauszuarbeiten. Auch der Integrationstypus muss Berücksichtigung finden.

## Cyber Due Diligence Scans durchführen

Zu einer quasi „flächendeckenden" Prüfung innerhalb einer Due Diligence gehören auch sogenannte (rapid) Scans, die auf spezifische Themen ausgerichtet sein können. Innerhalb einer Cyber Due Diligence bieten sich verschiedene Scans an. Diese dienen der Klärung des Sicherheitsprofils. Zu unterscheiden sind unternehmensintern ausgerichtete Scans und extern orientierte, etwa auf die Angreiferlandschaft und die zu erwartenden Angriffe und Methodiken. Für die Scans sollten auch Dritte beaufschlagt werden, so etwa sogenannte Intrusive Scans durch professionelle Hacker, also Versuche, in die Netze der M&A-Partner und die Aktivitäten der M&A-Teams einzudringen. Dafür sind entsprechende Genehmigungen einzuholen.

Zu den externen Scans, die keiner Genehmigung bedürfen, gehören Internet-Recherchen. Nötigenfalls Versuche im Dark Net – die aber juristisch abgesichert und den Aufsichtsbehörden gemeldet werden sollten. Grundsätzlich sollten kombinierte Scans der Hard- und Software-Infrastruktur vorgenommen werden. Dabei geht es um den Einsatz jüngster Technologien, Schutzeinrichtungen wie HW, SW und Sicherstellung, dass die letztbekannten Sicherheitslücken durch „Security Patches" zeitnah geschlossen werden. Bei IT-nahen Geschäften sind z.B. Security Scans der Server des Targets vorzunehmen. Besondere Risiken eröffnen sich durch Open Source-Software-Produkte. Zur Sicherheitsprüfung bieten sich externe Fachspezialisten an.

## Cyber-Security bei M&A als Mensch-Maschine-System implementieren

Die Prüfungen sollten „systemische" Betrachtungen einschließen, also neben der technischen Seite auch den Humanfaktor. Probleme können nämlich auch durch menschliches Fehlverhalten entstehen, wobei unwissentliches und böswilliges Verhaltenswesen einzuschließen sind. Fehler, Lücken und Probleme können auf Nachlässigkeit, Frustration, Abwehr und kriminelle Energie zurückgeführt werden. Gefährder sind Frustrierte, Verlierer und Gegner des Deals. Insbesondere die Phasen der Unsicherheit, Ängste vor Veränderungen und Furcht vor Jobverlust können bei M&A unerwartete Handlungen hervorbringen, auch Sabotage und Spionage von innen.

Systematische Personaluntersuchungen können Risikoquellen aufdecken. Dies muss unter Beachtung der DSGV erfolgen, Mitarbeiter müssen darüber informiert werden, und Maßnahmen sollten schnellstens gezogen werden. Mit Sensibilität im personellen Umgang und einem psychologisch hinterlegten kulturellen Change Management können potenzielle Gefahrenherde im Innen- und Umgebungsbereich der M&A-Parteien eingedämmt werden. Summa summarum: „Inside Protection" ist genauso wichtig wie „Outside Protection" bei einem Deal.

## Cyber-Schutzmaßnahmen nach dem Closing

Die klassischen Due Diligences wie Vendor und Purchaser Due Diligences, werden vor dem Closing durchgeführt. Darüber hinaus sind nach dem Closing – wenn der Käufer erstmals vollen Zugang zu allen Ressourcen hat – weitere Prüfungen durchzuführen, nun durch direkten Zugriff im realen Objekt. Für eine solche Untersuchung hat sich der Begriff „Post Closing Due Diligen-

ce“ eingeprägt, die der neue Eigentümer macht. Im Zuge eines Cyber-Risiko-Assessments können nun diejenigen Aktivitäten nachgeholt werden, die sich vor dem Closing rechtlich verbieten. So können sogenannte „White hat hatches“ angeheuert werden, mit der Aufgabe, Netzwerke und Produkte zu „hacken“ und „spots“ zu entdecken, an denen Angreifer in das unternehmensinterne Netz eindringen können. Über die unmittelbar daraus abzuleitenden Maßnahmen hinaus sollten danach – insbesondere bei IT-getriebenen Geschäften – kontinuierlich durchzuführende Aktivitäten zur Entwicklung und Installation neuer und immer sicherer Software eingerichtet werden. Nota bene: Der technologische Wettlauf mit den Angreifern geht immer weiter…

## Notoperationen vornehmen

Wann auch immer vor, während oder nach M&A können Notmaßnahmen erforderlich werden. Darauf sollte man sich grundsätzlich einstellen und Notfallpläne und Ressourcen für „Feuerwehreinsätze“ vorhalten. Sensoriken in der Technik und Aufmerksamkeit der Mitarbeiter sind entscheidend. Das Erkennen früher Signale ermöglicht schnelle Aktionen. Geschwindigkeit im Handeln rettet Daten und verhindert die Ausbreitung der Schäden. Im Extremfall kann es sinnvoll sein, Teile des Firmennetzes oder das ganze Unternehmen vom Internet temporär abzukoppeln. Der damit zweifellos entstehende Schaden durch das Abschalten von Prozessen, sogar in der Fertigung, kann wesentlich größere Schäden durch externe Angriffe vermeiden. Die Analogie zu großen Waldbränden bietet sich an: Schneisen schlagen, damit die Brände nicht überspringen. Mit einem großen Unterschied: Bei IT kann es sich um Millisekunden handeln.

## Sichere Strukturen präventiv aufbauen

Präventiv sollen Strukturen mit intern trennenden Firewalls geschaffen werden, sodass Bereiche notfalls separiert werden können. Hochsicherheitsbereiche sind zu identifizieren und entsprechend auszustatten. Die Anzahl der Zugänge vom Internet in das interne Unternehmensnetz sind zahlenmäßig möglichst gering zu halten und gut kontrollierbar zu gestalten. Angriffe über die Unternehmensperipherie sind beliebt, weil meist weniger geschützt. Hier bietet sich eine Reihe von Möglichkeiten zum Schutz an, sie etwa außerhalb einer Firmen-Firewall anzusiedeln, die Datenzugänge zu regeln und automatisiert zu sichern, etwa über limitierte Datenraten, Filter und Sicherheits-Scans.

## Sicherheit kostet Zeit

Zeitdruck und Hektik im M&A-Prozess generieren besondere Cyber-Risiken. Deshalb kann es nötig werden, die Geschwindigkeiten einzelner M&A-Prozesse temporär herabzufahren, eventuell sogar ein „Time-out“ zu vereinbaren, um Sicherheitslücken zu schließen. Das Ziel muss dabei sein, das Target auf ein höheres Sicherheitsniveau zu bringen. Projekterfahrungen zeigen, dass dies durchaus auch über ein halbes Jahr laufen kann, bis die entsprechenden Maßnahmen in der IT, personell und in der Organisation etabliert und geprüft sind. Auch dies muss für große und professionell zu führende M&A-Projekte als Möglichkeit vorgesehen werden.

Für den immer zeitkritischen Ablauf eines M&A-Projektes heißt dies, dass derartige „Schleifen“ oder „Auskopplungen“ so zu gestalten sind, dass nicht das Gesamtprojekt behindert oder gefährdet wird. Auch hierzu bieten sich Lösungen an, beispielsweise über Sonderverträge, die das Nachlaufen von bestimmten Aktivitäten erlauben, etwa über das Closing hinaus. Das kann dazu führen, dass IT-Security-Sonderteams geschaffen werden, in denen Mitarbeiter (als Delegates) beim Target verbleiben, bis das Problem gelöst ist. Die Kosten dafür können geteilt oder verrechnet werden. Höhere Sicherheit kostet gut investiertes Geld. Beschleunigungen machen solche Prozesse noch teurer.

## Die Cyber-Risiken bei M&A gehen über die Projektlaufzeit hinaus

Beobachtungen von Angriffen haben ergeben, dass professionelle Hacker systematisch Schwachpunkte beim (schwächeren) Target suchen, sich dort also einnisten. Sie schlagen erst dann los, wenn die Integration formell abgeschlossen ist. Dann hoffen sie, dass die IT-Systeme noch nicht harmonisiert sind und sie so durch die schwächeren Sicherungsfenster des bisherigen Targets in das neue integrierte Unternehmen eindringen können. Sie treffen dann die (bisher besser geschützte) IT des wertvolleren und damit zahlungskräftigeren Übernehmers. Der Schaden kann dort viel größer sein, und die Forderung bemisst sich nach der Schadenhöhe, die das angegriffene Unternehmen durch „Lösegeldzahlung“ vermeiden kann. Somit kann der späte Angriff viel lukrativer sein als der frühere.

## Cyber-Schwachstellenanalysen zum M&A-Prozess empfehlen sich

Nachfolgend einige Orientierungspunkte für Schwachstellenanalysen, aus denen dann Abhilfe- und Abwehrmaßnahmen zu entwickeln sind:

**(a) Prozessorientiert**

- Instabilitäten im Vorfeld: Informations-Lecks, Spionage, Brüche von Geheimvereinbarungen, Fakes als Ergebnisse aus Kandidaten-Screenings.
- Risiken nach dem Signing: Eindringlinge in Datenräume, Störungen und Defizite bei der Due Diligence
- Brüche im Prozess: Stabübergaben, etwa am „Day One“ nach dem Closing
- Datenreste und Spuren nach dem formalen Projektabschluss

**(b) Mitarbeiterorientiert**

- Wer sind die Verlierer? Wer bangt um seinen Job?
- Wer ist frustriert?
- Geringes Engagement: nur temporäres Interesse, Absprungwillige
- Spionage im Auftrag Externer

**(c) Stakeholder-betrieben**
- Wettbewerber greifen über Cyber an
- Kunden der beiden M&A-Parteien starten Gegenoffensiven
- Spionage von verschiedensten Seiten
- Gesteuerte (Fake-) Nachrichten
- Nachrichtendienste, „Beifang" über M&A im Zuge breiterer Ermittlungen
- Gezielte Insider-Informationen an Wettbewerber
- Gezielte Schädigung der Wirtschaft durch konkurrierende Länder

**(d) Infrastrukturorientiert**
- IT-Arbeitsplätze
- Software
- Netz-Infrastruktur, Sicherheitsnetz: Verbindungspunkte nach außen
- Dezentrale Angriffe: multi-regional, Standorte, Landesgesellschaften

## Ratschläge an Unternehmer

Trotz der Vielfalt an Einfallstoren, der zahlreichen Angriffspfade und -technologien kann sich ein Unternehmer, der sich auf einen M&A-Fall vorbereitet – sei es als Käufer oder Verkäufer – einige wenige und einprägsame Regeln zu eigen machen:

**Regel 1: Sichern Sie Ihr Investment**
Der Wert des bei zur Disposition stehenden Unternehmens(-teils) kann durch Cyber-Angriffe schnell zunichte gemacht werden. Der Deal kann damit platzen. Dieses Risikobewusstsein sollte Sie zum Nachdenken führen, wo in Ihrem speziellen Fall die Angriffsrisiken liegen. Systematische Analysen, unter Einbezug interner und externer Fachleute können Schaden abwenden.

**Regel 2: Cyber-Sicherheit bei M&A ist gut investiertes Geld**
Glauben Sie nicht an das Märchen, dass Cyber-Abwehr bei M&A unverhältnismäßig teuer und der Einsatz von Fachleuten unklar und unüberschaubar sind – nur weil der sogenannte „Sense of urgency" in der Breite der Unternehmen noch nicht angekommen ist. Die nach Cyber-Risiken fachlich gut geführten Projekte haben gezeigt, dass der „Return on security" günstig ist und dass sich zahlreiche Methoden anbieten, aus denen ein Erfahrungsträger in diesem Geschäft das speziell für Ihren Fall passende und wirtschaftlich adäquate Leistungsmodell herausarbeiten kann. Cyber Security Managementbei M&A muss nicht teuer sein. Es muss so kompetent sein, dass es den Kompetenzen der Angreifer überlegen ist. Fehlende Kompetenzen sind von außen einzukaufen.

**Regel 3: Ein guter Feldherr sieht vor der Schlacht in alle Richtungen**
Ein M&A-Projekt läuft in der heißen Phase wie eine Schlacht ab. Ein guter Feldherr hat vorgesorgt, alle Angriffspunkte von außen und von innen lokalisiert und gesichert. Das muss vor dem M&A-Projekt erfolgt sein, während der Schlacht ist es zu spät. Ein für Cyber-Risiken gut aufgestelltes Unternehmen hat vor M&A zunächst einmal für größtmögliche Sicherheit im Vorfeld von M&A gesorgt, der „Stand-alone"-Position, so etwa auch nach dem Carve-Out einer zur Disposition stehenden Unternehmenseinheit, die im Niveau ihrer Sicherheitsaufstellung nicht gegenüber der (hoffentlich vorbildlichen) Aufstellung der Muttergesellschaft abfallen sollte.

**Regel 4: Halten Sie die Verteidigungsmauern hoch**
Angreifer loten Ihre IT nach Alter der Komponenten und den damit verbundenen (meist von den Anbietern publizierten) Schwachstellen aus. Sie wissen von den Lücken, die bei der Zusammenführung von Systemen entstehen. Sorgen Sie dafür, dass bereits vor der Fusion die Systeme beider Seiten dem jüngsten Sicherheitsstandard entsprechen.

**Regel 5: Klären Sie das spezifische Cyber-Risiko-Profil Ihres M&A-Falles und handeln Sie entsprechend**
Die Risikoprofile laufen nach den klassischen Dimensionen: Branche – Wertschöpfungsstufe – Regionalität: Was ist Ihnen bekannt? Was ist neu? Was ist denkbar? Je unterschiedlicher die M&A-Kandidaten, desto höher die Risiken. Diese sind zu lokalisieren und vertiefend zu analysieren. Dementsprechend sind im Projekt adäquate Kapazitäten und Kompetenzen bereit zu stellen.

**Regel 6: Aufmerksamkeitsdefizite nicht zulassen – schnell agieren**
Gehen Sie davon aus, dass die Angreifer systematisch die Schwachpunkte in einem M&A-Fall analysieren. Sie nutzen dazu öffentliche Daten, Firmeninformationen und Verlautbarungen über den M&A-Prozess. Setzen Sie eine spezielle Cyber Security Task Force für Ihr M&A-Projekt auf – bestehend aus Fachleuten beider Seiten (etwa nach dem bekannten Modell eines „Clean Teams") unter Einbezug externer Kompetenzträger auf Feldern, die Ihnen fehlen.

Eine grundlegende Darstellung über Cyber Security Management in Konzernen, speziell über Angriffs- und Verteidigungs-Technologien, Strategien und den Verteidigungspakt „Charter of Trust" findet sich im Buch des Autors Kai Lucks: „Der Wettlauf um die Digitalisierung – Potenziale und Hürden in Industrie, Gesellschaft und Verwaltung" , erschienen im Schaeffer-Poeschel-Verlag 2020.

**Prof. Dr. Kai Lucks**

Kai Lucks ist Gründer und Vorsitzender des Bundesverbandes Mergers & Acquistions. Er hat 35 Jahre bei Siemens und seinen Joint Ventures im Medizin- und Energiebereich gearbeitet und zeichnete in der Zentrale für die Strategieprojekte, Kooperationen und M&A verantwortlich.

Foto: Privat

# Wer zahlt, verliert – Was man über Ransomware wissen muss, um keine falschen Entscheidungen zu treffen

**Frank Kölmel**
Cybereason

Ransomware hält die digitale Welt auf Trab. Mit einem Abflauen der Angriffsdichte ist in der kommenden Zeit nicht zu rechnen. Denn Ransomware Angriffe sind relativ leicht durchführbar und immer noch sehr erfolgversprechend für die Angreifer. Was muss man also wissen, um im Falle eines Falles einen kühlen Kopf zu bewahren und richtig zu reagieren und im besten Fall schon vor dem Worst-Case richtig geschützt zu sein?

Zahlen oder nicht zahlen – das ist hier nicht die Frage. Zumindest nicht für Cybersecurity-Experten. In der Hoffnung, schnell die Business-Continuity wiederherstellen zu können, scheinen aber immer noch viele Unternehmen sehr schnell auf digitale Lösegeldforderungen einzugehen. Würden die meisten Unternehmen nicht zahlen, würden die USA beispielsweise nicht überlegen, die Zahlung solcher Forderungen unter Strafe zu stellen. Die Stoßrichtung ist bei dieser Überlegung der US-Regierung aber auf alle Fälle die richtige. Denn der Erfolg solcher Zahlungen ist nicht garantiert und viel schlimmer: Mit dem Geld könnten terroristische Aktivitäten unterstützt und nationalstaatliche Hackergruppen finanziert werden. Damit nimmt eine erfolgreiche Ransomware-Attacke ganz neue Dimensionen an und in einem Schneeball-Effekt können Cyber-Angreifer so immer schneller und immer effizienter Geld erbeuten.

## „Zu klein, um Opfer zu werden" gibt es nicht

Natürlich stellt sich die Frage, wie wichtig staatlich unterstützte Hackergruppen im Alltag von Unternehmen sind. Aber selbst, wenn ein privates Unternehmen „nur" Opfer „normaler" Hacker wird, unterstützen Lösegeldzahlungen auch hier weitere kriminelle Aktivitäten. So ebnet ein erfolgreicher Angriff zumindest den Weg für die nächsten Attacken auf andere Opfer. Und Hackergruppen, die Nationalstaaten nahestehen, sind öfter aktiv, als man eventuell annehmen möchte. Denn jedes Unternehmen bietet ihnen ein mögliches Ziel. Die Aussage „Mein Unternehmen ist zu klein, um von diesen Akteuren angegriffen zu werden", ist reine Augenwischerei. Im simpelsten Fall ist ein kleines Unternehmen, das gegebenenfalls auch nur über eine schlechte Cyberabwehr verfügt, ein Ziel, das schnell und unkompliziert Geld bringt. Im schlimmsten Fall sind aber auch kleinere Unternehmen ein wichtiger Schritt auf dem Weg zu den ganz großen Fischen. Sobald ein Unternehmen Schnittstellen, Kontaktpunkte oder Daten zu anderen Unternehmen hat, die näher an den eigentlichen Zielen liegen, werden sie für Cyber-Kriminelle interessant. Denn ein Dienstleister des eigentlichen Ziels könnte den Angreifern genug Informationen und Daten liefern, damit diese eine täuschend echt aussehende Rechnung mit einem schadhaften Link erstellen können, um so in das System des Zielunternehmens zu kommen. Und auch wenn solch eine Verbindung eventuell nur über viele Ecken besteht, bedeutet das nicht, dass die Hacker diesen Weg nicht gehen werden. Ist das Ziel nur wichtig genug, sind Angreifer bereit viel Zeit und Ressourcen zu investieren, um dorthin zu gelangen.

## Eine neue Qualität von Angriffen

Vor allem staatlich unterstützte Angreifergruppen haben oft sehr spezifische Opfer im Blick und sind bereit, viel Aufwand in Kauf zu nehmen, um in deren Netzwerke zu gelangen. Um

das zu schaffen, setzen Sie oft neue Maßstäbe, was die Qualität von Angriffen betrifft. Ein Bedrohungsakteur, der dies erst kürzlich beeindruckend gezeigt hat, ist MalKamak. Diese Hacker-Gruppe hebt die Verschleierung ihrer Aktivitäten im Opfernetzwerk auf ein neues Level. Während die Angriffe dieser Hacker vor allem auf kritische Infrastrukturen im Nahen Osten abzielt, sind ihre Aktivitäten letztendlich für uns alle relevant. Denn hier zeichnen wichtige Trends und Entwicklungen ab. Frei nach dem Motto: „Was bei den großen Angreifern funktioniert, klappt wahrscheinlich auch in der Masse!“

Digitale Angriffe werden dabei immer zugespitzter und die Angreifer immer geschickter, wenn es darum geht, Cybersecurity zu umgehen. MalKamak nutzt beispielsweise Dropbox (eine oftmals als sicher eingestufte Anwendung), um nicht ins Netz der Verteidiger zu gehen. MalKamak ist zwar vor allem auf Cyber-Spionage aus – aber ihre Herangehensweisen und Taktiken sind sehr effizient und könnten sich schon bald in der Masse der Ransomware-Angriffe niederschlagen. Daher müssen sich quasi alle Unternehmen fragen, ob sie nicht schon längst Opfer geworden sind, ohne es mitzubekommen. In Zukunft wird es daher auch immer wichtiger, jede einzelne Netzwerkaktivitäten zu überprüfen und sie in korellation mit anderen Netzwerkereignissen zu stellen. Denn einzeln betrachtet wirkt so manche Aktivität in der digitalen Umgebung eines Unternehmens harmlos – ganzheitlich betrachtet erkannt man vielleicht aber doch, dass sie Teil eines Angriffs ist und sich nur gut tarnt. Was müssen Entscheider also wissen, um sich mit dem Thema Ransomware informiert auseinandersetzen zu können?

## Erfolgsgeschichte Ransomware

Die Zahl der Ransomware-Angriffe steigt stetig. Nicht zuletzt ist das Erfolgsmodell „RaaS“, also Ransomware as a Service, dafür verantwortlich. Das Software Engineering Institute (SEI) der Carnegie Mellon University definiert RaaS als „ein neues Geschäftsmodell für Ransomware-Entwickler. [Diese Akteure] verkaufen oder vermieten ihre Ransomware an Partner, die sie dann zur Umsetzung eines Angriffs verwenden.“ In diesem Geschäftsmodell können die Entwickler die Höhe des Lösegelds festlegen, die Verhandlungen mit den Opfern koordinieren und dann einen Teil des Lösegelds für ihre Dienste einbehalten. Die Partner erhalten den Rest für ihren Beitrag zur Durchführung des Angriffs, so Bleeping Computer.

Dabei darf RaaS nicht unterschätzt werden. Die Angriffe sind keine harmlosen Spielereien von Hobby-Kriminellen. Teilweise steht hinter den RaaS-Anbietern ein Team aus fähigen Hackern, welche die Schadsoftware schreiben. Und auch der Service-Gedanke kommt bei ihnen nicht zu kurz. So können „Kunden“ Tutorials zur Schadsoftware bekommen, und manche stellen sogar einen Kundenservice wie herkömmliche SaaS-Anbieter bereit. Damit wird die Anzahl ausgeklügelter Ransomware-Attacken in der nahen Zukunft nur noch weiter steigen. Zu glauben, man könne selbst kein Opfer werden, ist also eher Wunschdenken als Realität.

## Die Kosten steigen

Die Angriffe werden nicht nur mehr, sie werden für die Opfer auch immer kostspieliger. Die REvil Forderung an Acer über 50 Millionen US-Dollar ist eine der bislang höchsten digitalen Lösegeldforderungen, die uns bekannt sind. In der Höhe sind sie bislang ein starker Ausreißer – aber gleichzeitig auch Teil des Trends zu immer höheren Forderungen.

Zusätzlich zu dem Lösegeld bringt eine erfolgreiche Ransomware-Attacke aber auch noch weitere Kosten mit sich, die Unternehmen nicht unterschätzen sollten. In einer Studie zu den tatsächlichen Kosten von Ransomware haben uns über die Hälfte der befragten Unternehmen in Deutschland (51 Prozent) geantwortet, dass die Marke und der Firmen-Ruf nach einer erfolgreichen Attacke Schaden genommen haben. Da verwundert es auch nicht, dass sogar 75 Prozent der Befragten signifikante Umsatzeinbußen hinnehmen mussten. Dies kann sogar so weit führen, dass aufgrund einer erfolgreichen Attacke Mitarbeiter entlassen werden müssen. In Deutschland war dies bei immerhin 19 Prozent der befragten Unternehmen der Fall – mehr als genug, um die Gefahren und Kosten abseits der Lösegeldforderungen ernst zu nehmen. Dieser Fakten sollten sich alle Entscheider bewusst sein, wenn sie sich für oder gegen einen besseren Ransomware-Schutz entscheiden.

## Allzweckwaffe Backup?

Die Datensicherung galt lange Zeit als probates Mittel gegen Cyber-Erpresser. Und tatsächlich hilft ein Backup immer noch dabei, wichtige Daten nicht zu verlieren, sollte man doch Opfer einer Ransomware Attacke werden. Natürlich ist es aufwendig, das Backup wieder einzuspielen – aber dies ist allemal die bessere Option als die Daten zu verlieren. Dessen sind sich auch die Kriminellen bewusst und haben Mittel und Wege gesucht, um auch diese Form der Abwehr zu umgehen.

Zum einen hilft es den Erpressern, länger unentdeckt im Netzwerk zu sein. Hier spielt natürlich die kriminelle Innovationskraft zur Verschleierung der eigenen Taten, wie wir sie bei MalKamak sehen, eine wichtige Rolle. Denn je länger die Malware im System ist, desto älter muss auch das Backup sein und desto mehr Daten gehen beim Zurücksetzen auf einen alten Stand des Systems verloren. Viel wichtiger ist aber die sogenannte „Double Extortion“. Denn wie oben beschrieben, ist neben dem Datenverlust auch der Vertrauensverlust eine ernstzunehmende Gefahr für Unternehmen. Jener wiegt umso schwerer, wenn plötzlich die verschlüsselten Daten im Netz auftauchen. Aus diesem Grund exfiltrieren viele Ransomware-Angreifer die Daten, die sie verschlüsseln vorher und bedrohen das Opfer mit der Veröffentlichung dieser Daten. Egal ob es sich also um Daten aus der Produktentwicklung oder Kundendaten handelt, möchte das Opfer diese nicht in der Öffentlichkeit sehen. So ist das Backup zwar immer noch eine gute Möglichkeit, um dem Verlust der Daten vorzubeugen. Als Waffe im Kampf gegen Ransomware ist die Datensicherung allein aber schon lange ein stumpfes Schwert.

## Bloß nicht zahlen

In der Hoffnung, dass die Angreifer die Daten schnell wieder entschlüsseln und nicht ins Netz stellen, könnten Unternehmen in Versuchung gebracht sein, das Lösegeld schnellstmöglich zu zahlen. Aber am anderen Ende der Forderung stehen immer noch kriminelle Erpresser. Damit ist die Zahlung kein Garant dafür, dass dies auch so geschieht. Ein aktueller Bericht zeigt, dass

sich 2020 56 Prozent der Ransomware-Opfer für die Zahlung entschieden haben. Aber ganze 17 Prozent der Unternehmen, die das Lösegeld beglichen haben, erhielten ihre Daten trotzdem nicht zurück. Ein Spiel mit dem Feuer, bedenkt man, wie die Forderungen steigen. Dabei ist die erfolglose Entschlüsselung teilweise keine böse Absicht. Manche Erpresser haben schlicht nicht die Fähigkeit (oder das Interesse) einen voll funktionsfähigen Entschlüsselungscode zu schreiben.

Aber die relativ unsichere Aussicht auf Erfolg ist nicht der einzige Grund, warum es sich für Unternehmen nicht lohnt zu zahlen. Oft ist die Zahlung nämlich nur der Anfang einer Reihe weiterer Angriffe. Denn für die Angreifer sind zahlungswillige Opfer ein gefundenes Fressen. Ganz nach dem Mott „Wer einmal zahlt, tut es auch wieder“. Die Zahlen sind hier eindeutig: 80 Prozent der Unternehmen, die Lösegeld bezahlt haben, wurden Ziel erneuter Erpressungen. Dabei müssen es nicht einmal immer dieselben Angreifer sein. Die Information darüber, ob ein Opfer schnell bereit ist zu zahlen und damit ein gutes Ziel darstellt, lässt sich auch gut an andere Kriminelle weiterverkaufen.

## Proaktiv gegen Ransomware

Angriff ist die beste Verteidigung. Das gilt vor allem bei der Abwehr von Ransomware-Angriffen. Wer den Angreifern also nicht immer nur hinterherrennt, sondern ihnen proaktiv das Leben schwer macht, wird auch auf lange Sicht gegen sie bestehen. In diesem Katz-und-Maus Spiel immer einen Schritt voraus zu sein wirkt wie eine unlösbare Aufgabe. Schließlich können die Kriminellen immer neue Maschen ersinnen, welche die Verteidiger auf dem falschen Fuß erwischen. Aus diesem Grund sollten Unternehemen auf Lösungen wie XDR (Extended Detection and Response) setzen, welche keine starren Parameter zum Erkennen von Angreifern benötigen, sondern Angriffe auch dann erkennen, wenn diese auf ganz neuen Ideen basieren. Mit der Hilfe von Behavioral Analytics und künstlicher Intelligenz erkennt XDR nämlich auch sicherheitsrelevante Zwischenfälle, die bisher unbekannt sind. Um das zu schaffen, nutzt XDR die Analyse von Ereignis-Telemetrie in Systemen, die über Endpunkte wie Laptops und mobile Geräte hinausgehen und auch Cloud-basierte Ressourcen, Benutzeridentitäten, Netzwerk-Tools und andere Teile der IT-Infrastruktur einschließen. So erfasst die XDR-Plattform alle Ereignisse im Netzwerk und bringt diese in Verbindung miteinander. Verdächtige Aktivitäten werden so schnell und präzise erkannt und Angreifer können gestoppt werden, bevor sie Schaden anrichten.

## Den Kriminellen einen Schritt voraus

Was bedeutet das alles aber für den Umgang mit erfolgreichen Ransomware-Angriffen und den Schutz vor eben jenen? Sollte es zum schlimmsten Fall gekommen sein und die Hacker haben wichtige Daten verschlüsselt, heißt es: Ruhe bewahren! Überstürzte Zahlungen helfen nur den Kriminellen. Jedes Opfer einer Ransomware-Attacke muss sich bewusst machen, dass die tatsächlichen Kosten am Ende viel höher ausfallen und die Zahlung des Lösegelds keine Garantie dafür ist, schnell und umfänglich alle Daten wiederzuerlangen. Zusätzlich offenbart man sich als zahlungswilliges Opfer, das auch in Zukunft wahrscheinlich ein lohnendes Ziel darstellt. Ist das Kind erst in den Brunnen gefallen, ist der meiste Schaden schon angerichtet. Hier hilft nur noch, sich die Fähigkeiten von Profis an Bord zu holen und Schadensbegrenzung zu betreiben, die nicht den Kriminellen Geld in die Kassen spült. Je weniger Geld bei den Angreifern ankommt, desto unattraktiver wird diese Angriffsart in Zukunft sein. Wer nicht zahlt, hilft also auch der gesamten digitalen Gesellschaft, indem der Geldhahn für die Hacker zugedreht wird.

Um es gar nicht so weit kommen zu lassen stellen, wie dargelegt, moderne XDR-Lösungen mit Behavioral Analytics und künstlicher Intelligenz ein wichtiges Werkzeug dar, um den Angreifern proaktiv begegnen zu können. Wichtig für das Verständnis zum Schutz vor Ransomware ist, dass es nicht darauf ankommt möglichst viel und starke künstliche Intelligenz einzusetzen. Dies wäre eventuell die sprichwörtliche Kanone, mit der man auf Spatzen schießt. Beim Schutz vor Ransomware sollte also das Zeitfenster zwischen dem ersten Eindringen eines Angreifers in das Netzwerk und dem Zeitpunkt, zu dem Verteidiger in der Lage sind, den Angriff zu erkennen zu und darauf zu reagieren, minimiert werden. Es kommt also nicht auf die Menge der KI an, sondern auf deren optimalen Einsatz, um dieses Ziel zu erreichen. Dabei lohnt sich die Auseinandersetzung mit diesen Lösungen gleich doppelt: Denn die optimierte Bedrohungsanalyse und -abwehr mit modernem XDR bietet nicht nur den so dringend benötigten Schutz, sondern entlastet auch das Security-Personal. Je genauer und übersichtlicher ein Alarm ist, desto einfacher können die Experten mit diesem umgehen und die nötigen Gegenmaßnahmen einleiten.

Letztendlich sind Verständnis und Abwehr von Ransomware-Angriffen kein Hexenwerk. Wichtig ist, dass darüber gesprochen wird und ein Austausch stattfindet. Zu einem guten Teil werden Angreifer mit dieser Masche wohl immer noch Erfolg haben, weil manche Unternehmen die Summe aus Scham zahlen – in der Hoffnung, dass der erfolgreiche Angriff nicht bekannt wird. Das gießt aber Öl ins Feuer der Ransomware-Plage. Gemeinsam können wir es aber schaffen, dass immer mehr digitale Lösegeldforderungen erfolglos bleiben. Dann verlieren die Kriminellen mit der Zeit auch ihre Lust an dieser Angriffsform.

**Frank Kölmel**

Frank Kölmel bringt über 25 Jahre Branchenexpertise mit und war zuletzt bei Palo Alto Networks beschäftigt. Zuvor führte Frank Kölmel die Geschäfte von FireEye in Mittel- und Osteuropa. In diesem Zusammenhang hatte er das Managed Security Services -Angebot von FireEye in Deutschland ins Leben gerufen.

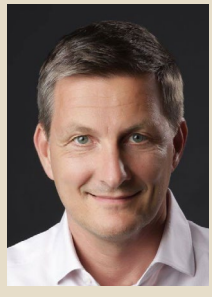


Foto: Privat

# 1.1 RANSOMWARE

## Ransomware automatisch abwehren

Die Anzahl der weltweiten Ransomware-Angriffe ist im vergangenen Jahr enorm gestiegen und obwohl sich das Prinzip der Erpressung dahinter nicht verändert, so werden die Methoden doch raffinierter. Die wichtige Frage von Unternehmen lautet daher: Wie gehen wir am besten mit Lösegeldforderungen um und wie können wir sogar verhindern, dass sie unser Unternehmen treffen?

Um eine Lösung zum Stoppen von Ransomware-Angriffen zu finden, gilt es zunächst deren Methoden zu verstehen, mit denen sie sich Zugang zu den Systemen eines Unternehmens verschaffen. Die beliebtesten Angriffswege folgen hier:

- **Phishing-E-Mails** – Der Angreifer versucht den Benutzer zu verleiten, einem Link zu folgen oder einen infizierten Anhang zu öffnen.
- **Remote-Desktop-Protokoll** – Unternehmen nutzen das Protokoll, damit die IT-Abteilung die Rechner der Mitarbeiter aus der Ferne warten kann, was einen Port öffnet – darauf spekulieren Kriminelle. Es ist eine der sehr häufig ausgenutzten Schwachstellen.
- **Drive-By-Downloads von kompromittierten Websites** – Ein Benutzer besucht unbewusst eine infizierte Webseite von der sich selbstständig eine Malware herunterlädt – meist sogar, ohne die Aufmerksamkeit des Nutzers zu erregen.
- **USB-Sticks und andere Wechseldatenträger** – Über diese Speichergeräte können Viren ebenfalls in Firmennetzwerke gelangen, wenn ein Anwender sie unbedarft in den Anschluß steckt. Häufig passiert dies mit zufällig gefunden Geräten, auf deren Inhalt die Person neugierig ist. Zufällig aber lagen diese Speichergeräte nicht herum – sie wurden von Verbrechern platziert.

**Best-Practice der Sicherheitsprinzipien**

Der Kampf gegen Ransomware erfordert eine umfassende Sicherheitsstrategie – es gibt keine bestimmte Lösung, die man von der Stange kauft und alle Sorgen sind vorbei. Stattdessen muss eine echte Defense-in-Depth-Methodik angewandt werden. Die komplette Strategie dagegen auf nur ein Standbein zu stellen, birgt ein großes Risiko. Die Best-Practice besteht dagegen daraus, ein Netz von Produkten zu spinnen, die zusammenwirken. Diese können dann automatisierte Aufklärung und schnelle Reaktion auf alles bieten, was sich in den Firmennetzwerken abspielt. Unternehmen benötigen daher eine Kombination aus Endpoint Detection & Response (EDR), Intrusion Detection und/oder Prevention Systemen (IDS/IPS), Security Information and Event Management (SIEM), Security Orchestration, Auromation and Response (SOAR) und einer zentralen Konsole, die all diese Komponenten automatisch steuert und Ereignisse auf einer Oberfläche vereint anzeigt – so erhalten die Fachkräfte auch die Sichtbarkeit des Datenflusses, die sie dringend benötigen. Jede Komponente spielt hierbei eine einzigartige Rolle und hilft IT-Sicherheitsingenieuren, die richtige Wahl zur richtigen Zeit aufgrund der richtigen und aller Informationen zu treffen. So kann beispielsweise die Besatzung eines Security Operations Center (SOC) wirklich gezielt reagieren.

Wen mehrere Lösungen zum Zug kommen, hat das zudem den Vorteil, dass das Netzwerk aus unterschiedlichen Blickwinkeln erfasst wird und so größeres Vertrauen in die Unversehrtheit der eigenen Infrastruktur gelegt werden kann. Außerdem lassen sich die Daten besser kontrollieren und bei Beschädigungen ist schnelles Handeln möglich. Wer auf diese verschiedene Blickwinkel verzichtet, der betrachtet im Grunde genommen nur die Vordertür seines Hauses und ist in dem Glauben, dass dies der einzige Weg sei, wie jemand in das Haus gelangen könnte. Er fühlt sich sicher, doch vergisst dieser jemand die Fenster und die Hintertür. Ein Fehler, der für Unternehmen ebenso schwerwiegende Folgen hätte.

Neben den genannten Sicherheitslösungen müssen auch klassische Firewalls gegen die Bedrohung durch Ransomware angepasst werden. Dabei kommt es besonders auf die Grundlagen an.

**Aufbau einer Verteidigungsmauer**

Firewalls sind so konzipiert, dass sie den gesamten Datenverkehr blockieren, mit Ausnahme dessen, was durch die Sicherheitsrichtlinien ausdrücklich erlaubt wurde. Aber mit der Zeit werden diese Kataloge aufgebläht, da sich über Jahre hinweg Änderungen ergeben und oft veraltete Regeln dort ansammeln. Daher lauten die Empfehlungen für Firewalls:

- **Das Durcheinander von Regeln entfernen** – Im Laufe der Zeit hat eine Firewall wahrscheinlich zahlreiche Administratoren hinter sich und jeder hat die Geräte anders verwaltet. Von Benennungen der Objekte hin zum einfachen Hinzufügen von Regeln am unteren Ende der Firewall-Regelbasis. Doppelte Objekte müssten außerdem beseitigt werden und unbenutzte Regeln entfernt, um die Übersicht zu wahren. Zudem benötigen diese Richtlinien allesamt einen nachvollziehbaren Pfad zur Prüfung. Transparenz und Kontrollinstanzen sind entscheiden für den Erfolg. Eine Nachlässigkeit hier aber kann alles durcheinander bringen.
- **Regeln laufend validieren** – Obwohl bestimmte Regeln zu einem bestimmten Zeitpunkt ein sinnvoller Zusatz zu Katalog einer Firewall waren, bedeutet

Hier geht es zu weiteren Blogbeiträgen

**Tim Bloomer, Sales Engineer, AlgoSec**

das nicht, dass sie Jahre später noch über eine Daseinsberechtigung verfügen. Firewall-Pflege benötigt daher ein automatisiertes Verfahren, mit dem sich die eigene Regelbasis laufend neu zertifizieren lässt, als ob es sich um eine weitere Änderungsanfrage handeln würde. Auf diese Weise wird verhindert, dass Administratoren ständig Änderungen bearbeiten müssen und die gesamte Regelbasis neu zertifizieren. Wenn das in einem fortlaufenden Prozess geschieht, bleibt alles sortiert und es wird sichergestellt, dass ein Unternehmen die Erwartungen seiner Kunden erfüllt oder übertrifft.

- **Entfernen von überflüssigen Objekten** – Oft wird eine Änderungsanforderung zu jeder Firewall innerhalb des Datenstroms hinzugefügt wird, weil der Administrator nicht die Zeit hatte genauer vorzugehen. Hier kommt erneut eine Security-Automatisierung ins Spiel, um diesen Prozess korrekt durchzuführen. Wenn Daten angefordert werden, dann bedeutet das nicht, dass jede Firewall im Netzwerk die Ausnahmeregel beinhalten muss – die Daten kommen möglicherweise gar nicht bei ihr vorbei. Eine automatisierte Richtlinienverwaltung wird daher die Anfrage für jede Firewall auswerten und sicherstellen, dass den Firewalls keine überflüssigen Objekte hinzugefügt werden.
- **Einrichtung eines Änderungsverfahrens für Policies** – Gutes Firewall-Management benötigt ein durchdachtes Änderungsverfahren, welches eine vollständige Dokumentation aller Änderungen für das Auditing und zur Einhaltung der Compliance erstellt. Es gibt an, was zu welchem Zeitpunkt und warum geändert wurde.

Ransomware-Angriffe stellen ein besonders gefährliches Problem dar, wenn ein abtrünniger Mitarbeiter (Insider) daran beteiligt ist. Die oft zitierte Mikro-Segmentierung für das Netzwerk hilft auch hier. Ihre Einführung ist unerlässlich geworden – und durch Security-Automatisierung endlich in angemessener Zeit und mit angemessenen Kosten zu schaffen. Diese Maßnahme schränkt jeden Angreifer in seiner Bewegungsmöglichkeit innerhalb des Systems stark ein. So bleibt der Schaden im Falle einer erfolgreichen Attacke in klar abgesteckten Grenzen stecken.

**Absicherung endet nie**

Die vorgestellten Methoden, um sich gegen Ransomware-Angriffe besser zu schützen, stellen lediglich den Kern, nicht aber das gesamte Spektrum von Möglichkeiten zur Absicherung dar. Die sich stetig entwickelnde IT-Technologie und die ebenso fortschreitende Angriffsmethode der Angreifer erfordern gemeinsam von IT-Sicherheitsgruppen, stets auf der Hut zu sein und die eigene Verteidigung anzupassen. Die jüngste Notwendigkeit, um Schritt halten zu können, ist die Automatisierung alltäglicher und zu umfangreicher Prozesse. Das schaufelt den Fachkräften auch Zeit frei für große Projekte und entlastet sie, angesichts des Fachkräftemangels und vieler Überstunden. Einmal eingerichtet, können alle Beteiligten eines Unternehmens ruhiger an ihre Arbeit gehen – trotz ständiger Meldungen über erfolgreiche Ransomware-Attacken in den Nachrichten.

Tim Bloomer

## Ransomware: Zahlen oder nicht zahlen, das ist die Frage

Wenige Gedanken über die IT-Sicherheit lassen Führungskräfte in Unternehmen wohl so wenig in Ruhe schlafen, wie die Überlegung, was bei einem erfolgreichen Ransomware-Angriff zu tun ist. Dabei gilt: Je besser eine Firma vorbereitet ist, desto besonnener können alle handeln.

Die durchschnittliche wöchentliche Anzahl von Ransomware-Angriffen in den letzten 12 Monaten stieg weltweit um 93 Prozent. Mittlerweile werden jede Woche über 1200 Organisationen das Opfer einer Attacke. Nach Daten von Cybersecurity Ventures wird der durch Ransomware verursachte Schaden in diesem Jahr etwa 20 Milliarden US-Dollar (rund 17 Milliarden Euro) erreichen, was einer 57-fachen Steigerung gegenüber dem Jahr 2015 entspricht. Bis 2031 könnten die Kosten von Ransomware-Zwischenfällen sogar die schier unglaubliche Zahl von 265 Milliarden US-Dollar (rund 222 Milliarden Euro) übersteigen.

Warum die Zahl der Ransomware-Angriffe so stark steigt? Das lässt sich einfach erklären: Die Hacker werden für ihren Erfolg bezahlt. Es handelt sich um einen Teufelskreis: Gehen die Unternehmen auf die Erpressung ein und zahlen das Lösegeld, freuen sich die Angreifer und sämtliche Trittbrettfahrer. Das ruft förmlich zu weiteren Versuchen auf und viele Unternehmen erfüllen die Forderungen der Kriminellen ohne langes Zögern, weil sie auf Cyber-Risiko-Versicherungen zurückgreifen, was Hacker wiederum wissen.

**Ransomware zur Miete**

Die Zunahme der Angriffe hängt auch mit der Verfügbarkeit von Malware zusammen. Viele Hacker-Gruppen bieten Ransomware-as-a-Service (RaaS) an: Jeder kann diese Art von Bedrohung in entsprechenden Foren und Läden im Dark Net mieten, einschließlich Infrastruktur, Kompetenz zur Verhandlung mit den Opfern und Erpresser-Websites, auf denen gestohlene Informationen veröffentlicht werden können, um im Rahmen einer Doppelten oder Dreifachen Erpressung den Druck zu erhöhen. Das Lösegeld wird danach zwischen den Vertragspartnern aufgeteilt.

Doch ein Ransomware-Angriff beginnt oft nicht mit Ransomware. Häufig startet der Überfall mit einer schlichten Phishing-E-Mail, die schädliche Anhänge

enthält. Darüber hinaus arbeiten Hacker mit Betreibern von Bot-Netzen zusammen: Während der Ryuk-Ransomware-Angriffe wurde die Emotet-Malware als Türöffner und Lieferant der Ransomware verwendet. Sie infizierte das Netzwerk, schleuste danach Trickbot als weiteren multifunktionalen Trojaner ein, und dieser wiederrum öffnete das Tor für Ryuk, welche schließlich die Daten verschlüsselte.

**Dem Einbruch besonnen begegnen**

Cyber-Kriminelle haben keine Pausen. Sie verfeinern ständig ihre Technik, um die Entdeckung ihrer Malware zu erschweren und den Zahlungsdruck zu erhöhen. Ursprünglich verschlüsselte Ransomware lediglich Daten und forderte ein Lösegeld, um sie zu entsperren. Vor rund zwei Jahren fügten die Angreifer eine zweite Phase hinzu und stahlen vor der Verschlüsselung wertvolle Informationen. Sie drohten damit, diese bei einer ausbleibenden Zahlung des Lösegelds zu veröffentlichen – die Masche der Doppelten Erpressung war erfunden. Etwa 40 Prozent aller neuen Ransomware-Familien gehen nun so vor. Darüber hinaus wurde kürzlich eine dritte Phase beobachtet, in der auch die eigentlichen Opfer des Datendiebstahls, nämlich Geschäftspartner, Kunden, Patienten oder Journalisten kontaktiert werden, weil sensible Informationen über sie ebenfalls in den gestohlenen Datenpaketen enthalten waren – die Dreifache Erpressung. All das dient zur Steigerung des Lösegelds und der Wahrscheinlichkeit, dass irgendein Opfer bezahlen wird und damit weiter die Taschen der Verbrecher füllt.

Das Check Point Software Incident Response Team hat weltweit unzählige Ransomware-Fälle für Unternehmen bearbeitet. Es empfiehlt daher die Einhaltung der folgenden Schritte, wenn es zu einem Ransomware-Angriff kommt:

1) Einen kühlen Kopf bewahren

Im Fall einer geglückten Ransomware-Attacke ist es in erster Linie wichtig, nicht in Panik zu geraten. Die IT-Sicherheitsabteilung sollte umgehend verständigt werden. Eine Kopie der Lösegeldforderung ist hilfreich, denn sie wird für die Strafverfolgung und weitere Ermittlungen nützlich sein.

2) Computer isolieren

Infizierte Systeme müssen sofort vom Rest des Netzwerks getrennt werden, um weiteren Schaden zu verhindern und die willkürliche Bewegung durch das Netzwerk zu unterbinden. Gleichzeitig sollte die Quelle der Infektion identifiziert werden. Ein Ransomware-Angriff beginnt in der Regel durch eine andere Bedrohung. Die Hacker waren möglicherweise schon lange im System ansässig und haben nach und nach ihre Spuren verwischt, sodass die Erkennung des Auslösers für die meisten Unternehmen oft nicht ohne spezialisierte Hilfe zu bewältigen ist.

3) Backups im Blick behalten

Angreifer wissen, dass Unternehmen eine Wiederherstellung ihrer Daten aus Backups versuchen werden, um die Zahlung des Lösegelds zu vermeiden. Deshalb versuchen jene oft die Backups zu finden, um diese zu verschlüsseln oder zu löschen. Es sollten außerdem niemals externe Geräte und Wechseldatenträger, wie USB-Sticks, an infizierte Geräte angeschlossen werden, sonst werden diese zu verseuchten Überträgern. Vorsicht ist auch beim Wiederherstellen verschlüsselter Daten geboten, denn es kann beispielsweise durch einen fehlerhaften Schlüssel zu Beschädigungen der Ursprungsdaten kommen. Daher kann es sinnvoll sein, Kopien der verschlüsselten Daten zu erstellen. Außerdem werden nach und nach Entschlüsselungsprogramme entwickelt, die helfen können, bisher unbekannten Code zu knacken. Falls unverschlüsselte Backups vorliegen, sollte trotzdem vor einer vollständigen Wiederherstellung deren Integrität geprüft werden.

4) Auf Reboots und Systemwartung verzichten

Auf infizierten Systemen sollten automatische Updates und andere Wartungsaufgaben deaktiviert werden. Das Löschen temporärer Dateien oder andere Änderungen könnten Untersuchungen und Gegenmaßnahmen unnötig erschweren. Gleichzeitig sollten die Systeme nicht neu gestartet werden, da einige IT-Bedrohungen dann mit dem Löschen von Dateien beginnen.

5) Zusammenarbeiten mit den Polizeibehörden

Im Kampf gegen Cyber-Kriminalität und insbesondere gegen Ransomware ist die Zusammenarbeit mit den Strafverfolgungsbehörden der Schlüssel zum Erfolg. Unternehmenn sollten sich also frühzeitig mit der Polizei und dem nationalen Cyber-Abwehrzentrum in Verbindung setzen – Kritis-Betreiber sind ohnehin bei Strafe verpflichtet, dies umgehend und vollumfänglich zu tun. Zudem sollte auch das spezielle Incident-Response-Team einer vertrauenswürdigen IT-Sicherheitsfirma kontaktiert und die Mitarbeiter informiert werden. Eine Schulung der Angestellten, woran sie Ransomware und sonstige IT-Gefahren erkennen können, hilft außerdem sehr dabei, künftige Attacken abzuwehren.

6) Die Art des Ransomware-Angriffs identifizieren

Wenn die Nachricht der Angreifer nicht beschreibt, um welche Art von Ransomware es sich handelt, dann kann ein kostenloses Programm zur Identifikation benutzt werden. Auf der Website des Projekts No More Ransom findet sich häufig sogar ein Entschlüsselungsprogramm gegen die Ransomware.

7) Infektionskette durchspielen und Sicherheitslücken schließen

Unabhängig davon, ob es menschliche Faktoren waren oder die Technologie, die versagt haben, Unternehmen

**Christine Schönig, Regional Director Security Engineering CER, Office of the CTO, Check Point Software Technologies GmbH**

sollten alle Prozesse noch einmal durchgehen und ihre gesamte IT-Strategie überdenken. So stellen sie sicher, dass ein ähnlicher Vorfall nie wieder passiert – sonst kann der Ransomware-Angriff zu einer Wiederholungstat führen. Außerdem: Wenn eine Datenwiederherstellung stattgefunden hat, sollte man keineswegs den Vorfall einfach als gelöst betrachten, denn die Sicherheitslücke wurde nicht beseitig.

**Best practices um Attacken zu vermeiden**

Es ist gut, wenn man weiß, welche Maßnahmen ergriffen werden müssen, um mit einer erfolgreich verlaufenen Ransomware-Attacke am besten umzugehen, doch noch besser ist es, wenn alles Mögliche getan wurde, um den Angriff zu verhindern:

1. An Wochenenden und Feiertagen besonders aufmerksam sein. Die meisten Ransomware-Angriffe im vergangenen Jahr 2020 fanden an Wochenenden oder Feiertagen statt. An diesen Tagen reagieren Unternehmen langsamer auf eine Bedrohung, weil nur eine Notbesetzung die Absicherung übernimmt.
2. Updates und Patches regelmäßig installieren. WannaCry traf im Mai 2017 Organisationen auf der ganzen Welt schwer und infizierte über 200 000 Computer in drei Tagen. Ein Patch für die ausgenutzte EternalBlue-Schwachstelle war jedoch bereits einen Monat vor dem Angriff verfügbar.
3. Anti-Ransomware-Sicherheitslösung installieren. Ein Anti-Ransomware-Schutz beobachtet ungewöhnliche Aktivitäten, beispielsweise das Öffnen und Verschlüsseln einer großen Anzahl von Dateien. Wenn Anti-Ransomware-Schutz ein verdächtiges Verhalten feststellt, kann sofort reagiert werden, um grobe Schäden zu verhindern.
4. Essentielle Schulungen implementieren. Viele Attacken beginnen mit einer gezielten Phishing-E-Mail, die keine Malware enthält, sondern mithilfe von Social Engineering versucht, den Benutzer zum Klicken auf einen manipulierten Link zu verleiten. Die Aufklärung der Benutzer ist daher einer der wichtigsten Bestandteile des Schutzes gegen Ransomware-Angriffe.
5. Ransomware-Angriffe beginnen nicht mit Ransomware, daher sollte Schadsoftware im Allgemeinen im Blick behalten werden. Bot-Netze wie Trickbot und Dridex (und ehemals Emotet als größter Vertreter) infiltrieren Organisationen und schaffen die Voraussetzungen für einen anschließenden Ransomware-Angriff.
6. Backups und Archivieren von Daten sind unerlässlich. Wenn etwas schief geht, sollten Daten einfach und schnell wiederherstellbar sein. Es ist wichtig, konsequent Backups zu erstellen, auch auf den Geräten der Mitarbeiter. Führungskräfte müssen sich dabei entweder darauf verlassen können, dass die Angestellten selbst daran denken, das Backup einzuschalten, oder sollten es automatisiert laufen lassen.
7. Zugriff nur auf notwendige Informationen und Segmente des Netzwerks beschränken. Wenn die Auswirkung eines erfolgreichen Angriffs minimiert werden soll, dann ist es wichtig, dass Benutzer nur auf die Dateien, Programme und Bereiche des Netzwerks zugreifen können, die sie unbedingt für ihre Arbeit benötigen, während alles andere unsichtbar bleibt – dies ist das Konzept von Zero Trust, also „Kein Vertrauen“. Zusätzlich senkt eine Mikro-Segmentierung des Netzwerks das Risiko einer unkontrollierten Verbreitung von Ransomware im Netzwerk, weil letzteres in kleine Teile getrennt wird, an deren Grenzen der Datenverkehr scharf bewacht wird.

**Jede Zahlung motiviert die Hacker**

Sollen Führungskräfte die Lösegeldforderung nun bezahlen? Die Antwort ist nicht so einfach, wie oft dargestellt. Zwar liegen die Beträge manchmal im Bereich von Hunderttausenden oder Millionen von Euro, doch können Kosten durch Ausfälle kritischer Systeme diese Beträge schnell übersteigen. Es ist jedoch zu bedenken, dass sogar eine Zahlung nicht zwangsweise bedeutet, dass die Daten oder auch nur ein Teil davon entschlüsselt werden – man begibt sich in die Hand der Erpresser. Es sind Fälle bekannt, wobei Angreifer Fehler in die Kodierung geschmuggelt haben, sodass sie selbst die Daten nicht wiederherstellen konnten – geschweige denn die Unternehmer.

Freilich müssen die Führungskräfte an die Arbeitsplätze und die Produktion denken, doch andererseits motiviert jede Zahlung die Hacker zu weiteren Attacken und lockt Trittbrettfahrer an, was wiederum die Ransomware-Welle anwachsen lässt. Diese Zwickmühle lässt sich am besten vermeiden, wenn ein Unternehmen sich auf die Abwehr der Ransomware, sowie den Umgang mit einem erfolgten Angriff, bestmöglich vorbereitet.

Christine Schönig

## Schützen Sie Ihre Daten vor Ransomware-Angriffen

Ransomware-Angriffe nehmen rasant zu und stellen eine große Bedrohung sowohl für KMUs als auch für größere Unternehmen dar. Welche enormen Gefahren von Ransomware-Angriffen ausgehen, wurde einer breiten Öffentlichkeit erstmals im Jahr 2017 bewusst. Damals verbreitete eine unbekannte Hackergruppe ein Schadprogramm, das als „WannaCry“ bekannt wurde. Das Schadprogramm pflanzte sich unter Ausnutzung einer Schwachstelle des Betriebssystems Windows über das Internet auf zahlreiche Rechner fort. Innerhalb von Stunden infizierte WannaCry über 230.000 Computer in der ganzen Welt und legte zahlreiche Unternehmen und Einrichtungen lahm. Dabei verursachte die

Ransomware etwa vier Milliarden Euro an Schaden [1]. In Deutschland wurde u. a. die Deutsche Bahn in Mitleidenschaft gezogen. Zahlreiche Anzeigetafeln und Fahrkartenautomaten auf etlichen Bahnhöfen zeigten die typische Lösegeldforderung an.

Mittlerweile beherrschen Schlagzeilen über Erpressungsvorfälle unseren Alltag. Vor allem während des Höhepunkts der Corona-Krise im Juni 2020 ist die Zahl der Ransomware-Vorfälle laut einer Studie von Skybox Security [2] nochmal deutlich gestiegen.

**25 Tipps zum Schutz vor Ransomware**

Der Schutz digitaler Informationen, also die IT-Sicherheit, ist wichtiger denn je. Sie gilt als eine der größten Herausforderungen für das 21. Jahrhundert. Ransomware-Angriffe können für Unternehmen verheerende finanzielle Folgen haben und den Ruf eines Unternehmens enorm schädigen.

Im Folgenden werden vorhandene Möglichkeiten erklärt, wie sich Unternehmen, aber auch Privatpersonen gegen Ransomware schützen können:

**Sichere Nutzung von E-Mail**

- Blockieren Sie ausführbare Dateien in E-Mails: Die meisten Ransomware-Varianten verbreiten sich über E-Mail-Anhänge. Dabei kann es sich zum Beispiel um vermeintlich harmlose Word-Dateien handeln. Gelegentlich werden Schadprogramme jedoch auch als ausführbare Dateien verschickt, die über Dateiendungen wie .bat, .cab, .cmd, .exe, .js, .vbs zu erkennen sind. Konfigurieren Sie Ihren Mailserver so, dass derartige Anhänge blockiert werden. Es gibt keinen vertretbaren Grund, ausführbare Dateien per E-Mail zu versenden. Besonders Dateien mit doppelten Dateierweiterungen wie beispielsweise Rechnung.txt.vbs sollten abgelehnt werden. Nichts spricht für den Erhalt oder die Verwendung solcher Dateien.
- Vorsicht bei Anhängen und Links: Klicken Sie niemals auf Links/Anhänge in E-Mails. Außer Sie sind sich nach eingehender Kontrolle wirklich sicher, dass der Link/Anhang sicher ist. Empfehlenswert ist eine Dienstanweisung, Links/E-Mail-Anhänge erst nach Rücksprache mit dem Absender bzw. nach Vorankündigung zu öffnen. Es reicht nicht, dass man den Absender kennt. Ist der Rechner des Absenders mit einem Schadprogramm infiziert, so könnte eine Mail vom Schadprogramm im Namen des Absenders mit einer schon benutzten Betreff-Zeile verschickt worden sein.
- Geben Sie Ihre E-Mail-Adresse nicht arglos auf irgendwelchen Webseiten an. Seien Sie skeptisch, wenn die Mailadresse verlangt wird.
- Nutzen Sie auf Ihrem Mailserver Anti-Spoofing-Technologien wie Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC) und DomainKeys Identified Mail (DKIM).

**Allgemeine Schutzmaßnahmen**

- Zum Schutz der Verfügbarkeit und der Integrität wichtiger Daten sollten regelmäßig Datensicherungen erstellt werden. Bei einer Ransomware-Infektion besteht ein hohes Risiko für Datenverluste, da die Gefahr besteht, dass die vom Trojaner verschlüsselten Dateien nicht wiederhergestellt werden können.
- Deaktivieren Sie nach Möglichkeit Makros in Office-Dateien. Makros sind kleine Unterprogramme, mit denen sie in den großen Office-Paketen vollständige Programme entwickeln können (z. B. eine automatisierte Lagerverwaltung). Das Problem: Makro-Programm haben genug Rechte, um Schadsoftware einzuschleusen. Viele bekannte Erpressungstrojaner haben so bereits den Weg in Unternehmen, Schulen, Universitäten, Krankenhäusern und sonstigen Einrichtungen gefunden.
- Aktualisieren bzw. patchen Sie Ihre Software regelmäßig: Nicht gepatchte Programme werden von Hackern häufig für Cyberangriffe genutzt. So hatte sich WannaCry, eine der größten Ransomware-Wellen überhaupt, über die Sicherheitslücke namens „Eternal Blue“ verbreitet - einen Monat, nachdem diese Lücke gepatcht worden war. Ohne dieses fahrlässig langsame Patch-Management hätte man den Schaden deutlich reduzieren können. Trend Micro Research fand in einer aktuellen Studie [3] heraus, dass es im Durchschnitt beinahe 51 Tage dauert, bis ein Unternehmen neue Schwachstellen patcht.
- Einige Angreifer nutzen .VBS-Dateien (VBScript), um Erpressersoftware zu installieren. Deaktivieren Sie die COM-basierte Laufzeitumgebung „Windows Script Host“, wenn Sie dieses Feature nicht benötigen.
- Wenn Sie PowerShell nicht nutzen, deaktivieren Sie es. Windows PowerShell ist ein Framework zur Aufgabenautomatisierung. Es besteht aus einem Kommandozeileninterpreter und einer Skriptsprache. Kriminelle nutzen PowerShell häufig, um Ransomware aus dem Speicher auszuführen und so die Erkennung durch Antivirenlösungen zu umgehen.
- Eine gewisse Gefahr geht von aktiven Inhalten aus, da diese client-seitig im Browser auf dem Rechner des Benutzers ausgeführt werden. Dies gilt besonders für die Verwendung von Java aber in geringerem Umfang auch für die Script-Sprache JavaScript. Man hat zwar versucht, durch die Eigenschaften der Sprachen Sicherheitsgefahren auszuschließen, aber zum einen ist dies nicht vollständig möglich, zum anderen werden gelegentlich auch Fehler bei der Implementierung der Sprachen gefunden, die Sicherheitslöcher bieten. Man sollte daher die Ausführung von JavaScript und Java deaktivieren und diese nur bei Bedarf auf vertrauenswürdigen

**René Hifinger, Software-Entwicklung, Selbständiger Einzelunternehmer**

Internetseiten vorübergehend aktivieren.
- Deaktivieren Sie ungenutzte Funkverbindungen. Immer wieder werden z. B. kritische Sicherheitslücken in Bluetooth-Anwendungen entdeckt.
- Deaktivieren Sie das Windows-Remote Desktop Protocol (RDP) zum Schutz vor RDP-Exploits. Ransomware-Varianten wie beispielsweise Cryptolocker/Filecoder nutzen RDP als Einfallstor [4].
- Lassen Sie im Windows-Explorer alle Dateierweiterungen anzeigen. Jede Datei, die eine doppelte Dateierweiterung wie beispielsweise „foto.jpg.exe“ enthält, sollte als verdächtig betrachtet werden.
- Verwenden Sie eine moderne Antivirus-Software.
- Arbeiten Sie nicht mit Administrator-Rechten. Denn einmal mit Admin-Rechten gestartet, können Schadprogramme sofort die Systemkontrolle übernehmen.
- Nutzen Sie sichere Passwörter: Egal ob es der Zugang zum Betriebssystem, zu einem Anwendungsprogramm, zu einer Web–GUI oder dem E–Mail–Client ist, überall legitimiert man sich mit einem Passwort. Ein gutes Passwort:
- ist mindestens 10 Zeichen lang. Je länger das Passwort desto besser.
- beinhaltet Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
- ist in keinem Wörterbuch zu finden.
- enthält keine alphabetischen Buchstabenfolgen / einprägsamen Tastaturpfade.
- basiert nicht auf persönliche Daten.
- ist für jedes Konto einzigartig. Das Gleiche gilt auch für die benutzten Benutzernamen / E-Mail-Adressen. Mit der Verwendung unterschiedlicher Benutzernamen / E-Mail-Adressen steigt die Sicherheit der einzelnen Konten deutlich. Ein Angreifer weiß nie genau, welcher Benutzername bzw. welche E-Mail-Adresse bei der einzelnen Anmeldung verwendet wurde. Tipp: Nutzen Sie „catch all“ E-Mail-Adressen. Mit einem Catch-All-E-Mail-Account werden alle E-Mails, die an Ihre Domain gesendet werden an Ihr Postfach weitergeleitet – egal was vor dem @-Zeichen steht. Dadurch können Sie beliebig viele Aliase dynamisch nutzen. Bei Anbieter A registrieren Sie sich dann z.B. mit anbieter-a-49385@meinedomain.de, bei Anbieter B mit anbieter-b-38274@meinedomain.de.
- Wenn möglich, sichern Sie all Ihre Zugänge mit der sogenannten Zwei-Faktor-Authentifizierung (2FA) ab.
- Speichern Sie sensible und vertrauliche Daten unbedingt verschlüsselt.
- „AutoRun“ ist eine Windows-Funktion, mit der Benutzer Wechseldatenträger wie USB-Sticks und CDs sofort ausführen können. Malware-Autoren können diese Funktion nutzen, um Ransomware zu verbreiten. Sie sollten diese Funktion auf allen Arbeitsstationen deaktivieren.

**Maßnahmen auf Netzwerkebene**
- Unterteilen Sie Computernetzwerke in kleinere, separate Subnetzwerke, um die Verbreitung von Ransomware einzugrenzen. Vor allem Industrieanlagen und IoT-Geräte sollten in einzelne Bereiche unterteilt bzw. segmentiert werden.
- Ein wichtiges Werkzeug zur Hacker-Abwehr sind Firewalls. Eine Firewall gehört selbst in kleineren Unternehmen zum unverzichtbaren Standard, wenn es um eine Anbindung an das Internet geht.
- Cyberkriminelle nutzen immer öfter das TOR-Netzwerk für die Command and Control (C&C)-Kommunikation, wodurch sich ist das Aufspüren der C&C-Infrastruktur als deutlich schwerer erweist. Blockieren Sie bekannte IP-Adressen von Entry- und Exit-Nodes sowie Tor-Bridges. Blockieren Sie außerdem Anwendungen, die sich mit .onion-Domänen verbinden möchten.

**Organisatorische Maßnahmen**
- Schulungsmaßnahmen: Eine wichtige Grundvoraussetzung für den Schutz des eigenen Systems und der Arbeit mit dem System besteht darin, dass ein Benutzer ein allgemeines Verständnis für die dabei vorhandenen Sicherheitsprobleme entwickelt. Er soll Sicherheit nicht als Hemmschuh verstehen, sondern als Bestandteil seiner Arbeit, der ihn und die beteiligten Komponenten schützt. Regelmäßige Schulungsmaßnahmen zum Thema IT-Sicherheit helfen den Mitarbeitern, am Ball zu bleiben.
- Berechtigungsmanagement: Wenn es um den geschützten Zugang zu Computer-Systemen geht, ist ein gutes Berechtigungsmanagements-Konzept das A und O: Kommt ein Mitarbeiter neu ins Unternehmen, dann muss er in allen möglichen Systemen registriert und mit geeigneten Rechten ausgestattet werden. Diese Rechte können sich ändern und erfordern somit einen ständigen Managementprozess. Beim Verlassen stehen entsprechend viele Sperrungen an. Falsche Rechtevergabe und verspätetes Sperren steigern das IT-Risiko enorm. Es gilt die gesamte Berechtigungsstruktur im Auge zu behalten.
- IT-Notfallpläne: Unternehmen müssen bereits vor dem Eintritt von IT-Notfällen planen, wie sie mit solchen Situationen umgehen (Verantwortlichkeiten, Maßnahmenlisten…). Dadurch lassen sich Ausfallzeiten verkürzen und Schäden minimieren.

In der Praxis finden sich leider mehr als genug Unternehmen/Benutzer, die lediglich eine Antivirus-Software und eine Firewall nutzen und glauben, adäquat geschützt zu sein. Manche der in diesem Artikel beschriebenen Schutzmaßnahmen mögen einem möglicherweise etwas lästig oder unnötig erscheinen, aber mit einer Antivirus-Software und einer Firewall allein ist dem Schutz vor Ransomware definitiv nicht genüge

getan! Das Problem dabei ist, dass man vom Gegenteil möglicherweise erst überzeugt wird, wenn schon ein Schaden eingetreten ist.

René Hifinger

Quellen und Referenzen: **[1]** https://t3n.de/news/ransomware-reloaded-wannacry-1240246/ **[2]** https://www.skyboxsecurity.com/trends-report/ **[3]** https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/trends-and-shifts-in-the-underground-n-day-exploit-market **[4]** https://www.zdnet.de/88382240/ransomware-attackiert-vpn-und-rdp/

# 1.2 SOCIAL ENGENEERING

## Sicherheit in der flexiblen Arbeitswelt

Das Arbeiten von zuhause ist für viele Mitarbeiter nicht mehr wegzudenken. Auch die Arbeitgeber verstehen nach der Bewährungsprobe in der Corona-Pandemie, dass die Produktivität ihrer Mitarbeiter im Homeoffice nicht nachlässt – sie sind sogar noch produktiver als im traditionellen Büro. Daher können Unternehmen guten Gewissens Remote Work weiterhin in ihre Arbeitsweise integrieren und auf eine flexible Arbeitsweise umstellen, um den Mitarbeitern einen Mix aus Homeoffice und Büro zu bieten. Doch dies stellt sogar IT-Experten vor neue Herausforderungen in Sachen Sicherheit.

Die Anzahl an Bedrohungen durch Cyberattacken jeglicher Art haben in den letzten Jahren rapide zugenommen – von Phishing, Ransomware und DDoS-Angriffen bis hin zu Social Engineering. Laut IDG bestätigen 66 Prozent der Befragten IT-Manager, dass die Mitarbeiter im Homeoffice mehr Cyber-Risiken ausgesetzt sind. Auch die Anzahl der Mitarbeiter, die auf privaten, ungeschützten Geräten arbeiten (31 Prozent), ist unter dieser Prämisse erschreckend hoch. So hat auch der IT-Helpdesk alle Hände voll zu tun, um immer mehr Probleme der Remote Worker zu betreuen und sie vor Cyberbedrohungen zu schützen. Doch gilt es hierbei, die Maßnahmen so nutzerfreundlich und sicher wie möglich zu halten. Mitarbeiter sollten nicht zu stark durch das neue „Work-from-Anywhere“ und zu viele Arbeitsschritte eingeschränkt sein.

**Starkes Bewusstsein für IT-Sicherheit schaffen**

Alle Mitarbeiter – egal, ob remote, im Büro oder im Co-Working Space – müssen für Cyberbedrohungen sensibilisiert sein. Die IT-Verantwortlichen sollten sie darüber aufklären, wie böswillige Hacker agieren, welche Einfallstore sie ihnen allein durch die Wahl ihrer Passwörter liefern und welche Schritte und Tools sie zur Bekämpfung einsetzen können. Dabei gilt es, nicht nur Schulungen für die Mitarbeiter durchzuführen, sondern dem Thema IT-Sicherheit auch einen festen Platz in der Unternehmenskultur einzuräumen. Nur so entsteht eine übergeordnete Sicherheitskultur im Unternehmen und die Mitarbeiter verstehen den Wert von IT-Sicherheit, wenn dieser auch explizit gelebt wird. Dadurch nehmen sich auch die Mitarbeiter des Themas Security an und verhalten sich während der gesamten Arbeitszeit vorsichtig. Das minimiert das Risiko des Faktors Mensch als Sicherheitslücke.

**Solides Passwort-Management als Grundstein**

Im Durchschnitt besitzt jeder Mensch 30 Accounts, die es durch Passwörter zu schützen gilt. Egal ob von zuhause, im Büro oder irgendwo sonst auf der Welt: Ein starkes Passwort-Management ist unerlässlich. Allerdings verwenden Mitarbeiter ein Passwort im Schnitt 13-mal. Vor allem kleinere Unternehmen haben damit zu kämpfen. Das hat eine aktuelle Studie des Passwortmanagers LastPass zum Gebrauch von Passwörtern am Arbeitsplatz ergeben. Dadurch stellen diese Log-in-Daten noch immer das größte Sicherheitsrisiko in Unternehmen dar.

Bedenkt man, dass Datenverstöße in der digitalen Welt an der Tagesordnung stehen und sich nachweislich 80 Prozent der Datenschutzverletzungen auf schwache und mehrfach verwendete Passwörter zurückführen lassen, sollten Mitarbeiter immer wieder über Passworthygiene informiert werden.

Dennoch nutzen viele Anwender oft dieselben, unsicheren Passwörter über verschiedene Accounts hinweg. Zu den Favoriten zählen leider noch immer Zahlenfolgen wie „123456“ oder nebeneinanderliegende Tastenkombinationen wie „qwertz“. Auch Kombinationen mit Zahlen aus dem Geburtsdatum sind keine gute Idee. Mit einer Business-Passwort-Manager-Lösung erlangen Unternehmen mehr Kontrolle über das Passwort-Verhalten ihrer Mitarbeiter. So können IT-Verantwortliche und Nutzer Verstöße rechtzeitig abwenden und den Aufwand für die Verwaltung so gering wie möglich halten. Passwort-Manager verwalten alle Passwörter, die Nutzer individuell für die unterschiedlichsten Accounts aufsetzen, in einem sicheren Tresor. Dieser ist nur über ein starkes Master-Passwort des Users erreichbar. Die Mitarbeiter müssen sich also nur ein Passwort merken. Das vermeidet unsichere, einfache Passwörter und die mehrfache Verwendung desselben Passworts in unterschiedlichen Accounts.

**Single-Sign-On und Multifaktor-Authentifizierung als zusätzliches Security Layer**

Der Vorteil solcher Passwortmanager: Sie bieten zusätzliche Funktionen, wie beispielsweise Single-Sign-On (SSO) oder Multi-Faktor-Authentifizierung (MFA). Mit SSO können IT-Verantwortliche den Aufwand für die Passwortverwaltung verringern, indem sie die Anzahl der zu verwaltenden Passwörter erheblich reduzieren. Auf diese Weise verbinden sich

**Dan de Michele, Vice President Product LastPass, Logmein**

die Nutzer sicher mit den Anwendungen, ohne dass sie extra ein weiteres Passwort eingeben müssen. Unternehmen können so die vollständige Kontrolle sowohl über die Passwörter als auch den Benutzerzugriff erlangen, sofern die Accounts über SSO mit einem Passwortmanager verbunden sind. Dadurch erhalten die Log-ins eine zusätzliche Sicherheitsstufe.

MFA bietet darüber hinaus noch eine weitere Sicherheitsebene. Beim Einloggen müssen die Nutzer neben dem Passwort auch einen weiteren Code eingeben. Dieser wird in dem Moment des Einloggens kreiert und an ein anderes Gerät des Nutzers geschickt. Eine Variante dieses Verfahrens nutzt biometrische Sensoren für einen Fingerabdruck oder eine Gesichtserkennung. Nur mit dieser zweiten Sicherheitsebene lässt sich der Anmeldevorgang durch eine MFA abschließen. Solche Verfahren sind sehr vorteilhaft für IT-Admins, denn sie müssen sich keine Sorgen mehr um unsichere Passwörter ihrer Kollegen machen, um die Unternehmensnetzwerke zu sichern. Die gesamte Belegschaft ist geschützt, aber kann gleichzeitig ohne große Leistungseinbußen oder komplexe Sicherheitsprozesse sowohl im Büro als auch aus der Ferne arbeiten.

Auch der Netzwerkzugriff muss abgesichert sein

Zum Arbeiten aus der Ferne gehört in den meisten Fällen auch eine VPN-Verbindung, denn die einfache Nutzung mit einem einzigen Zugangspunkt und einer sicheren Datenübertragung ist sehr intuitiv. Laut der Umfrage von IDG gibt fast die Hälfte der IT-Verantwortlichen (45 Prozent) zu, dass die Mitarbeiter auf ungesicherte WLAN-Netze zugreifen. Dies liegt an einer nur geringfügigen Absicherung der VPN-Verbindung. Auch diese sollten IT-Administratoren zusätzlich absichern.

Jedoch sorgen genau die intuitiven, einfachen Eigenschaften von VPN für eine hohe Anfälligkeit gegenüber Cyber-Angriffen. Bereits ein Satz gestohlener Log-in-Daten oder ein durch Malware kompromittierter Computer reichen aus, um Hackern Zugriff auf sensible Unternehmensdaten zu gewähren. Im schlimmsten Fall können sie diese verschlüsseln und Lösegeld fordern. Um dies zu verhindern, benötigt die VPN-Verbindung ein zusätzliches Security-Layer. Auch hier kommt wieder MFA zur doppelten Absicherung ins Spiel. So vermeiden Unternehmen, dass sich unberechtigte Personen Zugang zum Netzwerk verschaffen – ohne zusätzliche, komplexe Anmeldeprozesse für die Mitarbeiter.

**Der Weg zur sicheren flexiblen Arbeitswelt**

Remote Work hat nach der Pandemie seinen festen Platz im Arbeitsleben gefunden und wird langfristig seinen Stellenwert behalten. Die IT muss sich daher auf eine flexiblen IT-Umgebung anpassen, um die dadurch steigenden Cyber-Risiken im Griff zu behalten. Die richtigen Tools und Features unterstützen sie dabei, das Angriffsrisiko zu minimieren, während die Mitarbeiter ohne große Einschränkungen produktiv und sicher von jedem Ort der Welt arbeiten können. Unternehmen sollten die risikoreichere Bedrohungslandschaft aus dem Homeoffice ernst nehmen und auf die richtigen Lösungen setzen, um für eine sichere flexible Belegschaft gewappnet zu sein.

Dan de Michele

**Dr. Torben Gülstorff,
Freier Journalist,
Redaktionsbüro
Dr. Torben Gülstorff**

## IT-Sicherheit richtig kommunizieren – Ansatzpunkt Unternehmensreputation

Im eigenen Unternehmen Verständnis und Bewusstsein für IT-Sicherheit zu erzeugen ist schwierig. Vor allem dann, wenn das obere Management nicht hinter einem steht. Dort ist man sich des vollen Schadenspotentials eines Cyberangriffs häufig gar nicht bewusst. IT-Sicherheitsabteilungen können hier gegensteuern, indem sie ein zentrales Asset in die Kommunikation mit ihren Geschäftsführungen einführen: die Unternehmensreputation.

Ende 2013, zu Beginn des gerade einsetzenden Weihnachtsgeschäfts, kam es bei einem der größten US-amerikanischen Einzelhändler, der Target Corporation, zur einer für damalige Verhältnisse gewaltigen Sicherheitspanne. Cyberkriminelle hatten sich über Phishing-Angriffe auf den Target-Zulieferer Fazio Mechanical Zugangsdaten zum Target-Netzwerk verschafft und dort die Malware Kaptoxa in Point Of Sale-Systemen installiert. Diese lieferte ihnen Kredit- und Bankkarten-Daten von mehr als 40 Millionen Target-Kunden sowie mehr als 70 Millionen Adress-Daten. Allein bis 2016 sollten sich die direkten Folgeschäden dieses Angriffs auf umgerechnet rund 285 Millionen Euro belaufen.

Nicht zuletzt die Reputation des Unternehmens wurde durch den Angriff nachhaltig in Mitleidenschaft gezogen. Eine rasante Talfahrt des Yougov Buzz-Scores – der Konsumentenbewertung – des Unternehmens setzte ein. In den ersten Tagen nach dem Zwischenfall fiel der Wert von 22,4 auf -19 Punkte. Zwar konnte das Unternehmen ihn in den folgenden Monaten etwas stabilisieren und anheben, doch hatte er auch 2019, mit 18,5 Punkten, noch immer nicht seinen Vorangriffswert erreicht. In Folge des Reputationsverlustes wechselten zahlreiche Kunden zu Konkurrenzunternehmen. Umsatz und Gewinn brachen ein. Im vierten Quartal 2013 schrumpfte der Profit um 50 Prozent. Für das gesamte Geschäftsjahr 2013 musste die Gewinnprognose um ein Drittel nach unten korrigiert werden.

**Schadenspotential von Cyberangriffen wird nach wie vor unterschätzt**

Das Beispiel Target zeigt: Erfolgreiche Cyberangriffe schädigen Unternehmen nicht nur direkt – durch Ausfall oder Einschränkungen der IT-Infrastruktur, durch

Datenverluste, durch Zahlungen von Lösegeld, von Strafen und Schadensersatzansprüchen – sondern auch indirekt – durch nachhaltigen Verlust an Reputation. Letzteres ist meist mit erheblichen Komplikationen für die Geschäftsbeziehungen verbunden – nicht nur in Hinblick auf die Kunden, sondern auch auf Partner, Zulieferer und Aktionäre. Als Hacker beispielsweise 2018 eine Sicherheitslücke von Facebook nutzten, um Konten von 50 Millionen Nutzern der Social Media-Plattform zu kompromittieren, fiel der Aktienkurs des Unternehmens in wenigen Tagen um drei Prozent. Die Target Corporation hatte 2013 sogar einen Einbruch von 10 Prozent zu verkraften. Zwar fängt sich der Aktienkurs nach einem Cyberangriff im Regelfall auch wieder, kurz- und mittelfristig können solche Werteinbrüche Unternehmen aber doch in erhebliche finanzielle Schwierigkeiten bringen.

**Reputation als Gesprächsansatz für mehr Cybersicherheit**

Und dennoch: In der internen Kommunikation zur und der Handhabung der Cybersicherheit vieler Unternehmen bleiben die möglichen Folgen eines erfolgreichen Cyberangriffs für die Reputation meist ausgeklammert. Jelle Wieringa, Security Awareness Advocate bei KnowBe4 sieht das Problem wie folgt: „Berichtet die IT-Sicherheitsabteilung von Cyberangriffen, konzentriert sie sich im Regelfall auf deren direktes Schadenspotential. Die Geschäftsführung, in deren Aufgabenbereich die Sicherstellung der Reputation für gewöhnlich fällt, ordnet die Relevanz der IT-Sicherheit dann falsch ein, verkennt das volle Risiko.“ Die Folge: eine unnötige Schwächung der IT-Sicherheit. Nach Meinung von Wieringa muss die oberste Managementebene voll hinter der IT-Sicherheitsabteilung stehen, wenn Investitionen in Sicherheitslösungen benötigt werden. Sie sollte innerhalb der Belegschaft Sicherheitskultur effektiv fördern und mit Schulungen und Trainings stets auf dem neuesten Stand halten. Um aber dies zu erreichen, muss die Geschäftsführung umdenken. Sie muss beginnen, das Asset Unternehmensreputation angemessen in ihre Kommunikation und Handhabung der IT-Sicherheit einzubinden. Hierzu bedarf es der Umsetzung des Begriffs „Reputation Driven Defense“. Wieringa definiert den Begriff wie folgt: „Damit sind die Auswirkungen gemeint, die ein Cyberangriff auf das Image eines Unternehmens haben kann und welche Folgen dies für die Security Posture des betroffenen Unternehmens darstellt.“

**Reputation richtig in den IT-Sicherheitsalltag integrieren**

Hierzu muss sie zunächst einmal die Bereiche der Reputation ihres Unternehmens, die von einem Cyberangriff in Mitleidenschaft gezogen werden können, genau definieren und konkretisieren. Wieringa sieht hier drei zentrale Vorgehensweisen: „Als erste Maßnahme müssen diese Ergebnisse dann in die Kommunikation mit der Geschäftsführung eingebunden werden. Zweitens müssen sie in die bestehende Sicherheitskultur des Unternehmens integriert werden. Jeder Mitarbeiter, egal auf welcher Hierarchieebene, muss über die weitreichenden Folgen eines Cyberangriffs für Umsatz und Gewinn ihres Unternehmens stets im Bilde sein. Drittens muss aus ihnen ein auf die Reputation fokussierter Maßnahmenleitfaden für den Fall eines erfolgreichen Angriffs erstellt werden, dessen Inhalt dann im Krisenfall als Anleitung dienen kann, um schnell und unkompliziert aus der Krise zu kommen. Hierbei muss vor allem ein zentraler Fehler, den viele Unternehmen nach wie vor begehen, vermieden werden.“

Dabei handelt es sich um den altbekannten Fehler, einen erfolgreichen Angriff möglichst lange geheim halten zu wollen. In der Praxis hat es sich als weit sinnvoller erwiesen, proaktiv vorzugehen, Verantwortung zu übernehmen und den Willen und die Fähigkeit, das Problem zu lösen, den Kunden und der Öffentlichkeit anschaulich vor Augen zu führen. Als positives Beispiel sei hier nur die Reaktion des Telekommunikationsdienstleisters Vodafone GmbH auf einen 2013 verübten Cyberangriff genannt, bei dem Hacker Stammdaten von über zwei Millionen Kunden erbeuteten. Vodafone entdeckte den Angriff, stoppte ihn, brachte ihn zur Anzeige, machte ihn öffentlich und entschuldigte sich am Ende auch noch bei seinen Kunden. Seine Reputation konnte das Unternehmen mit diesen Maßnahmen erfolgreich stabilisieren.

**Fazit**

Das Beispiel zeigt: wenn es um die Wahrung der Reputation geht, sind Transparenz und ein entschlussfreudiges Handeln der wahre Schlüssel zum Erfolg. Unternehmen sollten daher Sicherheitskultur als Teil ihrer Unternehmenskultur begreifen und entsprechend fördern. Darüber hinaus sollten sie sich mit dem Begriff der „Reputation Driven Defense“ auseinandersetzen und letztlich darin investieren, um bei einem Sicherheitsvorfall den Reputations-Schaden in den Griff zu bekommen.

Dr. Torben Gülstorff

## Vertrauen ist gut? Gegen Pishing hilft nur Zero Trust!

Mit der Corona-Pandemie wechselten zahlreiche Teams vom Büro ins heimische Arbeitszimmer – der „Everywhere Workplace“ war geboren. Ein flexibles Modell, das aber auch Schattenseiten mit sich bringt: Denn die Mitarbeiter greifen auf Firmenressourcen von Geräten aus zu, die sich oftmals der Kontrolle der IT-Abteilung entziehen. Damit einher gehen Gefahren für die Cybersecurity, beispielsweise Phishing. Die ideale Lösung: Zero Trust Security. (447 Zeichen)

**Herausforderung Everywhere Workplace**
Sowohl Mitarbeiter als auch Unternehmen schätzen die Flexibilität, von überall aus zu arbeiten. Denn der „Everywhere Workplace“ erhöht das Engagement, die Freiheit und Effizienz für alle Beteiligten. Dafür spricht auch eine Gartner-Umfrage: Demnach planen 90 Prozent der befragten Unternehmen, ihren Mitarbeitern zumindest teilweise die Möglichkeit zu geben, aus der Ferne zu arbeiten.

Mit diesen Vorteilen gehen aber auch Herausforderungen einher. Denn ortsunabhängiges Arbeiten bedeutet, dass Mitarbeiter von überall aus auf IT-Netzwerke, Anwendungen und Daten zugreifen. Dabei nutzen sie verschiedene, oftmals auch private Geräte und Internetverbindungen. Fakt ist deshalb: Sicherheitsmaßnahmen, mit denen IT-Teams Ressourcen normalerweise schützen, greifen hier oft nicht mehr – sofern die Mitarbeiter sich nicht so umsichtig verhalten, wie es erforderlich ist. Insofern hat diese Remote-Arbeitswelt auch die Angriffsfläche vergrößert und bringt neue Sicherheitsherausforderungen für Unternehmen mit sich.

**Johannes Carl, Expert Manager PreSales – UxM & Security, Ivanti**

**Ausgangslage: Mehr Phishing am Everywhere Workplace**
Zu diesem Schluss gelangt auch eine Studie des Security-Anbieters Ivanti zum Ausmaß von Pishing-Angriffen in Unternehmen. Mit der umfassenden Verlagerung der Arbeitsplätze an Remote-Standorte sind demnach die Angriffe, deren Raffinesse und die Auswirkungen von Phishing-Attacken deutlich gestiegen. Fast drei Viertel (74 Prozent) der Befragten sagen, dass ihr Unternehmen im letzten Jahr Opfer eines Phishing-Angriffs geworden ist, wobei alleine 40 Prozent im letzten Monat eine solche Attacke erlebt haben. Für die Studie wurden im Frühjahr 2021 über 1.000 IT-Experten in Unternehmen in den USA, Deutschland, Großbritannien, Frankreich, Australien und Japan befragt.

**Hintergründe sind vielschichtig**
Remote-Mitarbeiter greifen verstärkt mit mobilen Geräten auf Unternehmensdaten zu. Diese Situation nutzen Hacker offenbar aus und nehmen speziell Sicherheitslücken in diesem Umfeld in den Blick. Zu den neuesten Varianten der Angriffe gehören daher Smishing (SMS-Phishing)- und Vishing-Scams (Voice-Phishing).

Doch woran liegt es, dass die Attacken erfolgreich sind? Auch dazu gibt die Pishing-Studie Aufschluss. 37 Prozent der Befragten nennen als Hauptursache für erfolgreiche Phishing-Angriffe sowohl einen Mangel an entsprechender Technologie als auch zu wenig Achtsamkeit der Mitarbeiter. Viel zu oft verwenden Verbraucher ihre Arbeits-E-Mail oder berufliche Passwörter, um sich bei Verbraucher-Websites und -Anwendungen wie Essenslieferungs-Apps und Online-Einkaufsseiten anzumelden – mit entsprechenden Risiken für die IT-Security.

Auch der Pishing-Studie zufolge ist insbesondere das fehlende Gefahrenbewusstsein der Mitarbeiter der primäre Grund für erfolgreiche Angriffe. Hier beläuft sich die Zustimmung der Befragten auf 34 Prozent. Ein wichtiger Hebel zum Gegensteuern ist die entsprechende Schulung der Mitarbeiter – die offenbar auch vom überragenden Großteil der Unternehmen durchgeführt wird: Fast alle Unternehmen (96 Prozent) bieten Cybersecurity-Trainings an, um die Teams für häufige Angriffsarten wie Phishing und Ransomware zu sensibilisieren. Doch die Umsetzung lässt zu wünschen übrig. So stimmt nicht einmal ein Drittel (30 Prozent) der Befragten zu, dass ein Großteil der Mitarbeiter, also mehr als 80 Prozent, diese Schulungen auch absolviert haben.

**Personalmangel verschärft die Situation**
Das Verhalten der Mitarbeiter ist aber nur ein Grund für die verschärfte Lage. Denn wenn es darum geht, die Sicherheitslage eines Unternehmens unter Kontrolle zu bringen, braucht es entsprechende IT-Fachkräfte. Leider herrscht gerade in diesem Bereich ein großer Mangel. Das bestätigte im vergangenen Jahr rund die Hälfte der Befragten (52 Prozent). Davon sehen wiederum 64 Prozent das fehlende Personal als Ursache dafür, dass es zu lange dauert, Vorfälle zu beheben. Entsprechend glaubt nahezu die Hälfte (46 Prozent), dass die Zunahme von Phishing-Angriffen direkt aus einem Mangel an IT-Fachkräften resultiert.

**Zero Trust Security als geeignete Strategie**
Doch wie lassen sich in einem solchen Umfeld geeignete Sicherheitsmaßnahmen umsetzen? Zero Trust Security ist hier der geeignete Weg. Er ermöglicht es Unternehmen, jedes Asset und jede Transaktion umfassend zu verifizieren, bevor sie auf das Netzwerk zugreifen können. Dazu zählt etwa die starke Authentifizierung von Nutzern, laufend geprüfte Wartungszustände der Geräte und die Mikrosegmentierung von Netzwerken.

Zero Trust nimmt zudem die gesamte Umgebung des Nutzers in den Blick, bevor der Zugriff gewährt wird. Ein Beispiel hierfür ist die Analyse, ob Mitarbeiter von einem firmeneigenen Gerät über ein sicheres Unternehmensnetzwerk auf sensible Kundendaten zugreifen oder von einem privaten Smartphone über das kostenlose WLAN im Zug. Das Zero-Trust-Modell hilft Unternehmen dabei, sich zielführend gegen die wichtigsten Gründe von Datenschutzverletzungen wie gestohlene Anmeldedaten, die Wiederverwendung von Passwörtern und das Imitieren von Nutzern zu wappnen.

**Automatisierung treibt Zero Trust**
Automatisierung, die den Kontext berücksichtigt, ist der entscheidende Teil einer effektiven Zero-Trust-Authentifizierungsstrategie. Automatisierungstools enthalten

in der Regel grundlegende Zero-Trust-Sicherheitsfunktionen wie die kontinuierliche Bewertung des Gerätezustands, rollenbasierte Nutzerzugriffskontrolle und Standorterkennung. Mit Deep Learning haben Unternehmen die Möglichkeit, proaktiv und prädiktiv Probleme mit Konfigurationsdrift, Leistung, Anwendungsverfügbarkeit, Sicherheitsschwachstellen und mehr auf Geräten zu erkennen und dagegen vorzugehen, noch bevor der Endnutzer eine Störung feststellt.

Der Everywhere Workplace bringt Mitarbeitern und Unternehmen eine neue, flexible Arbeitswelt. Damit er aber seine volle Kraft entfalten kann, gilt es für Unternehmen, insbesondere das Thema Security rigide nach einem Zero-Trust-Modell zu managen. Auf diese Weise können sie sich optimal gegen Hackerangriffe rüsten.

Johannes Carl

## Insider Leaks – die unterschätze Gefahr

Insider-Vorfälle sind ein heikles, mitunter unangenehmes Thema, denn niemand möchte seinen Kollegen misstrauen oder ihnen unredliche Absichten unterstellen. Kein Wunder also, dass sich viele Unternehmen am liebsten gar nicht mit diesem Thema beschäftigen wollen. Dennoch gibt es gute Gründe hierfür: Der 2021 Data Breach Investigations Report von Verizon hat gezeigt, dass bei gut einem Viertel aller Sicherheitsverletzungen Insider involviert waren.

Daten stellen für die meisten Unternehmen ihr wichtigstes und wertvollstes Gut dar. Gleichwohl kontrollieren zu wenige Unternehmen ihre Daten adäquat, etwa in Hinblick auf Nutzung und Zugriff. Stattdessen sind oftmals zahlreiche Dateien für alle Mitarbeiter zugänglich und können nicht nur geöffnet, sondern auch kopiert, verschoben, verändert, gelöscht und an Dritte gemailt werden.

Der Zugriff auf Daten in jedem Unternehmen sollte jedoch idealerweise auf diejenigen beschränkt sein, die sie tatsächlich benötigen. Dieser Least-Privilege-Ansatz verringert die Wahrscheinlichkeit deutlich, dass diese Daten exfiltriert, beschädigt oder verschlüsselt werden, wenn ein Nutzerkonto (etwa durch Phishing) kompromittiert wird.

**Wie kommt es zu Insider-Vorfällen?**

Meist steckt hinter Insider-Vorfällen keine böse Absicht, wenngleich die Folgen ebenso verheerend sein können wie von gezielten Aktionen. Die meisten Mitarbeiter wollen in erster Linie ihre Arbeit erledigen – und zwar möglichst einfach und bequem. Dabei halten sie sich jedoch nicht zwingend an die Unternehmensrichtlinien, die den Umgang mit Daten regeln. So speichern sie Dateien auf gemeinsam genutzten oder vernetzten Laufwerken, ohne sich bewusst zu sein, welche weitreichenden Folgen das haben könnte. Im Grunde ist es ganz einfach: Je mehr Personen auf eine Datei zugreifen können, desto größer ist die Wahrscheinlichkeit eines Schadens durch ein kompromittiertes Konto.

Die Cloud hat vieles vereinfacht, aber einiges auch wesentlich komplizierter gemacht. In Zeiten, in denen die meisten Daten noch vor Ort gespeichert wurden, war der Datenzugriff leichter zu kontrollieren. Gleichwohl stellten auch hier inkonsistente Zugriffskontrolllisten (ACLs) und globale Zugriffsgruppen ein Risiko für die Daten dar, und es war auch „damals“ schon üblich, dass Benutzer Daten auf gemeinsam genutzten oder vernetzten Laufwerken speicherten. Durch die explodierenden Datenmengen und neue Speicherorte wurde es in den letzten Jahren immer schwieriger bis fast unmöglich, alle inkonsistenten ACLS zu finden und zu beheben. Entsprechend landen sensible Daten fast zwangsläufig irgendwann an einem unsicheren Ort.

**Der Trend zu Remote Work**

Die rasche Verbreitung von Cloud-basierten Collaboration-Tools in Folge des massiven Ausbaus von Homeoffice-Arbeitsplätzen hat dieses Problem noch verschärft. Tools wie Microsoft Teams ermöglichen es Benutzern, neue Speicherorte zu erstellen und den Zugriff auf die dort gespeicherten Daten mit jedem im Unternehmen zu teilen. Oft fehlt es den Sicherheitsverantwortlichen an Transparenz, wie Daten geteilt und neu gespeichert werden. Zum Beispiel kann jeder, der Microsoft Teams verwendet, mehrere SharePoint-Sites online erstellen, Benutzer mit verschiedenen Zugriffsebenen hinzufügen oder den Zugriff für jeden verfügbar machen: alles mit ein paar Klicks und ohne technisches Fachwissen – und ohne die IT-Abteilung hierbei einzubeziehen.

Effektive Zugriffsbeschränkungen für alle Daten könnten viel dazu beitragen, solche Praktiken einzudämmen, stellen jedoch eine große organisatorische Herausforderung dar. So ist es eine umfassende Aufgabe, sensible Daten und deren Sensibilitätsgrad zu identifizieren, um entsprechende Kontrollen anzuwenden. Hierzu müssen Unternehmen nämlich genau wissen, wo welche Daten gespeichert sind, wer Zugriff auf diese Daten hat, ob dieser Zugriff legitim ist und wer die Verantwortung für Entscheidungen über den Zugriff trägt.

**Daten klassifizieren, Berechtigungen reduzieren**

Oftmals wird empfohlen, dass die Ersteller der Daten diese entsprechend klassifizieren und kennzeichnen. Dies setzt jedoch voraus, dass die für die Kennzeichnung verantwortlichen Personen wissen, welche Daten überhaupt als sensibel anzusehen sind, und dass sie die Daten nicht absichtlich falsch kennzeichnen, um den Zugriff zu erleichtern und Ärger durch Einschränkungen zu vermeiden. Hier können intelligente

**Michael Scheffler, Country Manager DACH, Varonis Systems**

automatisierte Lösungen mit vorgefertigten Regeln und intelligenter Validierung helfen, die Daten adäquat zu klassifizieren.

Die Klassifizierung von Daten ist jedoch nur ein erster Schritt, reicht aber in der Regel nicht aus, um Risiken effektiv zu reduzieren und Compliance-Vorgaben einzuhalten. Hierzu müssen zusätzliche Metadatenströme, wie Berechtigungen und Datennutzungsaktivitäten, einbezogen und mit weiterreichenden Aktivitäten verknüpft werden.

Letztendlich entscheidend ist der Umgang der Mitarbeiter mit den Daten und deren Berechtigungen. Unternehmen sollten deshalb sicherstellen, dass Benutzer den Zugriff auf Daten nicht über das notwendige Maß hinaus ausweiten. Regelmäßige Schulungen zum Sicherheitsbewusstsein sind sinnvoll, garantieren aber noch keine absolute Sicherheit. Denn es ist nur eine Frage der Zeit, bis ein Mitarbeiter einen sicherheitsrelevanten Fehler macht. Und dies kann wirklich jedem passieren, wenn der Angriff etwa durch Spear-Phishing gut vorbereitet und auf das Opfer angepasst ist. Es geht schon längst nicht mehr darum, nicht angegriffen zu werden, sondern wie man mit einer solchen Attacke umgeht. Folgt man einem datenzentrierten Ansatz, um insbesondere die sensibelsten Daten etwa durch ein automatisiertes Berechtigungsmanagement zu schützen, lässt sich der Schaden deutlich reduzieren. Durch proaktive Schritte zum Sperren kritischer Informationen und eine intelligente Analyse des Nutzerverhaltens lassen sich Angriffe stoppen, noch bevor sie größeren Schaden anrichten. Grundlage hierfür ist die effektive Umsetzung des Least-Privilege-Ansatzes, der sowohl die lokalen als auch die Cloud-Datenspeicher und -dienste einbeziehen muss. Nur so lässt sich das Risiko effektiv reduzieren, dass Mitarbeiter (unabsichtlich) zu Innentätern werden.

Michael Scheffler

# 1.3 CLOUD

## Multi-Cloud-Sicherheit

**Komplexität beherrschen durch Machine Learning**

Im Zuge ihrer digitalen Transformation haben bereits viele deutsche Unternehmen Multi-Cloud-Infrastrukturen eingeführt, um Single-Points-of-Failure zu vermeiden und die Angebote der Cloud-Provider in technischer und wirtschaftlicher Hinsicht optimal zu kombinieren. Im täglichen Betrieb zeigt sich nun aber, dass dieser Schritt neben unbestreitbaren Vorteilen auch erhebliche Herausforderungen mit sich bringt: Der Komplexitätsgrad des Cloud-Infrastrukturmanagements wird durch Multi-Clouds um ein Vielfaches gesteigert, sodass Sicherheit und Compliance mit den bislang bewährten Methoden kaum noch umgebungsweit gewährleistet werden können.

Die unzähligen Abhängigkeiten der Multi-Cloud-Komponenten vergrößern die Angriffsfläche und erschweren die Nachverfolgung von Angriffsvektoren. Ohne zentralisierte Sichtbarkeit aller Vorgänge in der Infrastruktur gleicht die Jagd nach Eindringungspunkten einem Blindflug. Angesichts der Dynamik von Multi-Clouds wird die vorausschauende Definition von Regeln, jahrzehntelang das A und O des Sicherheitsmanagements, zur Sisyphus-Aufgabe.

**Unternehmen verlieren Vertrauen**

Vor diesem Hintergrund verlieren viele Unternehmen das Vertrauen in ihre Fähigkeit, Cyberangriffe in Multi-Clouds zu beherrschen, zu diesem Ergebnis kommt eine Studie* aus dem September 2020: Je mehr Cloud-Dienste genutzt werden desto größer ist die Bereitschaft, auf Ransomware-Forderungen einzugehen. Nur 10 Prozent der deutschen Unternehmen, die weniger als fünf Cloud-Dienste einsetzen, zahlten einen Teil des Lösegeldes. Von den Unternehmen mit mehr als zwanzig eingesetzten Cloud-Diensten gingen hingegen 60 Prozent auf die gesamte Lösegeldforderung ein. Nur ein knappes Viertel der befragten Unternehmen glaubt, dass die vorhandene IT-Sicherheit mit der Komplexität der Multi-Cloud Schritt halten kann.

**Multi-Clouds multiplizieren Aufwand**

Primär Regel- und Signaturen-basierte Sicherheitslösungen sind nicht Cloud-nativ, sondern stammen aus einer Ära klar abgesteckter Perimeter und vorsichtig geplanter Change-Prozesse. Cloud-Umgebungen sind aber ihrer Natur nach dynamisch und veränderlich, sodass die Definition granularer Regeln nie abgeschlossen ist. Um die Anzahl der False Positives zu reduzieren, werden Regeln außerdem meist für eindeutig definierbare Szenarien geschrieben, was die Effektivität bei ganz neuen Bedrohungen oder Vorfällen in der Grauzone begrenzt.

Multi-Clouds multiplizieren sowohl den Aufwand als auch die Komplexität der Regeldefinition, die jetzt für alle genutzten Cloud Provider durchgeführt werden muss. Entwickler können zum Beispiel Infrastrukturressourcen mit den vergleichbaren Services AWS CloudFormation, Azure Resource Manager oder Google Cloud Deployment Manager bereitstellen und verwalten. Wenn nun gewährleistet werden soll, dass die Ausführung von Build-Skripts in allen drei Clouds immer den aktuellen Sicherheitsregeln des Unternehmens entspricht, so verdreifacht sich der Aufwand.

**Alarmflut überfordert Sicherheitsteams**

Der Aufwand der Regeldefinition ließe sich theoretisch durch mehr Personal auffangen – praktisch sind solche Fachkräfte mit aktuellem Know-how kaum verfügbar. Aber herkömmliche Ansätze stoßen auch in ande-

*„The 2020 Ransomware Resiliency Report", Wakefield Research im Auftrag von Veritas Technologies, September 2020

rer Hinsicht an ihre Grenzen: Häufig konzentrieren sich die eingesetzten Sicherheitswerkzeuge auf ganz bestimmte Aspekte, was zu Informationssilos und unzähligen Alarmen führt.

Ohne Kontextinformationen und Priorisierung ist eine sinnvolle Verarbeitung der anfallenden Datenmengen in Multi-Cloud-Umgebungen nicht mehr menschenmöglich. Weitere Probleme für die Angriffsanalyse entstehen durch die begrenzte Sichtbarkeit von Microservices, Data Caches und temporären IP-Adressen, die oftmals nur wenige Minuten aktiv sind und dann gelöscht werden. Alle Aktivitäten, die nicht in dieser kurzen Zeit erfasst werden, gehen für Sicherheitsanalysen verloren.

**Verhaltensbasierte Sicherheit eliminiert Regeln**

Die künftige Entwicklung scheint absehbar: DevOps, Container und Technologien wie Serverless Computing drehen die Komplexitätsspirale weiter und erfordern gleichzeitig immer schnellere Reaktionen von der IT-Sicherheit. Dadurch entstehen fast unweigerlich nicht erkannte Sicherheitslücken in der Multi-Cloud, die von professionellen Angreifern ausgenutzt werden.

Um dieser Entwicklung zuvorzukommen, ist eine wachsende Zahl von Unternehmen bereit, den eigenen Sicherheitsansatz für die Cloud-Welt auf den Prüfstand zu stellen. Zwei Überlegungen stehen dabei im Fokus: Erstens muss ausnahmslos jede Multi-Cloud-Komponente zentral überwacht werden, blinde Flecken sind absolut inakzeptabel. Zweitens muss die Überwachung vollständig automatisiert ablaufen, denn die produzierten Datenmengen können manuell nicht ausgewertet werden. Händische Regeldefinitionen und Log-Auswertungen sind ausgeschlossen.

Diese Vorgaben lassen sich durch ein lückenloses Monitoring der Cloud-Prozesse und eine Machine-Learning-gestützte Analyse des Normalzustandes erreichen. Prozesse bilden die kleinsten vom Betriebssystem unterstützten Einheiten und sind verantwortlich für die gesamte Kommunikation, sowohl miteinander als auch mit externen Hosts. Sie haben zudem nachverfolgbare Startumstände, Hashwerte, Zwecke und Lebenszyklen und werden nicht zwischen unterschiedlichen Applikationen gemischt.

**Baseline zeigt Normalzustand**

In Echtzeit werden alle Interaktionen zwischen Prozessen erfasst, auch wenn sie innerhalb derselben Datei stattfinden. Das Monitoring erstreckt sich auf Prozesshierarchien, Prozesse/Machine-Kommunikation, Änderungen an Anwender-Privilegien, interne und externe Datentransfers und alle anderen Cloud-Aktivitäten. Auf Basis dieser lückenlosen Überwachung kann mittels Machine Learning eine temporale Baseline erstellt werden, die Aufschluss gibt über das normale Verhalten von Anwendern, Applikationen und Workloads in der Multi-Cloud.

Die gesammelten Daten werden zudem entsprechend der zugehörigen Cloud-Entität in Analysegruppen organisiert. Verhaltensbasiertes Machine Learning vergleicht das aktuelle Verhalten einer Cloud-Entität einerseits mit ihrem bekannten Verhalten im Zeitverlauf, andererseits aber auch mit dem bekannten Verhalten ähnlicher Cloud-Entitäten in der jeweiligen Analysegruppe. Anomalien, also alle abweichenden Aktivitäten, heben sich vor diesem Normalzustand deutlich ab.

**Wert für die Sicherheitspraxis**

Der automatisierte Abgleich mit dem bekannten Verhalten und der Analysegruppe identifiziert bekannte und unbekannte Bedrohungen. Viele Aktivitäten, die sich mit Regeln nur schwer erfassen lassen, können jetzt im Kontext bewertet werden. Dazu gehören zum Beispiel der Ab- oder Zufluss ungewöhnlicher Datenmengen in Amazon S3 Buckets, unerwartete Verbindungen von Applikationen, auffällige API-Aufrufe durch Container sowie jedes nicht normale Anwender-Verhalten.

Weil die Technologie den Normalzustand kennt, kann sie zudem viele reguläre Aktivitäten im Cloud-Datacenter als Bedrohung ausschließen. Das senkt die Zahl der False Positives und Alarme. Diese drastische Reduktion der Komplexität ermöglicht es der IT-Sicherheit, Multi-Cloud-Initiativen aktiv zu unterstützen, ohne Kompromisse beim Schutz einzugehen.

Bernd Mährlein

**Bernd Mährlein, Area Director Central Europe, Lacework**

## Sichere Cloud dank zertifiziertem Schutz

Die Rolle von Cloud- und Multi-Cloud-Umgebungen in Unternehmen wächst stetig – verstärkt auch durch die Corona-Pandemie und den damit verbundenen Auswirkun-gen auf Unternehmen und Unternehmenskulturen. Viele Arbeitgeber haben bereits verlauten lassen, nach den Einschränkungen und Schutzmaßnahmen gegen Covid-19 vermehrt auf ‚Work from anywhere' zu setzen und den eigenen Mitarbeitern mehr Homeoffice zu ermöglichen. Zur Umsetzung dieser Pläne bedarf es allerdings einer entsprechenden Infrastruktur und eines dafür optimierten technologischen und pro-zessualen Ökosystems. Der Grad der Digitalisierung, besonders in kleinen und mittle-ren Unternehmen (KMU), muss entsprechend angehoben werden, um in der neuen Arbeitswelt wettbewerbsfähig zu bleiben.

Cloud- und Multi-Cloud-Lösungen bieten nicht nur einen schnelleren Zugriff auf Un-ternehmensdaten, als es viele VPN-Lösungen können, sondern die Verlagerung von Anwendungen und Services in Cloud-Umgebungen erleichtert oftmals die tägliche Arbeit der eigenen Mitarbeiter erheblich. Neben diesen Vorteilen birgt die Migration in die Cloud allerdings auch diverse Stolpersteine, besonders in Sachen der

Sicherheit und des Datenschutzes, die vor dem Start von solchen Projekten beachtet und nach Abschluss regelmäßig geprüft werden müssen, um die Entstehung von Sicherheitslü-cken und Datenlecks zu verhindern bzw. auf diese schnellstmöglich zu reagieren.

**Alexander Häußler, Product Compliance Manager ISO/IEC 27001, TÜV SÜD Management Service**

**Identitätsmanagement und Zero Trust sorgen für Sicherheit im Homeoffice**

Neben möglichen Fehlkonfigurationen bleibt ein weiterer Angriffsvektor ein Problem für die Cloud: Zugangsdaten und Identitätsmanagement. Phishing ist nach wie vor eine der größten Cyber-Bedrohungen, die Mitarbeiter in Unternehmen unmittelbar betreffen. Die Bedrohungsakteure haben sich zudem das Homeoffice als neues An-griffsziel ausgesucht, um ihre Opfer mit falschen Liefer-Meldungen oder ausgefeilten Social-Engineering-Attacken auszutricksen und sich Zugangsdaten zu beschaffen. Durch die physische Trennung vom Unternehmensnetzwerk - und Kollegen - steigt die Verantwortung, die der einzelne Mitarbeiter als Teil einer Art menschlichen Fire-wall zur Bedrohungsabwehr trägt, enorm. Das erfordert nicht nur einen größeren Fo-kus auf Security Awareness, den es von Unternehmensseite zu setzen gilt, sondern eine Adaption von Least-Privilege- und Zero-Trust-Ansätzen. Dabei wird für jeden Nutzer initial und anschließend regelmäßig genau evaluiert, welche Rollen und Rechte er benötigt, und ob diese eventuell zu einem späteren Zeitpunkt nicht mehr benötigt werden. Das schränkt nicht nur dessen Bewegungsfreiheit innerhalb des Systems ein, sondern dadurch wird dafür gesorgt, dass selbst bei einem erfolgreichen Einbruch eines Kriminellen in das Netzwerk der dabei entstandene Schaden in Gren-zen gehalten werden kann.

Ein starkes Identitätsmanagement zur eindeutigen Identifikation, bei Bedarf durch ei-ne Mehr-Faktor-Authentifizierung, hilft ebenfalls, um Einbrüche und Datenlecks zu verhindern. Sogar wenn somit einmal Anmeldedaten und die dazugehörigen Pass-wörter durch Phishing abhandengekommen sein sollten, so helfen diese zusätzlichen Sicherheitsmaßnahmen dabei, die Kriminellen auszusperren.

**Fehlkonfiguration als Gefahrenquelle in der Cloud**

Eine Mehrheit der Sicherheitslücken in Cloud-Lösungen und der dadurch entstehen-den Schäden lässt sich auf initiale Fehlkonfigurationen bei der Migration zurückfüh-ren. Unternehmen, beziehungsweise deren IT-Abteilungen, gehen nach wie vor zu häufig davon aus, dass die Verantwortung für die Sicherheit von Daten und Anwen-dungen innerhalb der Cloud lediglich beim Anbieter der IaaS-Lösung (Infrastructure-as-a-Service) liegt. Allerdings garantiert dieser zumeist nur die Sicherheit der Cloud selbst. Sollten also unternehmen Anwendungen oder Services dorthin verschieben, so sind sie auch selbst für die Absicherung dieser verantwortlich.

Im Zuge der Covid-19-Maßnahmen war es für viele KMU notwendig, schnell zu han-deln, um die Geschäftskontinuität zu gewährleisten. Während nun IT-Sicherheitsabteilungen oftmals die Kräfte fehlen, um sich dem Problem der Fehlkonfi-gurationen anzunehmen, haben die Cyber-Kriminellen bereits reagiert: Mehr Malwa-re und Ransomware wird über Sicherheitslücken in der Cloud in Unternehmen ein-geschleust. Eine aktuelle Studie von IDG Research zeigt: Jedes dritte Unternehmen hat in den vergangenen 12 Monaten einen wirtschaftlichen Schaden durch Angriffe auf die von ihnen genutzten Cloud-Dienste erlitten – wiederum ein Drittel der be-troffenen Unternehmen hatte sogar mit einem kompletten Stillstand aufgrund der An-griffe zu kämpfen.

**Normen schaffen Vertrauen**

Einer der zuverlässigsten Wege zur sicheren Nutzung der Cloud ist die Überprüfung des Systems durch unabhängige Experten. Diese können dabei helfen, die IT-Sicherheitsabteilungen zu entlasten und die Daten und Anwendungen innerhalb der Cloud-Umgebung zu sichern. Dabei helfen ihnen unter anderem die Normen ISO / IEC 27001 und deren Erweiterung 27701. Die Normenreihe fordert beispielsweise die Implementierung eines Informationssicherheits-Managementsystems (Information Security Management System, ISMS) zur Sicherung des technologischen Ökosystems von Unternehmen. Dabei handelt es sich um eine Aufstellung von Regelungen, Maß-nahmen und Programmen, die innerhalb eines Unternehmens angewendet werden sollten. Wichtig ist, dass dabei aber mehr als nur die verwendete Technologie und die digitale Infrastruktur eines Unternehmens betrachtet wird. Dabei setzt ein ISMS be-reits auf der Prozessebene an, um sein Ziel der Informationssicherheit im gesamten Unternehmen zu erreichen. Durch diesen ganzheitlichen Ansatz helfen die Normen dabei, jeden Aspekt der Arbeit mit Cloud-Lösungen sicherer zu gestalten: von der Migration über die Datenspeicherung bis hin zu den Zugriffen der Nutzer auf Anwen-dungen und Informationen.

Wer also dafür sorgt, dass eigene Lösungen nach den entsprechenden Normen zerti-fiziert sind, der kann wirklich von einer sicheren Cloud sprechen. Zudem hilft die Zerti-fizierung im Schadens- oder Haftungsfall: die Normenreihe ISO / IEC 2700x bietet Un-ternehmen im Falle eines Rechtsstreits ein solides Fundament für die Argumentation.

**Nur eine sichere Cloud bringt Vorteile**

Laut einer Umfrage von Gartner setzen nicht nur mehr Unternehmen auf Cloud-Lösungen, um ihre bestehenden technologischen Ökosysteme zu erweitern, sondern 75 Prozent der Unternehmen, die diese bereits verwenden, spekulieren, in Zukunft einen Cloud-First-Ansatz zu verfolgen. Viele dieser Un-

ternehmen erkennen den Stel-lenwert der Sicherheit von Daten und Informationen innerhalb der Cloud an – daher steigt der Wunsch, diesen Schutz bestätigt zu bekommen. Eine Zertifizierung der ver-wendeten Cloud-Lösungen und -Dienste nach den Normen ISO / IEC 27001 und 27701 hilft dabei, das entsprechende Vertrauen zu schaffen, und somit den Weg zu einem sicheren ‚Work from anywhere' als Prinzip und einer sicheren, neuen Arbeits-welt zu schaffen.

Alexander Häußler

## Viel zu komplex? Wie Unternehmen Multi-Cloud-Umgebungen effektiv absichern können

Die Bereitstellung von Daten und Anwendungen im Rahmen einer verteilten Workforce, geplante Kostenreduktion, verbesserte Skalierbarkeit und die Grundlage für die digitale Transformation: Seit dem Beginn der Pandemie sehen immer mehr Unternehmen die Vorzüge des Cloud Computings und haben Ihre Digitalisierung hier teilweise schneller vorangetrieben als ursprünglich geplant. Oft werden hierbei Multi-Cloud Umgebungen eingesetzt, um auf die individuellen Bedürfnisse der einzelnen Unternehmensbereiche besser eingehen zu können. Doch wo sich Vorteile ergeben, lassen sich auch Nachteile finden: In Multi-Cloud-Umgebungen nehmen diese die Form von Undurchsichtigkeit, wodurch schnell Sicherheitslücken zum Beispiel durch Fehlkonfigurationen entstehen können. Tanja Hofmann, Lead Security Engineer bei McAfee, spricht über die Risiken in der Multi-Cloud und die notwendigen Sicherheitsmaßnahmen.

Fast alle Cloud-Angriffe sind das Ergebnis von Fehlkonfigurationen für die Unternehmen selbst verantwortlich sind. So ergeben sich für die IT ganz neue Herausforderungen, um einen sicheren Betrieb der eingesetzten Lösungen zu ermöglichen. Andererseits sollte Mitarbeitern das Arbeiten von zu Hause ermöglicht werden. Hierzu wurde die Transformation in die Cloud vorangetrieben: Weltweit stieg der Einsatz von Cloud Services und -Anwendungen um 50 Prozent. Nun – nach einem Jahr – ist eine Rückkehr zu alten Prozessen kaum mehr denkbar. Was neben den Vorteilen einer dezentralen IT-Infrastruktur jedoch ebenfalls bleibt, sind die Cyber-Schwachstellen, die mit der Umstellung auf Cloud-Systeme einhergegangen sind. Das liegt vor allem daran, dass der Sicherheitsaspekt aufgrund des spontanen und schnellen Wandels in vielen Unternehmen zu kurz gekommen ist. Die Beseitigung dieser Schwachstellen sollte nun eine hohe Priorität einnehmen, da sich dieses Vorhaben – besonders in wachsenden Multi-Cloud-Umgebungen – als herausfordernd herausstellen kann.

### Wenn Fehlkonfigurationen das Bedrohungspotenzial steigern

Immer mehr Unternehmen verbinden verschiedene Cloud Services, -Anwendungen und -Plattformen miteinander, die in der Regel von unterschiedlichen Providern bereitgestellt werden. Laut einer Untersuchung der IDC betonen 87 Prozent der Befragten, dass sie bereits auf Multi-Cloud setzen beziehungsweise sich in der Planungsphase befinden. Der Vorteil einer solchen Umgebung: Jeder Anforderung wie Speicher, Skalierbarkeit oder Datenschutz wird ein passender Cloud Service oder eine -Anwendung, die aus voneinander unabhängig agierenden, miteinander gekoppelten Microservices besteht, zugeordnet. Durch solch eine modulare Architektur erhalten Unternehmen genügend Flexibilität, Cloud-native Anwendungen zu entwickeln und zu hosten.

Doch je mehr Komponenten die Cloud-Infrastruktur erhält, desto undurchsichtiger und unübersichtlicher kann sie werden. Mit schwindender Transparenz steigt das Risiko, Schwachstellen und akute Bedrohungen nicht rechtzeitig zu erkennen sowie zu beheben – für Cyber-Kriminelle eine willkommene Möglichkeit, um schnell und unbemerkt in das Multi-Cloud-Geflecht einzudringen. Ein Beispiel für eine solche Schwachstelle ist die Fehlkonfiguration von Cloud-Systemen, wie zum Beispiel durch (fehlerhafte) Berechtigungsprotokolle oder Systeme, die nicht regelmäßig von der IT gepatcht werden. Unternehmen begünstigen solche Fehlkonfigurationen, indem sie die betroffenen (Cloud-) Systeme nicht an ihre eigenen Anforderungen anpassen, sondern Standardeinstellungen anstandslos übernehmen. Auch in diesem Fall trüben viele Cloud-Systeme den Blick für das Wesentliche: IT-Admins müssen mehrere Cloud-Konfigurationen auf einmal verwalten können.

**Tanja Hofmann, Principal Security Engineer, McAfee**

### 360°-Sicherheit: Jeder trägt einen Teil der Verantwortung

Die richtige Sicherheitsstrategie hilft dabei, das volle Potenzial der Multi-Cloud ausschöpfen zu können, und sorgt gleichzeitig dafür, dass Schwachstellen, wie zum Beispiel Fehlkonfigurationen, rechtzeitig vor Cyber-Kriminellen und ihren Intentionen abgesichert werden. Das 360° Shared Responsibility Model gibt hierfür eine eindeutige Orientierung vor, mit der sich Verantwortlichkeiten einteilen und Sicherheitsmaßnahmen entwickeln sowie umsetzen lassen. Wichtig zu bedenken ist, dass die Verantwortung über die Sicherheit von Cloud-Umgebungen nicht allein bei den Cloud Service Providern liegt. Diese konzentrieren ihre Sicherheitsbestreben vornehmlich auf die physischen Bestandteile des Netzwerks sowie die Hosting-Infrastruktur.

Das Identity and Access Management (IAM) hingegen liegt primär in den Händen der Unternehmen, die den Cloud Service beanspruchen. Sprich:

Unternehmen bzw. deren IT-Teams kümmern sich um die Identitätsverwaltung und die Vergabe von Zugriffsrechten. Im Umkehrschluss bedeutet dies, dass auch Fehlkonfigurationen von Cloud-Systemen im Verantwortungsbereich der Unternehmen und nicht der Service Provider liegen.

**Trotz Komplexität für sichere Multi-Cloud-Umgebungen sorgen**

Sobald die Verantwortlichkeiten in Sachen IT-Sicherheit definiert und den verschiedenen Instanzen zugeordnet sind, müssen Unternehmen auch auf technischer Seite für Lösungen sorgen, die das allgemeine Sicherheitsniveau stärken. Hierfür bieten sich einerseits Cloud-Security-Posture-Management-Lösungen (CSPM) an, die IT-Teams einen zentralen und ganzheitlichen Einblick in das gesamte Sicherheits-Management ermöglichen. Gleichzeitig sind sie in der Lage, Cloud-Umgebungen basierend auf vorgegebenen Best Practices kontinuierlich und automatisiert zu überwachen. Auf diese Weise können sie Fehlkonfigurationen selbst in den komplexesten Umgebungen schnell ausfindig machen und aufgrund dieser Erkenntnisse dann die passenden Maßnahmen ergreifen. Darüber hinaus helfen CSPM-Lösungen dabei, die Compliance unternehmensweit einzuhalten.

Andererseits gilt es, Lösungen zu implementieren, die mehr Transparenz über Workloads in der gesamten Multi-Cloud-Umgebung ermöglichen und die effektive Absicherung auf Host-Ebene vereinfachen. Für diesen Zweck eignet sich eine Cloud Workload Protection Platform (CWPP). Eine solche, auf moderne Cloud-Infrastrukturen angepasste Plattform setzt auf Netzwerkesegmentierung, führt Maßnahmen zum Schutz der Systemintegrität durch, scannt das System auf Malware und überwacht das Nutzerverhalten.

**Fazit**

Als Teil unseres Arbeitsalltags unterstützt die Cloud nicht nur verteilte Teams dabei, effizient zusammenzuarbeiten, sondern gestaltet die Arbeit insgesamt einfacher und ressourcenschonender. Der hohe Grad an Anpassungsfähigkeit einer Multi-Cloud-Umgebung führt dazu, dass sich dieses Modell mit zunehmender Beliebtheit ausbreitet. Doch je mehr Cloud-Systeme miteinander interagieren, desto mehr geht die Transparenz der Infrastruktur verloren und das Risiko von Cyber-Schwachstellen in Form von Fehlkonfigurationen steigt. CSPM- und CWPP-Lösungen verschaffen IT-Teams eine bessere Übersicht über ihr Sicherheits-Management und machen sie mithilfe von Automation auf Fehlkonfigurationen aufmerksam. So lassen sich konfigurationsbedingte Schwachstellen im Handumdrehen schließen, bevor Cyber-Kriminelle auch nur einen Finger rühren können.

Tanja Hofmann

## Multi Layer-Security statt eindimensionalem Schutz gegen Cyberkriminalität

IT-Sicherheit wird auch heute noch oft mit dem eindimensionalen Schutz von Endpunkten und Endgeräten gleichgesetzt. Da Malware das Endgerät sowohl als Ziel und als Einfallstor nutzt, müssen Schutzmaßnahmen dort greifen – so lautet die Argumentation der Verfechter. Die Wahrscheinlichkeitsberechnung der IT-Sicherheit belegt jedoch, dass sich die Effizienz des Schutzschirms durch die Kombination unterschiedlicher Security-Maßnahmen deutlich steigern lässt.

Wenn ein Schutzmechanismus 99,9 Prozent aller Attacken erkennt und verhindert, bedeutet das, dass nach wie vor eine aus tausend Bedrohungen durch das Schutzaster rutschten kann. Diese Rechnung wird lediglich beispielhaft angeführt, denn es soll nicht der Eindruck entstehen, dass es sich dabei um effektiven Schutz handelt. Kombiniert man aber verschiedene, spezialisierte Abwehrmechanismen an verschiedenen Punkten einer Transaktion, lässt sich die Effizienz der Sicherheit erhöhen. Jede Schutzmaßnahme spielt dabei ihre eigenen Stärken zur Erkennung und Abwehr von Angriffen aus.

Die Wahrscheinlichkeitsberechnung zeigt, dass sich verschiedene Schutzschirme in ihrer Wirksamkeit nicht nur aufaddieren, sondern vervielfältigen. Zwei Kontrollmechanismen mit der gleichen Effizienz von 1 in 1000 reduzieren den Erfolg eines erfolgreichen Angriffs auf eine Wahrscheinlichkeit von 1 in einer Million. Um diese Multiplikation der Effizienz zu erzielen kommt es darauf an, unterschiedliche Technologien für die IT-Sicherheit einzusetzen, um darüber verschiedene Angriffsarten abzudecken. Dazu sollte beispielsweise die Untersuchung von SSL-Traffic auf Malware und Zero-Day-Attacken ebenso zählen, wie das Durchleuchten von Angriffsflächen, die ein Unternehmen durch seine Infrastruktur im Internet exponiert hat.

**Kombinierter statt isolierter Schutz**

Folgende Kategorisierung hilft Unternehmen beim Erstellen ihrer Sicherheitsstrategie durch eine Risikobewertung. Sie sollten Technologien unterscheiden, die für den Schutz und Vorbeugung vor Angriffen oder deren Erkennung stehen. Schutzstrategien für den Endpunkt gehen oftmals damit einher, eine bekannte Bedrohung durch Malwarefilter über die Erkennung bekannter Muster abzuwehren. Möchte man darüber hinaus unbekannte Angriffsarten erkennen, muss man auf Verhaltensanalyse setzen und darin nach Mustern im Vorgehen der Angriffe suchen und nicht mehr nach einer spezifischen Malware-Art. In einem nächsten Schritt könnte dazu nicht nur die eingehende Kommunikation auf Malware-Muster und Verhaltensweisen untersucht werden, sondern

ebenso der outbound-Datenverkehr, um damit beispielsweise Command & Control-Traffic oder das Abfließen vertraulicher Informationen zu verhindern. So lassen sich je nach Sicherheitsbedürfnis eines Unternehmens nach und nach verschiedene Schichten an Abwehrmechanismen auffahren in Richtung einer Multilayered-Sicherheitsstrategie.

Neben dem Schutz vor und der Erkennung von Malware geht eine dritte Kategorie weit über die genannten klassischen Abwehrmechanismen hinaus. Der dritte Weg lässt sich aufbauend auf dem berühmten chinesischen Militär-Strategen und General Sun Tzu formulieren. Er war der Ansicht war, dass der größte Sieg derjenige ist, der keinen Kampf erfordert. Auf die IT-Sicherheit übertragen bedeutet das, dass sich Angriffe dadurch vermeiden lassen, dass man Malware-Akteuren gar nicht erst eine Angriffsfläche bieten sollte. Diese Vermeidungsstrategie wird heute noch viel zu selten im Zuge der Risikominimierung von Unternehmen eingesetzt. Im Gegenteil sind sich Unternehmen ihrer Angriffsflächen vielfach gar nicht bewusst.

Die Vorgehensweisen zur Ebenen-artigen Risikominimierung lassen sich wie folgt zusammenfassen: Der erste Weg möchte den eingehenden Angriff abwehren, der zweite versucht Bedrohungen auf Basis von Verhaltensanalyse zu entdecken und unschädlich zu machen und der dritte möchte Angriffe von vorneherein verhindern. Diese drei Methoden zusammengenommen bauen eine starke Abwehr auf und minimieren die Wahrscheinlichkeit eines erfolgreichen Cyber-Angriffs.

**Zero Trust reduziert die Angriffsfläche**

Unternehmen sind also gefordert, je nach ihrer Risikobereitschaft Abwehrmechanismen aufzufahren. Mit der simplen Logik von Wahrscheinlichkeitsberechnungen können sie ihr Schutzniveau so verargumentieren, dass es auf Basis von klaren Prinzipien leicht verstanden werden kann. Um auch die mögliche Angriffsfläche zu minimieren, eignet sich der Aufbau einer auf dem Zero Trust basierenden Sicherheitsstrategie. Wenn jeder Mitarbeiter oder auch Drittparteien das Unternehmensnetz mit vollem Zugriff auf alle Dateien und Anwendungen betreten darf und auf diese Weise Einblick in die gesamte Struktur des Netzwerkes hat, dann ergibt sich daraus eine deutlich erhöhte Angriffsfläche. Es reicht lediglich ein gehackter Mitarbeiter-Account, um großen Schaden im gesamten Netzwerk anzurichten. Besonders die Homeoffice-Situation führt zu einer hohen Zahl an Angriffen, da Mitarbeiter zuhause weniger aufmerksam sind und gleichzeitig ihre Arbeitsgeräte weniger geschützt sind. Konfigurationsfehler oder mögliche Schwachstellen in VPN-Hardware, die zusätzlich offen über das Internet erreichbar sind, lädt Angreifer zum Eindringen und zu lateraler Bewegung im Netzwerk ein.

Hier kommt Zero-Trust Network Access ins Spiel als Alternative für die Absicherung des Fernzugriffs. Durch ein Cloud-basiertes Modell wird der Anwender auf Basis von Autorisierung und Authentifizierung auf dem direkten Weg mit seiner Anwendung verbunden – ohne eben das gesamte Netzwerk für den Zugriff zu öffnen. Jeder Mitarbeiter kann durch die Berücksichtigung des Konzepts des Least Privilege nur auf die Daten zugreifen, die er für seine Arbeit wirklich benötigt, so dass dem Bestreben mach dem Minimalprinzip der Zugriffsberechtigungen gerecht wird. Da für diese Art der Zugangsberechtigungen auf Applikationsebene kein Netzwerkzugang mehr benötigt wird, lassen sich traditionelle Angriffsvektoren ausschalten.

**Marc Lueck, EMEA CISO, Zscaler**

ZTNA legt die Grundlage für ein umfassendes neues Connectivity- und Sicherheitskonzept, dass durch die Kombination von Identifikationstechnologie und Kontrollmechanismen aus der Cloud entsteht. Als positiver Nebeneffekt steigt auf diese Weise die Geschwindigkeit der Anbindung von Remote-Mitarbeitern deutlich, weil das Rechenzentrum als Security-Flaschenhals wegfällt und zusätzlich sinken die Kosten, da auf MPLS-Bandbreite verzichtet werden kann. Stattdessen dient der lokale Internet-Übergang als Weg zur Cloud, die die Policies der Zugriffsberechtigungen brokert und Sicherheits-Hardware obsolet macht.

Oberstes Ziel: Vermeidung von Angriffsflächen

An Multi-Layer-Security führt kaum ein Weg vorbei, wenn ein Unternehmen seine im Internet exponierte Angriffsfläche reduzieren möchte. Wenn die Infrastruktur nicht mehr im Internet für Angreifer sichtbar ist, können auch keine Attacken mehr gestartet werden. Besonders die Zunahme von Fernarbeit – und damit von Mitarbeitern, die von verschiedenen Standorten mit manchmal unzureichend gesicherten Geräten auf die Unternehmensdaten zugreifen möchten – spricht für die Transformation der Sicherheitsinfrastruktur. Durch ZTNA als Bestandteil einer Multilayer Sicherheitsstrategie lässt sich die Wahrscheinlichkeit eines erfolgreichen Angriffs noch einmal deutlich reduzieren.

Marc Lueck

## Den steigenden Bedarf an Managed Security Services gezielter decken

Angesichts der verschärften Bedrohungslage durch immer mehr Cyberattacken steigt im Unternehmensumfeld die Nachfrage nach externen IT-Security-Dienstleistern. Diese neue Dynamik im Markt für Managed Security Services (MSS) weckt nun auch zunehmend das strategische Interesse vieler Hersteller. Sie bewegen sich auf die MSS Provider zu, denn diese brauchen heute nutzerfreundliche, Cloud-native Tools an die Hand, um die unterschiedlichsten Umgebungen ausreichend abzusichern. Der Grundstein für die

Zusammenarbeit ist bereits gelegt – doch es gibt auch noch einige Hürden zu meistern.

Cyberkriminalität belastet die deutsche Wirtschaft immer mehr. Belief sich die Schadenssumme 2019 noch auf rund 100 Milliarden Euro, vermeldet der Bitkom im August 2021 ein neues Rekordhoch von mehr als 220 Milliarden Euro pro Jahr. Neun von zehn Unternehmen wurden laut der Umfrage des Digitalverbandes Opfer von Diebstahl, Spionage oder Sabotage. Erpressungen, Systemausfälle und Betriebsstörungen haben sich mehr als vervierfacht und bereits jedes zehnte Unternehmen sieht seine geschäftliche Existenz bedroht. Dabei gehen Hacker immer aggressiver vor und nutzen gezielt Schwachstellen von Drittanbietern aus, um sich Zugriff auf die Systeme möglichst vieler Unternehmen zu verschaffen.

**Wolfgang Kurz, CEO und Founder, indevis GmbH**

So infiltrierten Cyberkriminelle etwa eine Schwachstelle beim Software-Unternehmen Kaseya mit Ransomware und verschlüsselten die IT-Systeme der Kunden – darunter auch deutsche Unternehmen – und erpressten Lösegelder. Nach einem ähnlich perfiden Muster, das auf die Software-Lieferkette eines Drittanbieters zielte, lief Ende 2020 auch der Solarwinds-Hack ab, der vor allem staatliche US-Institutionen traf. Die Attacken auf eine zentrale US-Ölpipeline, das irische Gesundheitssystem sowie den weltgrößten Fleischproduzenten zeigten zudem, wie schnell auch die Versorgungssicherheit dahin sein kann.

Diese Aufzählung an Cyberattacken veranschaulicht, wie sich die Bedrohungslage zusehends zuspitzt. In der Folge steigt der Handlungsdruck für Unternehmen, ihre IT-Landschaften vor den Gefahren im Netz zu schützen. Software-Provider sollten etwa ihre Lieferketten durch eine strukturierte Deployment Chain mit Unit-Tests, automatischer Codeanalyse sowie einer besseren Updateversionsprüfung vor Manipulationen schützen. Auf der Software-Anwenderseite sollten Firewalls installiert sein, die eine Kommunikation zwischen Schadsoftware und Command-and-Control-Server der Hacker unterbinden. Dazu müssen die Firewall und ihr restriktives Regelwerk exakt konfiguriert sein.

**Sicherheitsverständnis und -bedarf**

Die Technik bildet allerdings nur eine Säule für die IT-Sicherheit. Denn diese stützt sich auch auf Prozesse, Organisation und Schnittstellen sowie Benutzer-Awareness. Um diese Punkte kümmern sich meist die Security-Teams in Unternehmen. Das Problem: Viele IT-Abteilungen gelangen hier an ihre Kapazitätsgrenzen. Denn sie sind meist aufgrund des Fachkräftemangels dünn besetzt. Daher lagern immer mehr Unternehmen ihre Sicherheitssysteme teilweise oder komplett aus. Auf diese Weise wächst der Bedarf an Managed Security Services (MSS) ständig. Im Markt steckt also viel Dynamik, von dem sowohl Hersteller als auch MSSP profitieren können. Das setzt jedoch ein gemeinsames Handeln im Sinne der Anwenderfirmen voraus, deren Sicherheitslücken es zu schließen gilt.

Um Missverständnisse vorzubeugen: MSS erhöhen das Schutzniveau auch bisher erheblich und werden das auch weiter tun. Die Bezieher erhalten in der Regel eine Ende-zu-Ende-Lösung, die vom Provider exakt auf ihre Bedrohungssituation zugeschnitten wird. Ein solches Vorgehen verlangt vom Dienstleister, die besten Security-Produkte auszuwählen und weiterzuentwickeln. Gehostet werden die aufeinander abgestimmten Sicherheitstechnologien im Rechenzentrum des MSS-Beziehers oder in der Cloud. Der MSSP installiert und betreibt die Technik auf Wunsch auch im Rund-um-Service. Dieses Prinzip bleibt so bestehen.

**Hersteller und Provider reden über besseren Service**

Der wachsende MSS-Bedarf wird nun jedoch auch für die Hersteller immer interessanter. Sie stufen das Segment als strategisch wichtig ein und setzen so einen offenen Dialog mit den spezialisierten Dienstleistern in Gang, der seit geraumer Zeit läuft. Gesprächsbedarf besteht in erster Linie deshalb, weil sich die Bedingungen, unter denen die Sicherheitstechnologien genutzt werden, verändert haben. Die typische Hersteller-Anwendung, die On-Premises läuft, richtet sich an den Administrator beim Kunden. Diese IT-Fachkraft steuert den Betrieb einer Ende-zu-Ende-Lösung heute nicht mehr allein, sondern eben in vielen Fällen gemeinsam mit dem MSSP-Team. Das geschieht am besten über eine zentrale Konsole. Die Cloud-Fähigkeit der Anwendungen gewinnt daher enorm an Bedeutung, die der bisherige Designansatz ausblendet. Fakt ist: Das Cloud-Hosting gehört heute unbedingt dazu, um die richtige Kombination aus Sicherheitsfunktionen und Betriebsmodell für eine Firma zu finden und aufzusetzen. Doch auch wenn Hersteller intensiv an einem Cloud-ready-Portfolio arbeiten, unter anderem erkennbar an den Zukäufen von Cloud-Providern, benötigt dieser Prozess Zeit, um alle nötigen Funktionen in der Cloud abzubilden.

**An gängigen Abrechnungsmodellen orientieren**

Die verstärkte Cloud-Nutzung hat weitere Konsequenzen, denen sich die Gesprächspartner widmen sollten. So stellen aus MSSP-Sicht Mandantenfähigkeit und Management-Funktionen Kriterien dar, an denen sich entscheidet, wie Cloud-native eine Anwendung ist. Zudem funktionieren Cloud-Dienste in der Regel nach dem Pay-as-you-use-Prinzip. Aus diesem Grund sollten sich die Hersteller von den bis dato üblichen 10er-Paketen, Mindestumsatzvorgaben und Startgebühren schnell verabschieden. Es gilt also, neue Billing-Tools für einen flexiblen Cloud-Konsum zu entwickeln, über die klar und fair abgerechnet werden kann.

**Beziehungspflege zahlt sich sicher aus**

Zum Sicherheitsgewinn müssen Kunden aber auch selbst beitragen. Sie stehen in der Pflicht, intern pas-

sende Strukturen zu schaffen, an die MSSP andocken und die Hersteller-Instrumente schärfen können. Darüber hinaus empfiehlt es sich, dass Inhouse-IT-Experten ihre Rolle neu definieren. In Zeiten komplexer und vielschichtiger IT-Landschaften können interne IT-Administratoren nicht überall selbst Hand anlegen. Vielmehr sollten sie sich als „Business Enabler" der Fachabteilungen verstehen, wozu ihnen die externen Spezialisten die Freiräume verschaffen. Im Alltag funktioniert das Miteinander von IT-Abteilung und MSSP-Team am besten, sobald alle das Prinzip der geteilten Verantwortung verinnerlichen und sich gegenseitig vertrauen. Bestimmte Sicherheitsvorfälle lassen sich nur lösen, wenn Detailwissen zu IT-Systemen oder Teilprozessen abrufbar ist – vom IT-Team des MSS-Beziehers. In dem Fall entfaltet die Sicherheitstechnologie die gewünschte Wirkung, an der Anwender, Dienstleister und Hersteller gleichermaßen interessiert sind.

Wolfgang Kurz

# 1.4 ARBEITSWELT

## Weckruf Cybersicherheit: Wie viele Vorfälle braucht es noch?

Sicherheitsvorfälle wie jüngst die Sicherheitslücke von Exchange-Servern, rufen gezielte Cyber-Angriffe hervor, stören Betriebsabläufe und können immensen Schaden verursachen. Im speziellen Fall wird geraten, davon auszugehen, dass betroffene IT-Infrastrukturen kompromittiert sind. Der Vorfall zeigt aber auch, wie nachlässig mit Cybersicherheit noch umgegangen wird – häufig fehlen sogar die Security Basics. Einige Unternehmenslenker stecken nach wie vor den Kopf in den Sand und hoffen, dass alles gut geht. Cyber Security ist aber keine Frage des Geschmacks und muss dringend zur Chefsache werden. Security-Verantwortliche sollten jetzt ihre Cyber Security auf den Prüfstand stellen und die dringend notwendigen Schutzmaßnahmen ergreifen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nach dem Microsoft Exchange-Hack Anfang März 65.000 Server identifiziert, die gefährdet sind. Diese lassen sich beispielsweise für Datendiebstahl missbrauchen. Am 16. März warnte das BSI, dass 10.000 Server noch nicht gepatcht sind. Eine Woche später lieferte die Softwarefirma F-Secure weitere Zahlen. Demnach wurden weniger als 50 Prozent der Sicherheitspatches eingespielt.

Der Vorfall zeigt Parallelen zur Citrix-Schwachstelle, vor der das BSI im Januar 2020 warnte. Im September sorgte die Attacke auf die Universitätsklinik Düsseldorf für Schlagzeilen. Beide Fälle verbindet: Wird zu spät gepatcht, können Cyberkriminelle entweder direkt attackieren oder in Ruhe Hintertüren für ihre Ransomware installieren und später angreifen. Dabei lassen sich Krypto-Trojaner und andere Schadsoftware mit End Point Detection und Security Information and Event Management (SIEM) aufspüren, bevor sie Schaden anrichten können.

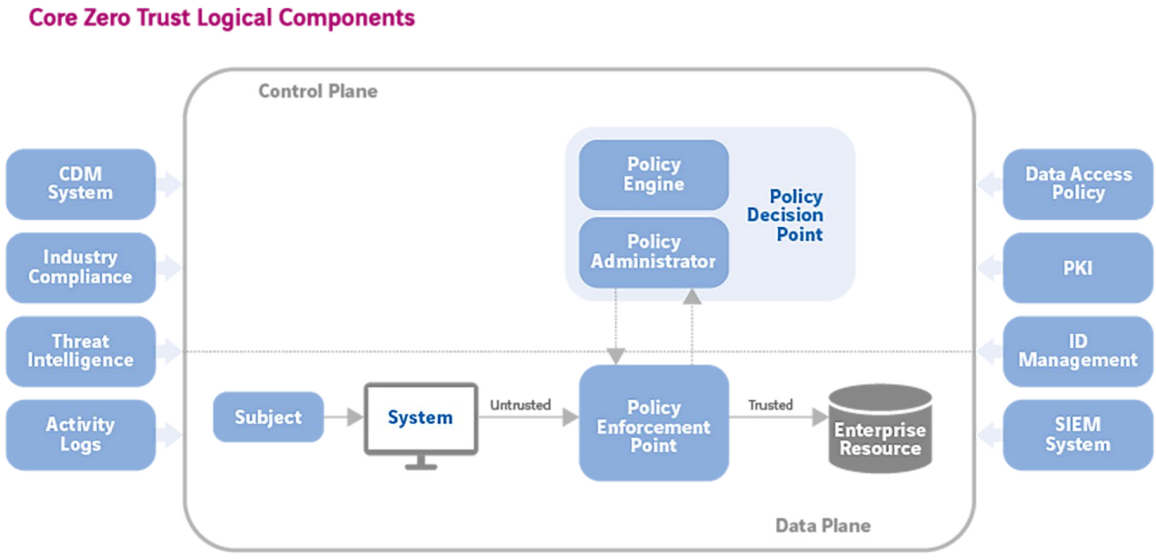
**Wie wappnet man sich gegen Schwachstellen?**
Sind Server über das Internet zugänglich, gibt es Security Basics, um die sich Unternehmen kümmern müssen. Exponierte Systeme können durch ein Intrusion Prevention System (IPS) sowie eine Web Application Firewall vor Eindringlingen geschützt werden, während Next-Generation-Antiviren-Software die Infektion mit Ransomware verhindert. Diese Technologien wären schon geeignet, um ein Eindringen zu erkennen und die Installation einer Backdoor möglichst zu verhindern. Die nötigen Sicherheitstechnologien komplettieren Schwachstellen- sowie Patchmanagement, Penetration Testing sowie SIEM. Es handelt sich dabei um erprobte Cyber-Security-Bausteine, die jedes Unternehmen eigentlich längst implementiert haben sollte.

Aber trotz prominenter Sicherheitsvorfälle wird Cyber Security noch nicht die Bedeutung beigemessen, die sie haben sollte. Nur selten wissen Entscheider über den Sicherheits-Status in ihrem Unternehmen Bescheid und können die richtigen Maßnahmen einleiten. Auf dem Weg zur widerstandsfähigen IT-Infrastruktur für Unternehmen, helfen diese fünf Schritte:

**1. Cyber-Security-Check als Bestandsaufnahme**
Am Anfang steht eine Reifegrad-Messung der firmeneigenen Cyber Security. Diese kann man sich vorstellen, wie eine Inspektion beim Auto: Cyber-Security-Experten öffnen die Motorhaube und schauen nach, was sich darunter verbirgt.

Anschließend bekommt das Unternehmen eine Einschätzung, wo es in Bezug auf die wichtigsten Cyber-Security-Aspekte steht und wo dringendes Handeln erforderlich ist. Einen ersten Selbsttest können Sicherheitsverantwortliche sogar online machen. So ein Cyber-Security Check zeigt anhand von Fragen zu Awareness/Prevent, Detect, Protect, Response, Recover, Compliance, Manage/Control, und Identity, einen ersten Wasserstand. Die Verortung dauert nur wenige Minuten und gibt gute erste Anhaltspunkte für die wichtigsten Sicherheitsmaßnahmen. Dazu kann beispielsweise eine Schwachstellen-Management-Lösung zählen.

**Ben Kröger, Technische Leitung Cyber Security, Axians IT Security**




Bildbeschreibung: Eine ZTA besteht aus zahlreichen logischen Komponenten, die On-Premises oder Cloud-basiert betrieben werden können. Zur Kommunikation verwenden sie eine separate Management Ebene (Control Plane), während die Anwendungsdaten über die Data Plane kommunizieren.


**2. Regelmäßige Penetration-Tests zeigen Schwachstellen auf**

Um die eigene Angriffsfläche zu minimieren, haben sich Penetration-Tests bewährt. Automatisierte Pentest-Plattformen fokussieren sich auf Bedrohungen von innen und außen und ahmen einen Hackerangriff nach, wodurch Schwachstellen aufgedeckt werden. Anwender erhalten detaillierte Berichte mitsamt Vorschlägen für Sicherheitsmaßnahmen. Es empfiehlt sich, solche Tests regelmäßig durchzuführen. So kann kontinuierlich priorisiert werden und die Cyber Security verbessert sich laufend, zumal Pentests tiefgehender sind als ein gängiges Schwachstellenmanagement.

**3. Ein SIEM installieren – und handeln**

Es kommt häufig vor, dass Unternehmen gar nicht mitbekommen, wenn es einen Sicherheitsvorfall gegeben hat. Ein SIEM ist ein automatisiertes Frühwarnsystem für die IT, das sich genau darum kümmert. Es sammelt, analysiert und kategorisiert Informationen aus der gesamten IT-Infrastruktur. Dabei werden Anomalien und Abweichungen erfasst und bewertet, um sicherheitsrelevante Vorfälle zu erkennen. Hierfür ist die Implementierung einer Bedrohungserkennung mit NDR (Network Detection and Response), EDR (Endpoint Detection and Response und XDR (Extended Detection and Response) für ein Frühwarnsystem bei der aktuellen Bedrohungslage eine dringende Empfehlung für jedes Unternehmen.

Die reine Alarmierung ist aber lediglich die halbe Miete. Anschließend muss auf die Bedrohung reagiert werden. Für Unternehmen, die dies nicht selbst bewerkstelligen gibt es Services erfahrener Anbieter. Dabei schützen in einem Security Operations Center (SOC) spezialisierte Teams aus Cyber-Security-Analysten, Pentestern, digitalen Forensikern und Hacking-Experten die Systeme der Kunden rund um die Uhr.

**4. Einen Incident-Response-Plan aufstellen**

Bei einem Sicherheitsvorfall zählt vor allem die schnelle Reaktion. Deshalb sollten Unternehmen schon im Vorfeld in einem Incident-Response-Plan festlegen, wie organisatorisch und technisch zu reagieren ist. Ziel ist, eine Cyber-Attacke so einzudämmen, dass der Schaden so gering wie möglich ausfällt. Eine typische Reaktion auf einen Vorfall (Incident Response) durchläuft sechs Phasen. Vorbereitung, Vorfallerkennung, Eindämmung, vollständige Beseitigung, Wiederherstellung und gewonnene Erkenntnisse. Entscheidend für die umfassende Planung ist es, jeden Vorfall und jedes System individuell zu betrachten und die Reaktion darauf anzupassen.

**5. Den „Zero Trust"-Ansatz im Blick**

Sobald die Security-Basics stimmen, sollten Unternehmen sich um weitere Themen kümmern. Besonders im Fokus steht derzeit das Thema Zero Trust Architektur

(ZTA). Dieser Ansatz setzt auf das „Prinzip Misstrauen“. Einfach gesagt sollte jedes Unternehmen davon ausgehen, dass es bereits kompromittiert wurde. Der entscheidende Grundsatz lautet, dass das gesamte Unternehmensnetzwerk als nicht-vertrauenswürdige Zone betrachtet wird. Kommunikation darf immer nur auf die sicherste Art und Weise erfolgen. Dazu gehört die Authentifizierung aller Verbindungen und die Verschlüsselung des gesamten Datenverkehrs. Auch können Remote-Objekte und Assets ihrer lokalen Netzwerkverbindung nicht vollständig vertrauen – sie sollen davon ausgehen, dass das nicht unternehmenseigene Netzwerk stets feindlich gesinnt ist. Dieses Vorgehen schützt insofern, da nur gültige Anfragen an Servern akzeptiert werden – auch wenn es eine Schwachstelle wie bei Exchange gibt.

**Cyber Security ist keine Ansichtssache, sondern das Gebot der Stunde**

Noch sind Cyber-Bedrohungen in vielen Unternehmen unsichtbar und Entscheider sind deshalb häufig der Ansicht, dass sie gut gewappnet seien. Diese Einschätzung bleibt vielleicht noch eine Weile ohne gravierende Folgen. Es ist jedoch sehr riskant und gleicht der Fahrt in einem kaputten Auto – nach dem Motto: „Der Wagen fährt schon noch ein Stück“. Nur um zu sagen, wie lange noch, müsste man wissen, was dringend repariert gehört. Es ist also keine Ansichtssache mehr, sondern das Gebot der Stunde, endlich gegenzusteuern, damit es nicht zum Crash kommt.

Ben Kröger

## Wie Cyber Security der Zukunft aussieht

Auf künstlicher Intelligenz basierende Cyber Security Tools sind mittlerweile keine Zukunftsmusik mehr. Diese laufen innerhalb eines Security Operations Center (SOC) zusammen und sind durch ihre hochmoderne Ausrichtung auch für neuartige Angriffe gewappnet. Die innovativen Lösungen stellen eine unverzichtbare Stütze für SOC-Analyst:innen dar und ebnen Cyber-Security-Technologien der Zukunft den Weg.

In Unternehmen haben sich in vielen Bereichen bereits KI-basierte Lösungen etabliert, deren Unterstützung längst nicht mehr wegzudenken ist. Auch im Bereich der Cyber Security sind KI-basierte Lösungen unverzichtbar geworden. So gilt es, sich vor allem vor groß angelegten Cyberattacken, die von langer Hand geplant wurden, zu schützen und verteidigen zu können. Vollumfängliche Schutzstrategien und -konzepte bietet ein Security Operations Center (SOC). Es vereint sämtliche Cyber Security Services und nutzt dazu auch künstliche Intelligenz mit den dahinter liegenden Technologien wie Machine Learning und dessen Fähigkeiten zum Deep Learning. Durch die Kompetenz der Programme sich dauernd weiterzuentwickeln und neue Dinge zu erlernen, unterstützt es die Analyst:innen bei ihrer täglichen Arbeit essenziell. Ein SOC wird üblicherweise durch Spezialist:innen betreut. Mit ihrer Expertise in Kombination mit State-of-the-Art-Sicherheitstechnologien garantieren sie in Bezug auf Cybersicherheit die Zukunftsfähigkeit eines Unternehmens.

**Keine Chance für Kriminelle – mit diesen KI-basierten Tools**

Heute führt für Unternehmen kein Weg mehr daran vorbei sich mittels eines Security Operations Center vor Hackerangriffen zu schützen. Dabei wird die Expertise und das Know-how der Cyber-Security-Fachkräfte durch ein Security Information and Event Management (SIEM) und weitere KI-Tools ergänzt. Innerhalb des SIEM fungieren unterschiedliche Softwarelösungen, die auf künstlicher Intelligenz basieren, als Analysewerkzeuge. Diese beobachten das Verhalten von Anwendern oder Geräten im Netz und reagieren auf Anomalien, die sie gefunden haben. Zu diesen Tools gehören unter anderem das Modul für User and Entity Behavior Analytics (UEBA), Endpoint und Network Detection (EDR und NDR).

**Volker Scholz, Senior Security Architect, Axians IT Security**

**Anomalien identifizieren mit UEBA**

Cyberangriffe werden heute üblicherweise über viele Wochen und Monate hinweg aufwendig angelegt. Das SIEM selbst ist allerdings darauf spezialisiert sofort Eingriffe in das Sicherheitssystem in Echtzeit zu erkennen und zu melden. Um also auch über einen größeren Zeitraum langfristigen Schutz zu garantieren, unterstützt das Modul UEBA und ergänzt das SIEM umfassend. Durch ein innovatives Risikobewertungsverfahren und hochmoderne Algorithmen basiert es auf Regeln, denen Angreifer kaum ausweichen können. So ermöglicht das Modul Abweichungen und Diskrepanzen in der IT-Infrastruktur und bei User:innen aufzudecken. Darüber hinaus vergleicht UEBA das Verhalten der Anwender:innen mit dem einer ähnlichen Peer Group, um so noch mehr Informationen zum Verhalten der User:innen und Maschinen zu erlangen. Durch dieses gesammelte Wissen lässt sich mittels Machine Learning ein Modell aufstellen, das für die Abwehr künftiger Angriffe hilfreich sein kann.

**Vollumfängliche Analysen mit EDR und NDR**

SIEM beinhaltet außerdem Funktionen, um Anomalien auch innerhalb von Logdaten und Datenflüsse in Applikationen aufzudecken. Hier kommt ebenfalls wieder künstliche Intelligenz ins Spiel. So haben Systeme für Endpoint Detection and Response (EDR) zur Aufgabe, automatisiert nach Gefahren und Lecks an Endpunkten zu suchen. EDR sammelt und speichert dabei das Verhalten der Endgeräte und der damit verbundenen User:innen. Diese Informationen werden in


**Überblick zu den Aufgaben des SOC-Teams (Quelle: Axians)**

einer Datenbank zusammengetragen und können bei Bedarf auch für forensische Analysen genutzt werden. EDR prüft diese Daten anschließend auf die Evidenz von Schadsoftware. Darüber hinaus kann das System anhand der Verhaltensanalyse Angriffsversuche oder anderweitige atypische oder untersagte Aktivitäten erkennen und rechtzeitig mit automatisierten Gegenmaßnahmen reagieren.

Optimal ergänzt wird das EDR durch Systeme mit Network Detection and Response (NDR), die Abweichungen im Netzwerkverkehr identifizieren und festhalten. So werden Eindringlinge aufgespürt, sobald sie innerhalb des Netzwerks kommunizieren und es können automatisiert Reaktionen auf potenziell schädliche Aktivitäten im Netzwerk eingeleitet werden.

Zusammen mit UEBA optimiert der Einsatz von EDR und NDR das SIEM und garantiert einen vollumfänglichen Rundum-Schutz. Heutzutage kann so die gesamte Analyse und Abwehr bestmöglich ausgeschöpft werden.

### Erhöhte Sicherheit durch neuronale Netzwerke

Ein weiterer wichtiger Faktor im Kontext des SIEM sind Produkte wie beispielsweise QRadar von IBM. Eine KI wie IBM Watson Advisor hat die Möglichkeit, externe Informationen außerhalb des Unternehmens miteinzubeziehen und zu bewerten. So unterstützt die KI die SOC-Analyst:innen im Rahmen des Threat Hunting dabei, zusätzliche Daten über weitere Angriffspfade zusammenzutragen. Durch diese Zusammenarbeit von Mensch und KI können auch Angriffsversuche aufgedeckt werden, die innerhalb des eigenen Systems noch nicht als potenzielle Bedrohung vorlagen.

### Künstliche Intelligenz in der IT-Landschaft der Zukunft

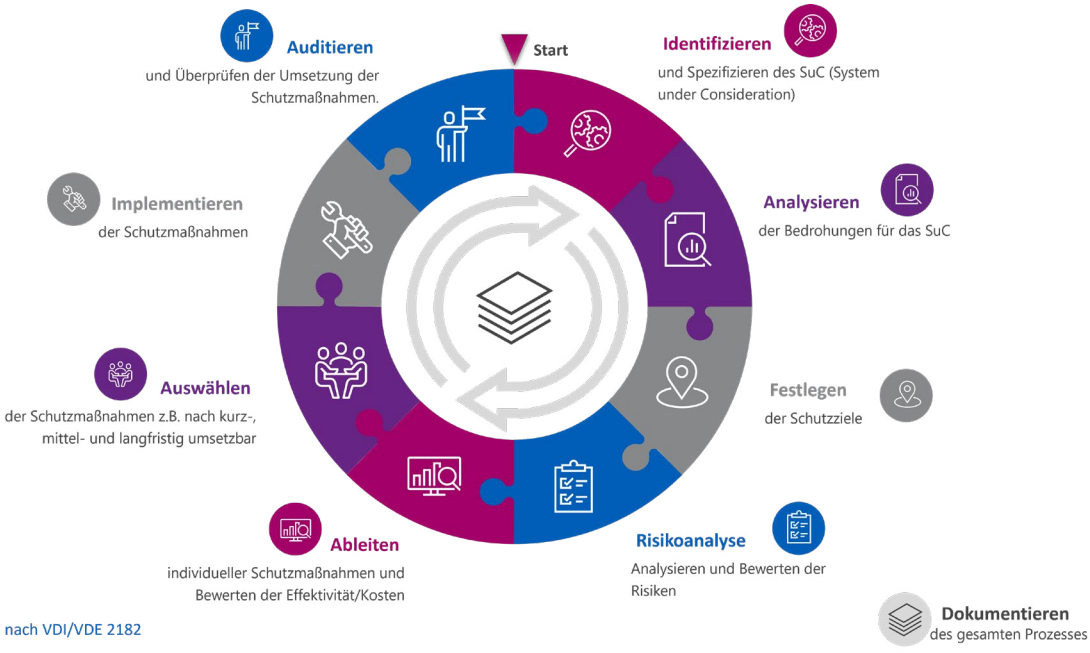
Selbst die kompetentesten Expert:innen stoßen ohne die Hilfe KI-basierter Tools an ihre Grenzen angesichts der immer komplexer werdenden IT-Infrastrukturen und der damit verbundenen zahlreichen Angriffsmöglichkeiten. Auch Kriminelle selbst machen von immer innovativeren Instrumenten und umfangreichen Algorithmen Gebrauch, sodass herkömmliche Sicherheitssoftware nicht mehr ausreicht. Intelligente Lösungen müssen her: Sie unterstützen die Cyber-Security-Fachkräfte dabei, potenzielle Gefahren zu erkennen, Bedrohungslagen adäquat einzuschätzen und schlussendlich bestmöglich darauf einzugehen und zu handeln. Besonders bei wiederkehrenden Aufgaben, die zur Routine gehören, helfen die KI-Lösungen immens. So ermöglichen die Programme durch die Anwendung künstlicher Intelligenz nicht nur mehr freie Kapazitäten für die IT-Mitarbeiter:innen, sondern garantieren auch ein höheres Sicherheitsniveau.

Für IT-Entscheider:innen ist es also unbedingt empfehlenswert, sowohl ein Security Operations Center als auch die dazugehörigen KI-Tools in der unternehmensinternen Cyber-Security-Strategie zu berücksichtigen. Dabei ist es aufwendig, eine eigene Inhouse-Lösung zu stemmen – nicht zuletzt, da ein 24/7 Support nötig ist, um rund um die Uhr Cybersicherheit zu garantieren. Hier kommen spezialisierte Dienstleister ins Spiel: Mit Leistungen wie SOC-as-a-Service können Unternehmen interne Ressourcen sparen und diese anderweitig sinnvoll einsetzen. Gleichzeitig garantieren die externen Cyber-Security-Expert:innen jederzeit auf dem neuesten Stand der Technik zu sein, um auch auf neuartige Cyberattacken reagieren zu können.

Volker Scholz

## Warum ein ganzheitlicher IT-/OT-Security-Ansatz wichtig ist

Aufgrund zunehmender Digitalisierung nimmt die Vernetzung auch im Produktionsumfeld zu. Damit steigt auch das Risiko für Angriffe auf industrielle




**Ablauf eines OT Security Risiko Assessment (Quelle: Axians)**

Steuerungssysteme. Das kann nicht nur gravierenden finanziellen Schaden anrichten, sondern im schlimmsten Fall Menschenleben gefährden. Was sollten Unternehmen tun, um sich zu schützen?

Bei OT, kurz für Operational Technology, denkt man zunächst an Produktionsanlagen. Tatsächlich umfasst der Begriff generell Systeme zur Steuerung und Überwachung von physikalischen Prozessen. Sie kommen nicht nur in der Industrie, sondern in nahezu allen Branchen zum Einsatz, zum Beispiel in der Trinkwasser- und der Stromversorgung oder der Gebäudeklimatisierung. Ohne OT wäre unser Leben, so wie es heute ist, nicht vorstellbar, denn sie liefert die Automatisierungstechnik, die für uns im Alltag selbstverständlich geworden ist.

Durch die Digitalisierung nimmt die Vernetzung zu. OT-Systeme sind nicht mehr nur untereinander, sondern auch mit IT-Systemen vernetzt. Die Konvergenz findet in beide Richtungen statt: In ERP-Systeme bspw. werden auch Produktionsinformationen hinterlegt und steuern Fertigungsaufträge in das MES (Manufacturing Execution System) ein, das MES wiederum sendet Betriebs- und Maschinendaten an das ERP zur Auswertung zurück. Das bedeutet: Angriffe auf die Server oder Datenbank des ERP wirken sich direkt auf die Produktion aus. Hinzu kommt, dass durch den zunehmenden Einsatz von Fernwartungssystemen für Maschinen und Anlagen zwingend eine Verbindung zum Internet benötigt wird. Sind diese Verbindungen unsicher umgesetzt oder werden selbst nicht regelmäßig gewartet, stellen sie eine Schwachstelle dar, die ausgenutzt werden kann. Dazu kommt das Risiko für Angriffe von innen, das selbst in isolierten Netzwerken besteht – etwa durch einen infizierten USB-Stick oder Laptop, den ein:e Mitarbeiter:in oder Service-Techniker:in anschließt. Tatsächlich rangiert das Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware auf Platz eins der Top-Ten-Bedrohungen für Industrial Control Systems (ICS), so eine Analyse des BSI.

### OT-Systeme sind besonders gefährdet

Sind Kriminelle einmal eingedrungen, können sie sich dank der weitreichenden Vernetzung von einem beliebigen Angriffspunkt aus in der gesamten IT-/OT-Umgebung bewegen, wenn entsprechende Schutzmaßnahmen fehlen. Mit jedem vernetzten Gerät wächst die Angriffsfläche. IT-Systeme in der Produktion bspw. sind meist besonders anfällig für Cyberattacken, weil sie häufig mit einem veralteten Betriebssystem betrieben werden, für das es keine Sicherheitsupdates mehr gibt. Gerade Angriffe auf OT-Systeme können gravierende Folgen haben. Hier geht es nicht nur um großen finanziellen Schaden, durch Anlagenstillstände und Reputationsverlust. Fehlfunktionen von Maschinen und Anlagen können auch Menschenleben gefährden, etwa wenn in einem Krankenhaus medizintechnische Geräte ausfallen oder die Strom- und Trinkwasserversorgung gefährdet sind. Unternehmen, die zu den kritischen Infrastrukturen zählen, unterliegen daher dem IT-Sicherheitsgesetz und müssen Mindeststandards für die Cyber Security sowie strenge Meldepflichten für Cybervorfälle einhalten.

**Timmi Hopf, Business Development Manager, Axians Deutschland**

### Gezielte und ungezielte Angriffe

Bisher sehen wir noch wenige Angriffe, die sich wirk-

lich gezielt gegen OT-Systeme richten. Häufig handelt es sich um breit gestreute Ransomware-Attacken auf IT-Systeme, bei denen Produktionsanlagen als Kollateralschaden mitbetroffen sind. So konnte im März dieses Jahres, aufgrund einer Ransomware-Attacke auf die IT-Systeme des Königsberger Unternehmens „Fränkische Rohrwerke", an weltweit 22 Produktionsstandorten eine Woche lang nicht produziert werden. Es ist leider davon auszugehen, dass es künftig mehr spezialisierte Angriffe auf Produktionsumgebungen geben wird. Denn diese sind für Kriminelle sehr lukrativ, sei es zur Erpressung oder Industriespionage und leider häufig noch schlechter geschützt als die Systeme der Unternehmens-IT.

**Das sollten Unternehmen tun**

Um sich zu schützen, sollten Unternehmen Cyber Security ganzheitlich betrachten und die Produktion in ihre IT-Sicherheitskonzepte zwingend integrieren und diese um die Anforderungen der OT erweitern. Die folgenden Schritte unterstützen dabei:

1. Awareness schaffen
   Arbeitsschutz- und Sicherheitsschulungen sind etablierte Maßnahmen, um die Sicherheitskultur in Unternehmen hochzuhalten. Der wahrscheinlich wichtigste Schritt, um mit den Herausforderungen der zunehmenden Vernetzung Schritt halten zu können, ist Mitarbeiterbefähigung bzw. -entwicklung. Mitarbeiter:innen mithilfe von Schulungen und Trainings für Cyber Security zu sensibilisieren, sollte auch im Produktionsumfeld regelmäßig durchgeführt werden.
2. Verantwortlichkeiten klären
   Um eine vollumfängliche Cyber Security Kultur im Unternehmen zu etablieren, müssen IT- und OT-Verantwortliche zusammenarbeiten. Häufig gibt es hier Herausforderungen in der Kommunikation, weil unterschiedliche Anforderungen aufeinandertreffen. Ein wichtiger Schritt besteht darin, Vertreter:innen beider Bereiche an einen Tisch zu holen, Verantwortlichkeiten zu klären und das gemeinsame Vorgehen zu definieren. Diese Zusammenarbeit muss durch das Management gefordert und gefördert werden. Die Unterstützung durch einen strategischen Partner welcher sowohl über IT- als auch OT-Expertise verfügt, kann dabei als wertvoller Katalysator wirken.
3. Ein Security Assessment durchführen
   Basis für ein vollumfängliches Cyber Security-Konzept bildet die Bewertung der aktuellen Sicherheits-Aufstellung. Dafür gilt es zunächst, die IT und OT im Produktionsumfeld zu analysieren und Schutzziele zu definieren. Welche Systeme sind an welchen Prozessen beteiligt? Wer kommuniziert mit wem? Welche Schwachstellen gibt es, wie groß ist das Risiko, dass diese Schwachstellen ausgenutzt werden können, und was kann im schlimmsten Fall passieren? Daraus ergibt sich eine Risikobewertung. Für die Durchführung eines Security Assessments empfiehlt sich die Zusammenarbeit mit einem externen Partner, der nicht nur strategisch beraten, sondern im Bedarfsfall als Implementierungs-Partner auch in die nahtlose Umsetzungs-Verantwortung gehen kann.
4. Technische und organisatorische Maßnahmen ableiten
   Aus den Ergebnissen des Security Assessment lassen sich schließlich konkrete technische und organisatorische Maßnahmen ableiten, um die definierten Schutzziele zu erreichen. Dabei können gängige Security-Standards wie ISO 27001 und IEC 62443 als Grundlage dienen. Als konkrete, technische Maßnahme ist zum Beispiel die Einführung eines Network-Monitoring-Systems empfehlenswert, das das Produktionsnetzwerk rund um die Uhr überwacht. Es schafft Transparenz über die Komponenten, die sich im Netzwerk befinden, und schlägt Alarm, sobald verdächtige Aktivitäten auftreten.
5. Einen Notfallplan erarbeiten und testen
   Wenn es einmal zu einem Angriff kommt, gilt es schnell zu reagieren und Schaden zu minimieren. Daher sollten Unternehmen einen Krisenreaktionsplan aufstellen, in dem Verantwortlichkeiten und Handlungsanweisungen klar definiert sind. Dazu gehört auch ein Backup-Plan, der regelmäßig überprüft werden sollte. Da jedes Umfeld anders ist und eine andere Kritikalität hat, muss ein Notfallplan immer individuell entwickelt werden. Damit er im Ernstfall auch funktioniert, sollte er regelmäßig getestet werden.

**Wie ein Pharma-Unternehmen seine OT-Security optimiert**

Ein Pharma-Unternehmen setzt Infrastrukturen, die ursprünglich für die IT geschaffen worden waren, zunehmend für die OT ein. Dadurch kam es zu Kompromissen bei Verfügbarkeit, Betrieb, Wartung und Funktionalität. Unterschiedliche Nutzungsprofile von IT und OT konnten nicht ausreichend abgebildet werden. Das Unternehmen beauftragte daher externe Cyber Security Spezialist:innen mit der Erneuerung der IT und OT Infrastruktur. Die Analyse ergab, dass zwei eigenständige Infrastrukturen aufgebaut und sicher miteinander verbunden werden sollten. Dabei richteten die Cyber-Security-Experten eine funktionale Zonierung und Segmentierung des OT Netzwerkes entlang der Produktionsanlagen ein und qualifizierten die OT-Infrastruktur nach industriespezifischen Richtlinien wie IEC 62443 und GxP. Heute verfügt das Unternehmen über zwei autarke, sichere Infrastrukturen für IT und OT und konnte die Compliance und Verfügbarkeit der Produktionssysteme signifikant verbessern.

**Fazit**
Cyber Security Lösungen einzusetzen muss wirtschaftlicher sein, als es nicht zu tun. Der erste Schritt ist ein professionelles Security Assessment, um zielgerichtet, den individuellen Handlungsbedarf zu identifizieren und zu priorisieren. Nur wenn Unternehmen die Anforderungen von IT und OT in einem vollumfänglichen Cyber-Security-Konzept berücksichtigen, können sie ihre hochvernetzten Umgebungen auch zukünftig nachhaltig und angemessen schützen.

Timmi Hopf

## Ein pragmatischer Ansatz zur Erhöhung der Cyber-Sicherheit und Widerstandsfähigkeit für Unternehmen aus Industrie und Produktion

Am ersten Juliwochenende startete einer der größten Hackerangriffe der vergangenen Jahre. Durch den Angriff auf den US-amerikanischen IT-Dienstleister Kaseya, dessen Software den Angreifern als Einfallstor zu weltweit über 1.000 Unternehmen diente. In Schweden mussten daraufhin 800 Supermarktfilialen für mehrere Tage schließen.

Wieder wenige Tage darauf, am 6. Juli 2021, attackierten Kriminelle das Computersystem eines Landkreises in Sachsen-Anhalt und legten das gesamte IT-System und damit kritische kommunale Arbeitsbereiche lahm. Unter anderem konnten keine Sozialleistungen mehr ausbezahlt werden. Daraufhin wurde zum ersten Mal in der Geschichte Deutschlands in einem Landkreis der Katastrophenfall aufgrund eines Cyberangriffs ausgerufen.

Und auch in diesem Jahr bezahlte das amerikanische Versicherungsunternehmen CNA Financial laut US-Nachrichtenagentur „Bloomberg“ die bisher größte bekannte Ransomware-Zahlung aller Zeiten - 40 Millionen Dollar.

Die drei Beispiele aktueller Cyber-Vorfälle sind aus mehreren Gesichtspunkten interessant. Sie sind nur die Spitze des Eisbergs, denn der Großteil der Angriffe findet statt, ohne dass die Öffentlichkeit jemals davon erfährt. Nach dem Report „Status Quo von Ransomware 2021“ des britischen IT-Security-Anbieters Sophos ist mehr als jedes dritte Unternehmen (37%) im letzten Jahr von Ransomware-Angriffen betroffen.

Einige andere Zahlen gefällig? Wie der Antivirus-Anbieter Emsisoft berichtet, ist die durchschnittliche Lösegeldforderung von gerade einmal 5000 US-Dollar im Jahr 2018 auf rund 200.000 US-Dollar im Jahr 2020 gestiegen; die durchschnittliche Ausfallzeit nach einem Angriff stieg gegenüber dem dritten Quartal 2020 um 11% und beträgt laut des amerikanischen Ransomware-Spezialisten Coveware 21 Tage.

Cyber-Bedrohungen sind also im Bewusstsein der breiten Bevölkerung angekommen und werden in den nächsten Jahren noch sehr viel stärker in den Vordergrund rücken. Bei Unternehmen mit breiter IT-Nutzung stellen IT-Risiken schon seit langem eine immer größer werdende Herausforderung dar. Nun scheint es, sind vor allem hochautomatisierte und stark vernetzte Produktions- und Industrieunternehmen ins Fadenkreuz der Angreifer gerückt. Werden sensible und geschäftskritische Produktionsstätten angegriffen und beeinträchtigt, fällt es vielen Unternehmen umso schwerer den Lösegeldforderungen der Kriminellen etwas entgegenzusetzen.

Und auch zukünftig ist kein Ende abzusehen: Wir schätzen, dass die weltweiten Gesamtkosten für Unternehmen als Folge dieser Attacken in diesem Jahr 15 Milliarden Euro übersteigen werden. Die Corona-Pandemie hat zudem dazu geführt, dass Remote- Worker Hauptangriffsziel von Ransomware-Attacken sind und ggf. als Einfallstor für Unternehmen und ggf. Produktionsanlagen dienen.

Doch was kann man dagegen tun? Wir möchten im nachfolgenden auf einige mögliche Maßnahmen hinweisen, die wir in diesem Jahr ausführlich in unserem „Industrial Cyber Security Handbook“ beschrieben haben:

1. **Denken Sie vielschichtig** – Verstehen Sie Defense-in-Depth als zentrales Konzept, das Sie überall einsetzen können und sollten. Sei es im Einsatz unterschiedlicher Sicherheitslösungen in den unterschiedlichen Technologieschichten, in Form von Segmentierung und Zoning der einzelnen Netzwerke und Assetklassen oder indem Sie Ihr Sicherheitskonzept möglichst breit denken und aufstellen. Dies reicht vom physikalischen Schutz Ihrer Gebäude, Produktionslinien und Einzelkomponenten, über die zahlreichen technischen Möglichkeiten, bis hin zu Prozessen und Menschen in Form von Guidelines, Trainings und regelmäßigen Überprüfungsszenarien.
2. **Zentralisierung, Standardisierung und Automatisierung** – Die meisten Unternehmen stehen vor dem Problem, für den operativen Betrieb mit immer weniger Personal auskommen zu müssen. Dagegen hilft aus meiner Sicht nur eine Strategie: Versuchen Sie so viel wie möglich zu zentralisieren und zu standardisieren. Je weniger individuelle Prozesse, Tools und Tätigkeiten, desto mehr Zeit, Geld und Nerven sparen Sie. Der Aufwand und die Kosten für Cyber-Security Ihrer Produktionsstandorte darf sich nicht mit der Anzahl der Standorte multiplizieren, sondern muss effizient und zentral verwaltet werden können. Auch eine genaue Transparenz über externes Wartungspersonal und Lieferanten ist zwingend notwendig. Für diese und viele andere Herausforderungen gibt es bereits Standardtools, die einen guten Überblick, zentrales Management sowie maximale Transparenz und Nachvollziehbarkeit bieten.

**Stefan Pechardscheck, Global Head Technology, BearingPoint GmbH**

**Markus Seme, Geschäftsführer BearingPoint Österreich, Director Technology and Services, BearingPoint GmbH Österreich**

3. **Konfigurations- und Asset-Management** – Ein tragfähiges Konfigurations- und Asset-Management zählt zu den wichtigsten Aspekten, wenn es um Themen wie strukturierte Weiterentwicklung und Absicherung von Leit- und Automatisierungstechnik geht. Gerade bei größeren und komplexeren Umgebungen stößt eine Verwaltung mittels Excel oder eine, die rein auf manueller Erfassung basiert, schnell an ihre Grenzen oder skaliert schlichtweg nicht mehr. Noch dazu sind die Vorteile einer detaillierten und permanent aktuellen System- und Konfigurationsdokumentation nicht nur wichtig bei der Absicherung der Systeme. Auch Regeltätigkeiten wie Systemwartung, notwendige Ausbauten und erste Schritte in Richtung Industrie 4.0 sind ohne diese Daten-Basis nur schwer oder mit großem Risiko zu bewältigen. Wie die eingangs beschriebenen Cyber-Angriffe deutlich machen, bauen komplexere, cyber-physikalische Angriffe immer auf nicht-autorisierte Konfigurationsänderungen auf. Dabei sind oft nicht einmal Sicherheitslücken notwendig, sondern es wird Standardfunktionalität der Automatisierungstechnik quasi für ursprünglich nicht so vorgesehene Anwendungsfälle missbraucht. Wer also solche nicht-autorisierten Konfigurationsänderungen erkennen oder verhindern kann, kann sich auch vor solchen Angriffen wirksam schützen. Moderne, auf Leit- und Automatisierungstechnik spezialisierte Konfigurations- und Asset-Management-Lösungen, bieten neben dem automatisierten Erkennen von unautorisierten Konfigurationsänderungen oder dem Einbringen von nicht autorisierter Hardware in das überwachte Netzwerk, auch noch viele andere Features an. So werden zum Beispiel auch ungewöhnliche Zugriffe oder Datenflüsse auf Komponenten des Steuerungssystems gemeldet oder es können Wartungszugriffe von außerhalb, detailliert überwacht und eingeschränkt werden.
4. **Systematisch pragmatisch** – Da sich Technologien, Infrastrukturen und damit einhergehende Angriffsmöglichkeiten permanent weiterentwickeln, muss ein nachhaltiges Sicherheitskonzept ebenso kontinuierlich verbessert und auf vielen Ebenen angepasst werden. Zahlreiche Normen und Sicherheitssysteme wie die IEC 62443 oder das allgemeinere ISO 27001 adressieren genau diese Herangehensweise, der ganzheitlichen und kontinuierlichen Verbesserungszyklen, sind aber relativ aufwändig in der Umsetzung, wenn man die enthaltenen Empfehlungen und Vorgaben in der vollen Breite mit praktischer und noch dazu betriebswirtschaftlicher Sinnhaftigkeit umsetzen möchte. Wie bei vielen anderen Ansätzen zeigt sich auch hierbei, dass eine Kombination von langfristiger und systematischer Planung, mit pragmatischem, betriebswirtschaftlich sinnvollem Vorgehen am effizientesten ist.
   Damit ist gemeint, dass Zeit und Geld primär dort einsetzt werden sollte, wo gemäß der 80/20 Regel am schnellsten die größtmögliche Verbesserung an Sicherheit geschafft werden kann. Bestenfalls lässt sich diese Verbesserung dann sogar quantitativ oder qualitativ messen. Gleichzeitig sollen diese Einzelmaßnahmen, sich gegenseitig ergänzend, gut in ein nachhaltiges Gesamtkonzept passen.
5. **Personelle Verantwortung und dediziertes Budget** – Der letzte und vielleicht sogar wichtigste Tipp ist: Richten Sie eine dedizierte personelle Verantwortung für die Cyber-Sicherheit Ihrer Produktionsstätten ein. Wo diese Person oder dieses Team organisatorisch angesiedelt ist, ist dabei nicht so wichtig wie die Anforderung, dass sie unbedingt, zumindest grundlegende Kenntnisse in der Leit- und Automatisierungstechnik mitbringen muss. Darüber hinaus sollte es sich um eine dedizierte Stelle handeln, das heißt um jemanden, der 100 % seiner verfügbaren Zeit dieser Tätigkeit widmen kann.

Eine Implementierung aller oder eines Großteils der beschriebenen Maßnahmen und konkreten Schutzmechanismen verhindert mit hoher Wahrscheinlichkeit die am Anfang des Beitrags beschriebenen Maßnahmen.

Zusammenfassen bleibt daher noch einmal folgendes Fazit festzuhalten:

Die meisten Angriffe, auch auf Industrieanlagen, sind weit weniger komplex als angenommen und mit weit weniger Fachwissen und Ressourcen ausgestattete Attacken. Gegen solche Gefahren ist man auch mit Basismaßnahmen, wie sie etwa die CIS Security Controls empfehlen, schon recht gut abgesichert.

Da sich ein individuelles Security Konzept in jedem Fall immer erst Schritt für Schritt entwickeln und vor allem auch weiterentwickeln muss, ist die Kombination von Basismaßnahmen, auf die dann entsprechend fortgeschrittenere Methoden aufgebaut werden können, ein sinnvoller Ansatz.

Das Wichtigste aber ist: Setzen Sie einen ersten Schritt und bleiben Sie dran!

Stefan Pechardscheck, Markus Seme

## Hybrides Arbeiten – welche Maßnahmen jetzt getroffen werden (sollten)

Eine aktuelle Studie zeigt, wie sich Arbeitgeber und -nehmer auf der ganzen Welt auf den digitalen Arbeitsplatz der Zukunft vorbereiten. Was Mitarbeiter zudem wissen müssen, um ihre Arbeitsumgebung im Homeoffice bestmöglich zu schützen.

Mit der Wiedereröffnung der Büros blicken viele auf die pandemiebedingte Fernarbeit als Fallstudie für die Einführung einer flexiblen, hybriden Arbeitsumgebung. Das Aufkommen neuer Varianten führt aber

auch bei Unternehmen zu neuen Unsicherheiten im Zusammenhang mit der COVID-19-Pandemie. Nun geht es darum, einen langfristigen Plan zu entwickeln – ein Arbeitsmodell, das den Bedürfnissen von Mitarbeitern und Geschäftsführung gleichermaßen gerecht wird. Egal, ob es sich dabei um Arbeitsplätze im Büro, im Homeoffice oder um hybride Konzepte handelt. Mit welchen Wünschen, Möglichkeiten und Problemen sich Führungskräfte und Angestellte in dieser Umbruchsphase konfrontiert sehen, hat Entrust in seiner aktuellen Studie „Securing the New Hybrid Workplace“ untersucht.* Ein besonderer Fokus lag dabei auf Fragen zur Absicherung von hybriden Arbeitsplätzen.

Zu den wichtigsten Ergebnissen der Studie gehören:

- Hybride Arbeitsmodelle setzen sich weltweit durch, trotz großer Sicherheitsbedenken: Die überwältigende Mehrheit der Unternehmen geht langfristig zu einem hybriden Arbeitsplatzkonzept über. In Deutschland geben 73 % der Führungskräfte und 85 % der Mitarbeiter an, dass ihr Unternehmen derzeit einen hybriden Ansatz fährt – oder vollständig remote arbeitet und ein hybrides Arbeitsmodell in Betracht zieht. Allerdings berichteten 51 % der Mitarbeiter von teilweise erheblichen Produktivitätseinbußen aufgrund von Problemen beim Netzwerkzugang. Führungskräfte nennen die mangelnde Sicherheit von Heimnetzwerken (21 %) und den Verlust sensibler Unternehmensdaten (16 %) als größte Sorge.
- Besuchermanagement gewinnt auch in Deutschland an Bedeutung: Detaillierte Aufzeichnungen darüber, wer in Büroräumen ein- und ausgegangen ist, haben 2021 eine hohe Priorität: 88 % der Führungskräfte und 87 % der Mitarbeiter halten ein System zur Aufzeichnung und Kontrolle des Besucherverkehrs während der Arbeitszeiten für wichtig.
- Die Datensicherheit im Home Office bringt neue Herausforderungen mit sich: Mitarbeiter arbeiten heute dezentraler als je zuvor, weshalb Unternehmen ihre Datensicherheitskonzepte anpassen müssen. Aber während 84 % der Führungskräfte bestätigen, dass ihr Unternehmen seinen Angestellten Schulungen zum Thema Datensicherheit angeboten hat, nahmen nur 57 % der Mitarbeiter Notiz davon – was auf eine erhebliche Kommunikationslücke hindeutet.

**Neue Möglichkeiten des hybriden Arbeitsmodells**

Die Studie unterstreicht mit einer überwältigenden Mehrheit von 91 % weltweit den Wunsch von Angestellten nach einem hybriden Arbeitsmodell. Es steht außer Frage, dass Arbeitgeber diesem Bedürfnis nachkommen. 61 % der befragten Führungskräfte in Deutschland gaben zudem an, dass sie bei der Neubesetzung freiwerdender Positionen die Einstellung von neuen Talenten an geografisch unterschiedlichen Standorten in Betracht ziehen. Neue Möglichkeiten sind gefragt, die Onboarding- und Einarbeitungsprozesse in einem hybriden Arbeitsumfeld abzusichern und zu verbessern.

Was die Absicherung des hybriden Arbeitens angeht, so erklären 84 % der Führungskräfte in Deutschland, dass ihr Unternehmen über eine Richtlinie oder einen formellen Leitfaden verfügt. 93 % geben an, dass in ihren Richtlinien bewährte Verfahren zur Datensicherheit und zum Datenschutz erörtert werden.

Dennoch gibt es viele Sicherheitsbedenken gegenüber hybriden Arbeitsmodellen, die sich zumeist auf das Homeoffice beziehen. So machen sich deutsche Führungskräfte Sorgen um:

- die Sicherheit der Internetverbindung im Zuhause ihrer Mitarbeiter: 21 %
- das Durchsickern sensibler Unternehmensdaten: 16%
- Cyberangriffe durch bösartige Akteure: 24%
- mangelhafte Datenschutzmethoden: 18%
- mangelnde Privatsphäre in der Wohnung: 6%
- Phishing-Angriffe: 6%
- unzureichende Passwortverwaltung: 4%
- Verstöße gegen die Vorschriften: 2%

Die Studie zeigt, dass deutsche Abteilungsleiter als Konsequenz ihre Schulungsmethoden verbessern (57 %), neue Tools für die Zusammenarbeit einführen (39 %) und mobile IDs für Mitarbeiter an entfernten Standorten ausstellen (37 %). Darüber hinaus ergreifen die Führungskräfte im Zusammenhang mit der Einführung hybrider Arbeitsmodelle technologische Maßnahmen zur Kontrolle der firmeneigenen IT-Sicherheit – insbesondere Lösungen für das Identity Access Management (IAM) sind unverzichtbar geworden. Zukunftsfähige IAM-Software muss hybride Umgebungen unterstützen, die sowohl On-Premise-Systeme als auch SaaS-Applikationen nutzen und Unternehmen in die Lage versetzen, nicht nur die Zugriffsrechte ihrer internen Mitarbeiter effektiv zu managen, sondern auch jene von Mitarbeitern in Remote-Arbeit und (bei Bedarf) von externen Partnern aus aller Welt.

36 % der deutschen Unternehmen implementieren Technologien für Einmalpasswörter, 43 % nutzen die biometrische Authentifizierung und 21 % eine mobile Identitätsüberprüfung, um Hackern einen Schritt voraus zu sein und interne Daten zu schützen. Im internationalen Durchschnitt liegen deutsche Unternehmen bei der Einführung zukunftsweisender Authentifizierungstools damit jedoch eher im hinteren Bereich.

**Besuchermanagement für mehr Sicherheit in der Büroumgebung**

In Zeiten der anhaltenden Pandemie müssen Unternehmen neben der physischen und IT-Sicherheit auch die Gesundheit ihrer Mitarbeiter am Arbeitsplatz in

* Insgesamt wurden 1.500 Führungskräfte und 1.500 Angestellte aus 10 verschiedenen Ländern befragt.

**Kieran Hernon, VP Digital Identity Sales EMEA & APJ, Entrust**

ihre Vorsichtsmaßnahmen einbeziehen. Die Studie von Entrust belegt eine überwältigende Unterstützung für ein umfassendes Besuchermanagement innerhalb von Organisationen: 89 % der deutschen Führungskräfte und 87 % der Angestellten sprechen sich für ein System aus, das Besucher innerhalb des Bürogebäudes protokolliert und kontrolliert.

Die Gründe für diesen verstärkten Kontrollwunsch von Besuchern sind in erster Linie auf die Vorsicht im Zusammenhang mit COVID-19 zurückzuführen. 80 % der Führungskräfte und 79 % der Mitarbeiter nennen das Risiko der Verbreitung von COVID-19 als wichtigsten Grund für die Einrichtung eines Besuchermanagementsystems. Weitere Gründe sind der Schutz vertraulicher Informationen (43 % der Führungskräfte und 55 % der Mitarbeiter) sowie die Vermeidung von Körperverletzungsdelikten (44 % der Führungskräfte und 28 % der Mitarbeiter).

**Steigendes Bewusstsein für Datenschutzbelange**

Lange galt es als schwierig, Heimarbeit mit den unternehmensweiten Datenschutzrichtlinien in Einklang zu bringen. Hier scheinen die pandemiebedingten Maßnahmen zu einem Schritt in die richtige Richtung geführt zu haben: 84 % der deutschen Führungskräfte geben an, dass ihr Unternehmen Mitarbeitenden Schulungen zur Datensicherheit angeboten hat – für die überwältigende Mehrheit ist dies als Folge der COVID-19-Pandemie geschehen. Mithilfe von Schulungen können Unternehmen das Risiko von Sicherheitsbedrohungen wie Phishing- und Ransomware-Angriffen drastisch reduzieren, da diese das mangelnde Bewusstsein ihrer Adressaten ausnutzen.

Leider waren sich nur 57 % der Mitarbeiter bewusst, dass ihr Unternehmen Schulungen zum Thema Datensicherheit anbietet – was auf eine mangelnde Kommunikation in diesem Bereich hinweist.

**Globale Perspektive**

Im internationalen Vergleich sind Studienergebnisse aus einzelnen Ländern besonders interessant. Zu den wichtigsten internationalen Trends und Erkenntnissen gehören:

- Unternehmen in Saudi-Arabien (89 %) und den Vereinigten Arabischen Emiraten (87 %) sind am ehesten bereit, für neu zu besetzende Positionen Talente aus der ganzen Welt zu berücksichtigen. Gefolgt von Unternehmen in den Vereinigten Staaten und Singapur. Hier geben jeweils 73 % der Führungskräfte an, dass sie sich vorstellen könnten, neue Mitarbeiter unabhängig von deren Standort einzustellen.
- Unternehmen in Indonesien integrieren besonders häufig modernste Sicherheitstechnologien in ihre bestehenden Geschäftsabläufe: 75 % der Arbeitgeber geben an, dass sie Einmalpasswörter verwenden, 69 % nutzen biometrische Authentifizierungsmethoden.
- 65 % der Arbeitgeber in Japan waren sich einig, dass sie Datensicherheitsschulungen für das hybride Arbeitsmodell angeboten haben. Aber nur 36 % der Arbeitnehmer stimmen dem zu, was auf mögliche Probleme bei der Durchführung von Schulungen hinweist.

**So können Sie Ihre hybride Arbeitsumgebung optimieren:**

Unter Berücksichtigung der größten Sorgen vieler Führungskräfte und Mitarbeiter weltweit möchten wir Ihnen folgende, einfach umzusetzende Sicherheitstipps mit auf den Weg geben. So können Sie dazu beitragen, dass IT-Systeme auch im Homeoffice geschützt und Daten sicher bleiben:

- Erstellen Sie eine separate, sichere Internetverbindung für ihre Arbeitsbelange. Die meisten zeitgemäßen Internet-Router für Privatkunden bieten die Möglichkeit, mehr als ein drahtloses Netzwerk einzurichten. Mitarbeiter können so ein separates Netzwerk mit einer höheren Sicherheitsstufe aufsetzen (z. B. unsichtbare SSID, aktiviertes VPN, komplexe Kennwörter usw.).
- Verwenden Sie nur zugelassene Cloud-Dienste. Wenn eine Frist abläuft oder ein Kunde verärgert ist, kann es verlockend sein, unter Zuhilfenahme externer Dienste schnell die notwendige Anfrage zu erledigen. Ob es sich dabei um die Nutzung einer „kostenlosen“ Online-Ressource handelt, um eine Präsentation aufzupeppen, oder um das Hochladen von Inhalten in einen nicht genehmigten Dateifreigabedienst, weil sie zu groß für E-Mails sind – all diese Dienste werden nicht von der Unternehmens-IT geprüft und stellen eine Sicherheitslücke dar.
- Halten Sie Richtlinien für Passwörter ein. IT-Abteilungen können mit Identity- und Access-Management viel dazu beitragen, dass Benutzer und ihre Daten sicher bleiben. Mitarbeiter müssen ihnen aber auf halbem Weg entgegenkommen, indem sie ihre Passwörter sicher verwalten, ihre Geräte regelmäßig updaten und konform mit den Unternehmensrichtlinien halten.
- Trennen Sie berufliche und private Aktivitäten. Einer der Vorteile des Homeoffice ist die Möglichkeit, während der Pausen persönlichen Besorgungen und Erledigungen nachzukommen. Ganz gleich, ob es sich um Online-Shopping, soziale Medien oder persönliche E-Mails handelt: wenn Sie Ihren privaten Laptop, Ihr Tablet oder Ihr Telefon zur Hand haben, ist es besser, alle persönlichen Online-Aktivitäten auf diese Geräte zu beschränken – und damit sicherzustellen, dass die Arbeitsgeräte frei von Cyberangriffen bleiben, die über persönliche Konten erfolgen könnten.

**Über die Studie „Securing the New Hybrid Workplace"**

„Securing the New Hybrid Workplace" ist eine Studie des Ponemon Instituts im Auftrag von Entrust mit 1.500 Führungskräften und 1.500 Mitarbeitern aus den Vereinigten Staaten, Kanada, Großbritannien, Australien, Deutschland, Saudi-Arabien, den Vereinigten Arabischen Emiraten, Indonesien, Japan und Singapur. Die Daten wurden im Laufe des Jahres 2021 erhoben. Die Studie untersucht aktuelle Themen wie Best Practices für hybrides Arbeiten, Besuchermanagement in Bürogebäuden und den Einfluss hybrider Arbeitsmodelle auf die Sicherheit am Arbeitsplatz.

Kieran Hernon

# 1.5 REAKTIONEN

## Cybersicherheit braucht Digitalisierung … oder andersherum?

Eine erfolgreiche Digitalisierungsstrategie von Unternehmen braucht eine angemessene Cybersicherheit. Daraus lässt sich ableiten, dass eine Cybersicherheitsstrategie eine digitale Cybersicherheitsstrategie sein muss, sich am Geschäftsmodell und Digitalisierung ausrichten muss. Und weil die Dynamik der Digitalisierung hoch ist, ist die Verbindung dieser zwei Themenbereiche umso wichtiger.

Das Bundeskriminalamt hat in ihrer Sonderauswertung im Rahmen der Corona-Pandemie die Beschleunigung der Nutzung digitaler Dienste hervorgehoben.

„Die Gesellschaft weicht im Zuge der Corona-Krise vermehrt auf die digitale Welt aus - ein perfekter Nährboden für Cyberkriminelle." (BKA, Cybercrime in Zeiten der Corona-Pandemie, 30. September 2020). Die zunehmende Digitalisierung erfordert als logische Konsequenz, kontinuierlich und besser auf Cyberangriffe vorbereitet zu sein.

Diese Entwicklung zeigt, dass der Ansatz, Cybersicherheit und Digitalisierung zu verknüpfen sinnvoll und erfolgversprechend ist. Damit wird Cybersicherheit aus der Expertennische herausgeführt, ganz so, wie immer deutlicher wird, dass Digitalisierung ebenfalls kein reines Expertenthema sein darf. Diesen Gedanken konsequent weitergedacht, bedeutet es vielmehr, dass eine Haltung gegenüber der Cybersicherheit in Unternehmen gebraucht wird, die Cybersicherheit als Teil des Business versteht und nicht als Tradeoff zum Business – Cybersicherheit ermöglicht Digitalisierung.

Denn so, wie Digitalisierung ein kontinuierlicher Prozess ist, ist auch Cybersicherheit ein Aufgabenfeld, welches Unternehmen stetig weiterentwickeln müssen. Ein „Fertig" wird es weder in der Digitalisierung noch in der Cybersicherheit geben - es sind Daueraufgaben.

Es lassen sich weitere Verbindungen zwischen den Anforderungen an eine Organisation für erfolgreiche Digitalisierung und für erfolgreiche Cybersicherheit ziehen. So entsteht eine verstärkende Wechselwirkung zwischen Cybersicherheit und Digitalisierung.

**Aspekte der Digitalisierung**

Beispielhaft soll die Studie des Instituts der deutschen Wirtschaft für Anforderungen der Digitalisierung herangezogen werden. In der Studie (IW, Digitalisierung und mitarbeiterorientierte Führung, 2020) werden drei Megatrends für Digitalisierung aufgezeigt.

1. Zeitliche und räumliche Flexibilität von Beschäftigten
2. Automatisierung, Informatisierung und künstliche Intelligenz
3. Veränderung, Verantwortung, Vertrauen in der Führung

Veränderte mobilere Arbeitsformen sorgen für einen höheren Grad an Handlungsfreiheit und daraus resultierend für mehr Selbstkontrolle und -steuerung, möglicherweise aber auch für eine zunehmende Verunsicherung. Dies zusammen mit der fortschreitenden technologischen Entwicklung sorgt für veränderte Kompetenz- und Aufgabenbereiche. Insbesondere sind Veränderungsbereitschaft und Kreativität erforderlich, um die Innovationskraft von Unternehmen aufrechtzuerhalten und auf sich verändernde Marktentwicklungen schnell und angemessen reagieren zu können. Innovation entsteht durch ausprobieren und Mut, verbunden mit einer konstruktiven Fehlerkultur, in der Fehler frühzeitig erkannt werden und eine korrigierende Reaktion erfolgt.

Überträgt man diese Konsequenzen auf die Anforderungen für Cybersicherheit, so wird deutlich, dass Cybersicherheits-Kompetenz bei jedem einzelnen wichtig ist. Bei der zunehmenden Handlungsfreiheit ist es erforderlich, mögliche Risiken und Grenzen einschätzen zu können, also in der Lage zu sein, Dinge kritisch zu hinterfragen. Digitalisierungskompetenz und Cybersicherheitskompetenz haben also ähnliche Anforderungen, in der eigenverantwortliches Handeln einen wichtigen Teil ausmacht.

**Die veränderte Rolle von Experten**

Welch herausragende Rolle Daten in der Digitalisierung und für die Gesellschaft spielen, wird in der Datenstrategie der Bundesregierung deutlich. „Daten bilden die Grundlage der digitalen Gesellschaft. Mehr Daten innovativ, verantwortungsvoll und gemeinwohlorientiert zu nutzen, kann das Zusammenleben in Deutschland, in Europa und in der Welt bedeutsam verbessern und natürliche Ressourcen schützen." (Die Bundesregierung, Datenstrategie der Bundesregierung, 27. Januar 2021)

**Ralf Kleinfeld, Information Security Officer, Otto (GmbH & Co KG)**

Das Aufgabengebiet der Cybersicherheit stützt sich auf den Schutzbedarf von Daten und Geschäftsprozessen, somit lässt sich aus der Datenstrategie ein Auftrag für Cybersicherheit ableiten.

Dabei steht die Rolle von Cybersicherheitsexperten veränderten Rahmenbedingungen gegenüber, die auch Einfluss auf das Aufgabengebiet haben. Die Herausforderung ist, Unternehmen bestmöglich zu schützen und die zuvor beschriebenen Anforderungen der Digitalisierung zu ermöglichen. Der verwendete Begriff der Security Awareness, zu Deutsch Sicherheitsbewusstsein, muss weitergedacht werden. Es ist vielmehr eine Sicherheitskultur erforderlich, mit der Cybersicherheit zu einem Teil der Unternehmenskultur wird. Cybersicherheitsexperten stehen vor der Herausforderung dies zu fördern und sich selbst mit dem Geschäftsmodell auseinanderzusetzen. Dazu gehört, dass mit Hilfe von Sicherheitstechnologie ein starkes Fundament geschaffen wird, das dafür sorgt, dass das Arbeiten unter geschützten Bedingungen stattfinden kann. Für das, was Sicherheitstechnologie nicht abdecken kann, ist es erforderlich für Beschäftigte in Unternehmen einen Rahmen zu bieten, in dem die zunehmende Handlungsfreiheit, Selbstkontrolle und -steuerung geschützt möglich sind. Und zu dem Rahmen gehört, Beschäftigte durch Ausbildung, Beratung und Unterstützung zu befähigen, sicherheitsbewusst und sicherheitskompetent die jeweiligen Aufgaben im Unternehmen wahr zu nehmen.

**Cybersicherheit als unternehmerische Verantwortung**

Die Aufgabe der Cybersicherheit als Haltungsthema zu verstehen, macht deutlich, dass es eine Aufgabe des Unternehmens an sich und aller Beschäftigten ist. Dahinter stehen Werte, mit denen Unternehmen ihre Verantwortung für das Unternehmen, für Beschäftigte, Kunden und Geschäftspartner wahrnehmen können. Das ergibt als weitere Folgerung, dass das Aufgabengebiet der Cybersicherheit ein Teil der digitalen unternehmerischen Verantwortung darstellt. Dies wird in der bereits zitierten Datenstrategie der Bundesregierung deutlich und explizit hervorgehoben:

„Alle Akteure der Datengesellschaft stehen in der Verantwortung, Vertrauen zu schaffen und zu befördern. Wir wollen eine digitale Zukunft gestalten, der die Menschen vertrauen können. Dabei ist es unser Ziel, dass die Menschen durch rechtliche Regelungen und technische Maßnahmen geschützt werden und aufgeklärt agieren können: Selbstbestimmt und kompetent, unabhängig und sicher." (Die Bundesregierung, Datenstrategie der Bundesregierung, 27. Januar 2021)

Diese strategische Perspektive findet sich ebenfalls in der Cybersicherheitsstrategie für Deutschland wieder. (Bundesministerium des Innern, für Bau und Heimat, Entwurf Cybersicherheitsstrategie für Deutschland 2021, Juni 2021)

Die darin verankerten drei Leitlinien

1. „Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren
2. „Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken"
3. „Digitalisierung sicher gestalten" ergänzen die Datenstrategie nahtlos und stellen die gesellschaftliche Bedeutung von Cybersicherheit heraus. In der Cybersicherheitsstrategie werden konkrete Handlungsfelder aufgezeigt, die sich in die Cybersicherheitsstrategie von Unternehmen übertragen lassen. Für Unternehmen können aus diesen Handlungsfeldern Schwerpunkte für eine digitale Cybersicherheitsstrategie abgeleitet werden, beispielsweise in den drei folgenden Schwerpunkten
   1. Sicheres und selbst bestimmtes Handeln in einer digitalisierten Umgebung
   2. Gemeinsamer Auftrag von Fach- und Technologiebereichen
   3. Leistungsfähige und nachhaltige Cybersicherheitsarchitektur

In diesen Schwerpunkten gehen die in diesem Artikel beschriebenen Anforderungen an Cybersicherheit und Digitalisierung auf. Wenn Unternehmen diese in ihrer Cybersicherheitsstrategie verankern, so unterstützt eine erfolgreiche Umsetzung sowohl Digitalisierung als auch die Geschäftsentwicklung. Anhand der beiden referenzierten Strategiepapiere „Datenstrategie" und „Cybersicherheitsstrategie" wird die gegenseitige Abhängigkeit von Digitalisierung und Cybersicherheit überdeutlich, es erscheint nur logisch diese beiden Strategien in Verbindung zu nutzen.

Zusammenfassend bedeutet Cybersicherheit erfolgreich zu gestalten somit, dass sie in der Unternehmenskultur verankert wird und insbesondere ein Thema des Top-Managements ist.

1. Als Thema aller Beschäftigten, nicht nur - aber auch - von Cybersicherheitsexperten.
2. Als unternehmerische Verantwortung, als ein Business Thema und als Business-Unterstützungsfunktion.
3. Als Daueraufgabe, die kontinuierlich weiterentwickelt werden muss.

Kieran Hernon

## Mit Virtual Patching Schwachstellen wirksam beseitigen

Ein wirksames und zeitnahes Patchen von Sicherheitslücken ist essentiell, um Cyberangriffen rechtzeitig zuvorzukommen. Doch die Patch-Verwaltung ist aufwendig und benötigt Zeit. Virtual Patching dagegen führt sofort zu einer deutlich erhöhten Security, denn es signalisiert, dass Schwachstellen geschlossen sind.

Das schwächt die Angriffsbasis für Cyberkriminelle.

Ob Handel, Industrie oder Behörden – kaum ein gesellschaftlicher Bereich, der nicht auf Basis von Datenspeicherung, -analyse und -verarbeitung arbeitet. Mit der Datenverarbeitung hängt über Organisationen und Unternehmen jedoch auch das Damoklesschwert gezielter Cyberattacken. Sind diese erfolgreich, können die Kosten für die betroffenen Institutionen in die Millionen gehen. So zieht der Bitkom in ihrem aktuellen Bedrohungsbericht für 2020 eine Schadensbilanz von 223 Milliarden Euro jährlich durch Cyberangriffe – mehr als das Doppelte des Zeitraums 2018/19, als es 103 Milliarden Euro pro Jahr waren. Von den befragten Firmen sind 88 Prozent bereits Opfer von Angriffen geworden. Vor allem der Mittelstand ist betroffen, wobei es in erster Linie zu Ransomware-Attacken kommt. Es ist davon auszugehen, dass sich die Bedrohungslage weiter verschärft, denn Cyberkriminelle nutzen zunehmend auch automatisierte Systeme und Algorithmen, um ungepatchte Sicherheitslücken bei ihren potenziellen Opfern zu ermitteln. Unternehmen oder Behörden gelingt es nur unzureichend, sich dagegen zu wappnen. Ein Grund dafür ist ein unzureichendes Patch-Management der Hard-, Soft- und Firmware.

**Wo das Patch-Management mit der Zeit kämpft**

Was macht ein wirksames und rechtzeitiges Patchen so schwierig? Zunächst einmal sind moderne IT-Infrastrukturen in der Regel über Jahre gewachsen. Sie sind damit äußerst komplex und wenig transparent, so dass die Patch-Verwaltung zu einer aufwendigen und ressourcenintensiven Aufgabe geworden ist. Hinzu kommt: In bestehenden IT-Umgebungen werden noch immer veraltete Systeme gehostet, doch diese werden in der Regel nicht mehr durch die Hersteller unterstützt und es sind keine Patches mehr für sie vorgesehen. Und wenn es möglich ist, einen Patch in eine Client-Server-Architektur einzuspielen, ist ein zeitintensiver Test erforderlich. Doch gerade dann, wenn eine neue Schwachstelle aufgedeckt wird, dürfen Anwender im Wettlauf mit möglichen Cyberangriffen keine Zeit verlieren. Weitere Risiken für das Patching lauern außerhalb der IT-Umgebung. So lassen sich die angeschlossenen Geräte häufig nicht patchen, weil dies die Herstellergarantie auf zugesicherte Funktionen aushebeln würde. Dies ist vor allem bei Produktionsanlagen oder medizinischen Geräten heikel. Auch hier kommt der Zeitfaktor ins Spiel, denn Geräte- und Anlagenhersteller ebenso wie Softwarespezialisten benötigen ebenfalls einige Zeit, um nach Bekanntwerden einer Schwachstelle einen Patch einzuspielen. Dies kann beispielsweise bei einem SCADA-System, das technische Prozesse in einer automatisierten Fertigung steuert, bis zu 150 Tage in Anspruch nehmen – zu lange, um wirklich viel Sicherheit zu bieten. Betreibern bleibt im Grund nur die Möglichkeit, ungepatchte Systeme zu betreiben – obwohl sie sich Sicherheitslücken auf keinen Fall leisten können. Dies ist jedoch keine langfristige Lösung, denn nicht nur hochsensible Daten oder die eigene Reputation stehen bei einem erfolgreichen Angriff auf dem Spiel. Auch die Verfügbarkeit wichtiger Strukturen ist in Gefahr, vor allem für die Betreiber kritischer Infrastrukturen (KRITIS).

**Udo Schneider, IoT Security Evangelist Europe, Akima Media GmbH**

**Klassische Exploit-Filter versus Virtual Patching**

Häufig kommen auf Netzwerkebene Exploit-Filter in herkömmlichen IDS/IPS-Lösungen (Intrusion Detection System/Intrusion Prevention System) und Next-Generation-Firewalls zum Einsatz. Diese sollen Angriffe abwehren, die auf nicht gepatchte Schwachstellen erfolgen. Doch der Einsatz dieser Exploit-Filter hat einige Nachteile. Zunächst wirken sie lediglich gegen bekannte Angriffe. Ist ein Schadcode nur leicht abweichend programmiert, kann er die Schwachstelle mühelos passieren – der Filter ist wirkungslos. Für diesen neuen Exploit muss dann ein neuer, passender Filter entwickelt werden. Nicht nur, dass damit die Anzahl der Filter wächst und der Netzwerkverkehr verlangsamt wird. Diese meist unter hohem Zeitdruck entwickelten Filter sind fehleranfällig und decken die bestehende Schwachstelle nicht ausreichend ab. Damit steigt die Anzahl der False Positive-Meldungen. Ein Patching per Exploit-Filter kann Cyberattacken also nur in einem gewissen Maße wirklich effektiv ausschalten. Weitaus mehr Sicherheit bietet Virtual Patching, denn hier werden Schwachstellen auf Netzwerkebene automatisch geschlossen. In modernen IPS- und Firewall-Lösungen eingesetzte Virtuelle Patches decken Schwachstellen komplett ab und schützen sie damit auch vor künftigen Exploits. Die Technologie blockiert hierzu die von Cyberkriminellen zum Ausnutzen von Schwachstellen versendeten Datenpakete, beispielsweise einen unautorisierten Zugang zu einem System, einer Software oder einem Netzwerk-Element. Der Virtual Patch lässt den Angriff fehlschlagen, auch wenn die Schwachstelle weder von Herstellerseite noch durch Updates gepatcht ist. Diese Strategie sichert Sicherheitslücken so wirksam ab, dass selbst ungepatchte Systeme gegen künftige Attacken geschützt sind. Zudem sorgt Virtual Patching für einen Zeitvorsprung, denn die erkannten Lücken lassen sich später genauer in den Fokus nehmen und endgültig schließen. Dies ist notwendig, denn selbst wenn eine Schwachstelle durch einen Virtual Patch entschärft wurde, bleibt die Bedrohung bis zur Aktualisierung des Systems bestehen – wenn auch in geringerem Ausmaß.

**Schneller sein als die Angreifer**

Der Zeitvorsprung, den Virtual Patching bietet, ist entscheidend, denn je länger es dauert, eine Schwachstelle zu beheben, desto mehr Zeit erhalten Cyberkriminelle, um sie auszunutzen. Das IT-Marktforschungsunternehmen Omdia hat in einer aktuellen Analyse das

Gefährdungspotenzial von Sicherheitslücken untersucht. Dabei beschränkte es sich auf Schwachstellen, die von insgesamt elf Sicherheitsanbietern aufgedeckt wurden und mit einer CVE (Common Vulnerability and Exposure)-Nummer gekennzeichnet sind. Es zeigte sich, das mit 62 Prozent die Mehrheit der insgesamt rund 1370 Schwachstellen, die für 2020 gemeldet wurden, als „hoch riskant" einzustufen sind. Schwachstellen mit mittlerem Gefährdungspotential machen rund 20 Prozent aus, während nur drei Prozent aller Sicherheitslücken als unbedenklich eingestuft werden. Es ist jedoch davon auszugehen, dass die Zahl der Zero-Day-Schwachstellen noch weitaus höher liegt. Diese machen etwa 15 Prozent der aufgedeckten Bedrohungen aus und sind damit eine bedeutende Bedrohung für die Informationssicherheit. In der Zero-Day-Initiative (ZDI) arbeiten unabhängige Sicherheitsforscher, Technologieanbieter und Sicherheitsspezialisten weltweit zusammen, um diese Schwachstellen zu ermitteln. Mit Erfolg: Im vergangenen Jahr konnte die vom Sicherheitsspezialisten Trend Micro getragene ZDI rund 60 Prozent aller weltweit bekannten Vulnerabilities erstmals aufdecken. Trend Micro steht aufgrund seiner Größe und umfangreichen Erfahrung auch in der oben erwähnten Omdia-Analyse bezüglich der Anzahl der ermittelten Sicherheitslücken unter den elf in die Betrachtung einbezogenen Unternehmen an erster Stelle. Das Unternehmen bietet Virtual Patching an, das auf Daten der ZDI basiert.

* Source: 2020 Cyberthreat Defense Report, CyberEdge Group, LLC

**Virtual Patching bringt viele Vorteile**

Um den Wettlauf mit der Zeit in Bezug auf Bedrohungen zu gewinnen, ist Virtual Patching das Mittel der Wahl. Es ermöglicht ein automatisiertes Patch-Management in komplexen, hybriden Infrastrukturen und schließt bestehende Schwachstellen sofort. So sind die Systeme automatisch innerhalb von 24 Stunden nach Bekanntwerden einer Sicherheitslücke geschützt. Während die Patch-Technologie Angriffe auf diese Schwachstelle blockt, lassen sich Hersteller-Patches in Ruhe einspielen und testen. Die Technologie reduziert die Anzahl der False Points erheblich und schützt ungepatchte Legacy-Systeme, ebenso wie Server, die nur schwer upzudaten sind. Das reduziert auch den Druck auf die IT-Abteilung, die nicht selbst in die Software und Systeme eingreifen muss. Für Schwachstellen, die zuerst von der ZDI gefunden werden, stellen die der ZDI angegliederten Security-Anbieter – darunter Trend Micro – einen virtuellen Patch bereits vor Veröffentlichung der Schwachstelle bereit. So gewinnen Unternehmen im Durchschnitt 96 Tage Zeit – der durchschnittliche Zeitraum, den es bedarf, um eine dem Virtual Patching ähnliches Schutzniveau zu erreichen.

Udo Schneider

# Datenexfiltration: Den Dieben einen Schritt voraus bleiben

**Abstract**

Cyberattacken stellen eine massive Bedrohung für Unternehmen dar. Auch in Deutschland werden Daten durch schädliche Angriffe immer öfter erfolgreich abgegriffen. Um Datenexfiltration zu verhindern, müssen Unternehmen die frühe Phase des Angriffs erkennen und der Gefahr vorbeugen, statt erst zu reagieren, wenn die Täter bereits ins Netzwerk eingedrungen sind. Im Folgenden wird analysiert, welche Schritte für eine erfolgreiche Schadensabwehr nötig sind.

Wie die jüngsten Spionageangriffe durch die Hacker-Software Pegasus und der weltweite REvil-Kaseya-Angriff belegen, nehmen Cyberangriffe seit Jahren stark zu – insbesondere seit Beginn der Corona-Pandemie. Das belegt auch der Cyberthreat-Defense-Report* der CyberEdge-Group: Cyberkriminelle haben die Krisensituation für sich genutzt. 86 Prozent der befragten Unternehmen im Jahr 2021 wurden in den vergangenen zwölf Monaten mindestens einmal Opfer einer erfolgreichen Cyberattacke – so viele wie noch nie. Auch deutsche Unternehmen waren verstärkt Ziel der Angriffe, 91,5 Prozent der Befragten gaben an, Ziel eines Angriffs gewesen zu sein. Gemeinsam mit China liegt Deutschland damit auf dem zweiten Platz der Länder, in denen Angreifer erfolgreich in Organisationen eingedrungen sind. Für Unternehmen bedeutet ein schädliches Eindringen in das Netzwerk nicht nur den bloßen Verlust von Daten, sondern häufig langfristige Auswirkungen auf Finanzen und Ansehen. In Folge der Exfiltration von Daten, also dem nicht autorisierten Transfer von Daten eines Netzwerks, nutzen die Täter die gestohlenen Informationen etwa, um das Unternehmen zu erpressen. Sind durch den Angriff zudem Kundendaten betroffen, weitet sich der Kreis der Opfer aus und es kann zu erheblichen Einbußen der Reputation kommen. Für Unternehmen ist daher zentral, dass Netzwerk effektiv zu verteidigen und darüber hinaus die nachfolgenden Aktionen des Angreifers abzudecken. Dabei sind zahlreiche Schritte und vielschichtige Methoden zu beachten, die im Folgenden detailliert analysiert werden.

**Ziel der Angreifer hat sich gewandelt**

Datenexfiltration ist eine Form böswilliger Cyberoperationen. Bei dieser Art des Angriffs verschaffen sich Akteure, etwa mithilfe einer Schadsoftware, Zugang zu sensiblen Daten. Jedoch hat sich das Ziel der Angreifer im Laufe der Zeit gewandelt. Wurden diese früher von staatlichen Akteuren oder anderen Auftraggebern herangezogen, um bestimmte Unternehmen gezielt auszuspionieren und Innovationen zu stehlen, geht es heute weniger um die Vorteile für den Angreifer selbst. Die Cyberattacken zielen mittlerweile nicht mehr darauf ab, die gestohlenen Daten für eigene Zwecke zu

nutzen, sondern dem Opfer mithilfe der gewonnenen Informationen Schaden zuzufügen. Da Unternehmen die Offenlegung ihrer Daten fürchten, bietet sich für Täter die Gelegenheit, hohe Geldsummen zu erpressen. Exfiltration wird demnach mittlerweile aus monetären oder hacktivistischen Gründen betrieben. Für Netzwerkeigentümer, -betreiber und -verteidiger bedeutet dieser Wandel, dass sie für ausreichende Kontrollen sorgen müssen, um böswillige Angriffe zu erkennen, einzudämmen oder in Anbetracht der potenziellen Kosten ganz zu unterbinden.

**Exfiltration hat vielfältige Auswirkungen**

Im Bereich der Cybersicherheit gibt es zahlreiche Gefahrenquellen, die sofort drastische Folgen mit sich ziehen, etwa ein virulenter Ransomware-Vorfall. Trotzdem darf die Exfiltration von Daten nicht unterschätzt werden: Neben unmittelbaren Auswirkungen kann der Verlust sensibler Daten auch langfristig Gefahren bergen.

Dabei sind drei Hauptrisiken von zentraler Bedeutung: der Verlust von sensiblen Daten oder geistigem Eigentum, Rufschädigung und Erpressung. Ersteres kann Unternehmen im Wettbewerb mit Konkurrenten zurückwerfen. Werden zudem Kunden- oder Klienten-Daten abgegriffen, können regulatorische Maßnahmen, Vertrauensverlust der Kunden und somit eine Beeinträchtigung der Beziehungen die Folgen sein. Gelangt der Vorfall an die Öffentlichkeit, kann es zu einer langfristigen Rufschädigung kommen. Das Unternehmen ist gezwungen, verstärkte Öffentlichkeitsarbeit zu betreiben, um dem Image-Verlust entgegenzuwirken. Rufschädigung stellt insofern ein bedeutendes Risiko dar, dass ein Ruf zwar schnell zerstört, aber nur mühsam wieder aufgebaut werden kann. Das dritte zentrale Risiko ist die Erpressung durch Cyber-Kriminelle.

Die Risiken, die mit Datenverlusten oder Exfiltrationsereignissen verbunden sind, haben also beträchtliche Auswirkungen auf das Unternehmen und dessen Beziehungen. Hinzu kommt, dass die Quantifizierung und die Zeitspanne bis zur Manifestation der Folgen kaum abzuschätzen sind. Durch den Diebstahl von geistigem Eigentum kann das Unternehmen noch Jahre oder Jahrzehnte nach dem eigentlichen Vorfall getroffen werden. Reputationsverluste wiederum sind schwer zu messen und können kaum ausgeglichen werden. Vor dem Hintergrund der Zunahme an Hackerangriffen und der gewandelten Zielsetzung der Angreifer wird die Datenexfiltration künftig an Bedeutung gewinnen und akutere Folgen für Unternehmen haben als bisher. Für einen Schutz der Daten des Unternehmens ist es zwingend notwendig, dass Netzwerkverteidiger und -betreiber ihre Verteidigungsmaßnahmen so ausrichten, dass diese Angriffe schnellstmöglich erkannt und bestenfalls sogar verhindert werden können.

**Exfiltrationsaktivitäten frühzeitig identifizieren**

Bei der Exfiltration werden große Datenmengen zu neuen oder unbekannten Quellen verschoben. Das kann entweder durch einen direkten physischen Zugang zum Computer oder den Einsatz von Schadsoftware geschehen. Anders als man meinen würde, ist es allerdings nicht einfach, diese Bewegung zu erkennen. Nötig dafür ist eine Kombination aus Netzwerksichtbarkeit und aktiver Netzwerküberwachung. Ist beides nicht im nötigen Umfang vorhanden, erlangen Unternehmen keinen Einblick in die böswilligen Verhaltensweisen oder nehmen zwar Aktivitäten wahr, erkennen aber die Absicht dahinter nicht. Durch die Fehleinschätzung der Angriffe als legitime Aktivitäten entsteht ein erhebliches „Rauschen" bei der Erkennung.

Doch selbst wenn Unternehmen ausreichend Einblicke in ihr Netzwerk haben, ist das Erkennen der Angreifer eine Herausforderung. Mit Techniken wie der Verschleierung oder der Überlagerung durch andere Aktivitäten versuchen diese, die Sichtbarkeit zu minimieren und sich somit einer Aufdeckung zu entziehen. Möglich ist dies etwa durch folgende Techniken:

- Verwendung von legitimen Drittanbieterdiensten wie z. B. Cloud-Backup-Systemen oder webbasiertem Speicher als Ziel für durchgesickerte Daten. Die Beispiele reichen von gängigen Produkten wie Google Drive und Dropbox bis hin zu spezielleren Produkten eines Ökosystems wie beispielsweise im Zusammenhang mit dem Mega.io-Dienst.
- Datenverkehr über Nicht-HTTP-Dienste tunneln oder alternative Protokolle für große Datenübertragungen verwenden, die möglicherweise nicht mit demselben Maß an Sorgfalt überwacht werden.
- Aufteilung der Daten in kleinere Stücke für die Exfiltration, um zu vermeiden, dass abnormal große Datenströme das Netzwerk verlassen.

**Olaf Dünnweller, Senior Sales Director Central Europe, Gigamon**

Zwar erschweren diese Techniken das Aufspüren der Angreifer, machen sie allerdings nicht unmöglich. Wird die Überwachung der allgemeinen Traffic-Muster-Anomalien gemeinsam mit einer spezifischen Identifizierung bestimmter Techniken oder Verhaltensweisen eingesetzt, können Attacken erkannt werden. Der Zugriff auf Datasets wie den Netzwerk-Flow ermöglicht dies sogar dann, wenn die Daten verschlüsselt sind oder der Einblick in die Netzwerkaktivitäten eingeschränkt ist.

Die Identifizierung verdächtiger Netzwerk-Flows ist eine zuverlässige Methode, um Exfiltrationsaktivitäten zu identifizieren. Dabei spielt neben der Suche nach großen Datenströmen die Identifizierung der Richtungsabhängigkeit und des Upload-/Download-Verhältnisses eine große Rolle. Die Einschätzung, ob ein Datenstrom als „groß" angesehen werden kann, hängt natürlich von den üblichen Größenordnungen innerhalb des überwachten Netzwerks ab. Große Datenströme

sind ein Hinweis auf verdächtige Handlungen, da sie auf datenintensive Verbindungen wie Streaming, Fernzugriff oder ähnliche Aktivitäten hindeuten. Durch Hinzuziehen der Richtungsabhängigkeit und des Upload-/Download-Verhältnisses kann identifiziert werden, ob die Daten das Netzwerk verlassen. Ist das beim Großteil der Daten (80-90 Prozent) der Fall, deutet dies auf eine große Upload-Sitzung hin. Da es solche Sitzungen auch im legalen Unternehmenskontext gibt, ist im nächsten Schritt eine genauere Prüfung dieser Aktivitäten nötig. Neben schädlichen Angriffen könnten nämlich auch die gemeinsame Nutzung großer Projektdateien einen entsprechend großen Datenfluss erzeugen.

Die Effektivität des beschriebenen Vorgehens kann verstärkt werden, wenn ein analytischer Ansatz für Netzwerkverbindungen hinzugezogen wird. Somit werden die nicht-autorisierten ausgehenden Datenströme nicht nur identifiziert, sondern zudem die mit ihnen verbundene Netzwerkinfrastruktur analysiert. So kann die Verknüpfung eines verdächtigen ausgehenden Datenflusses mit einer neuen Netzwerkinfrastruktur oder einer Virtual Private Server (VPS)-Instanz verdächtige Aktivitäten aufdecken. Dieses Verfahren kann auch auf nicht standardmäßige Verbindungen (wie FTP oder andere Protokolle) zu unbekannten oder nicht vertrauenswürdigen Bestimmungsorten angewendet werden, um potenzielle Exfiltrationsaktivitäten zu ermitteln.

Mit Kombination dieser Strategien steht Unternehmen eine effektive Methode zur Verfügung, um Exfiltrationsereignisse aufzudecken. Sie können Exfiltration identifizieren, wenn oder kurz nachdem sie stattgefunden hat. Unternehmen haben durch die schnelle Erkennung die Möglichkeit, Reaktions- und Schadenbegrenzungsmaßnahmen zu ergreifen, wodurch die Zeit des unentdeckten Angriffs und die Zeitspanne bis zur ersten Reaktion verringert werden können. Im Umkehrschluss bedeutet dies allerdings, dass dem Angreifer ein Eindringen in das Netzwerk gelungen ist, weshalb sich der beschriebene Ansatz ausschließlich auf einen bereits erfolgreichen Angriff bezieht. Um Schaden vollkommen abzuwenden, ist es daher nötig, eine Exfiltration überhaupt zu verhindern.

### Mit der „Whole of Kill Chain"-Verteidigung Angriffe frühzeitig verhindern

Um Exfiltration vollständig zu verhindern, muss eine „Whole of Cyber Kill Chain"-Perspektive verfolgt werden. Diese bezieht sich auf den Ablauf eines typischen Cyberangriffs und versucht, im Kontext der Netzwerküberwachung und -verteidigung bereits die ersten Schritte des Angreifers zu unterbinden. Damit dies gelingt, suchen Verteidiger nach übergreifenden Pfaden und Abhängigkeiten, über die Angreifer ins Netzwerk gelangen und Daten aus dem Netzwerk geschleust werden könnten. Notwendige Wegbereiter beziehen sich etwa auf den ersten Zugriff, laterale Bewegungen, Datensammlung und die Datenbereitstellung.

Durch die Übernahme der Perspektive des Angreifers und der kritischen Untersuchung der nötigen Voraussetzungen für ein böswilliges Eindringen können neue Sicherheitsvorkehrungen abgeleitet werden. So kann eine Implementierung von allgemeineren Kontrollen auf dem Host und im Netzwerk nicht nur Exfiltrationsoperationen, sondern eine Vielzahl von Eindringungsversuchen abwehren. Durch die Identifizierung der wahrscheinlichen Eindringmechanismen des Angreifers und deren genaue Überwachung verringert sich die Wahrscheinlichkeit eines erfolgreichen Zugriffs durch einen Bedrohungsakteur. Die eingeführten Kontrollen reduzieren zudem die Angriffsfläche erheblich. Solche Kontrollen sind vor allem das Patchen von nach außen gerichteten Systemen, die Reduzierung von für den externen Zugriff verfügbaren Services, die Begrenzung der in das Netzwerk eingehenden Trafficarten und das Monitoring sensibler Aktivitäten wie Fernadministration oder -zugriffssitzungen.

Viele Unternehmen konzentrieren sich auf diese Schritte, um das Angriffsrisiko zu reduzieren. Jedoch erfordert eine echte, mehrstufige Verteidigung, dass man über die Netzwerkgrenze hinausgeht, um auch die nachfolgenden Aktionen des Angreifers abzudecken. Dem Angreifer stehen nahezu unbegrenzte mögliche anfängliche Zugriffsmechanismen zur Verfügung, zudem kann er Systeme oder Benutzer unterwandern, selbst wenn Elemente gepatcht oder anderweitig überwacht werden. Daher muss sich die Verteidigung auch auf interne Netzwerkverkehrsströme und Host-Items ausdehnen. Verteidiger müssen Techniken für laterale Bewegungen und deren Artefakte sowohl im Netzwerk als auch im Host-Verhalten identifizieren.

Während die zunehmende Einführung von EDR-Produkten (Endpoint Defense and Response) hostzentrierte Beobachtungen abdeckt, sind Investitionen in die Sichtbarkeit und Überwachung des Ost-West-Traffics unerlässlich, um das Eindringen von Angreifern in geschützte Netzwerke zu erfassen. Verteidiger müssen Techniken für laterale Bewegungen und deren Artefakte sowohl im Netzwerk als auch im Host-Verhalten identifizieren. Wenn diese Elemente zusammen implementiert werden, können sie sicherstellen, dass gegnerische Operationen abgedeckt werden, die von opportunistischen kriminellen Akteuren über gezielt vorgehende Hacktivisten bis hin zu staatlich gesponserten Bedrohungen reichen.

Für den Schutz der Daten und sensiblen Informationen eines Unternehmens müssen Verteidigungskräfte das Verhalten und die Tendenzen des Angreifers verstehen, um zu identifizieren, wie der Gegner vorgeht und welche Techniken für den Versuch des Eindringens genutzt werden. Sind diese Punkte festgestellt, muss eine Kombination aus EDR und Netzwerkverteidi-

gung und -reaktion (NDR – Network Detection and Response) eingesetzt werden, um eine mehrstufige Erkennung und Überwachung zu gewährleisten und potenzielle Lücken in der Sichtbarkeit zu schließen, die Angreifer möglicherweise zu ihrem Vorteil zu nutzen versuchen.

**Fazit**

Cyber-Bedrohungen schließen immer häufiger die Exfiltration von Daten ein. Zahlreiche Akteure, von Kriminellen über Hacktivisten bis hin zu staatlich gelenkten Eindringlingen, nehmen sich sensible Daten von Unternehmen als Ziel, um diese zu erpressen. Durch die Anwendung und Überwachung von starken Netzwerkkontrollen können Verteidiger und Asset-Besitzer sicherstellen, dass solche Verhaltensweisen so früh wie möglich erkannt werden. So können Unternehmen schnell auf den Angriff reagieren und mögliche Schäden begrenzen.

Verteidiger können sich nicht nur auf die Erkennung anomaler ausgehender Datenströme konzentrieren: Stattdessen erfordert eine robuste Verteidigung die Identifizierung von gegnerischen Aktionen in allen Phasen der Angriffe. Eine Reaktion ist daher nicht erst erforderlich, wenn der Angreifer bereits ins Netzwerk eingedrungen ist, sondern schon im Vorfeld. Sobald dies verstanden ist, können Schutzmaßnahmen im Netzwerk und auf dem Host implementiert werden, um jeden Schritt des Eindringens abzudecken. Nur durch diesen stabilen, in die Tiefe gehenden Abwehransatz können Verteidiger nicht nur das Bewusstsein für potenzielle böswillige Aktivitäten sicherstellen, sondern auch die Unterbindung oder Unterbrechung eines Eindringens ermöglichen, wenn die Aktionen frühzeitig im Lebenszyklus des Angreifers erkannt werden. Die Verteidigung gegen moderne Cyber-Bedrohungen, von Ransomware-Operationen bis hin zur Datenexfiltration zu verschiedenen Zwecken, ist zwar weder einfach noch kostengünstig, aber notwendig, um sicherzustellen, dass die Verteidiger mit der sich schnell entwickelnden Bedrohungslandschaft Schritt halten.

Olaf Dünnweller

## Feuer mit Feuer bekämpfen – Automatisierte Cyberangriffe lassen sich nur mit KI-gestützter Automatisierung abwehren

Immer mehr Cyber-Angreifer nutzen mittlerweile die Automatisierung, um ihre Angriffe schnell auszuführen und Bedrohungen mit atemberaubender Geschwindigkeit zu implementieren. Mittlerweile finden weltweit alle 39 Sekunden Cyberangriffe statt. Die einzige Möglichkeit, mit diesen Bedrohungen Schritt zu halten und sie effizient abzuwehren, besteht in der Automatisierung der Maßnahmen zur Abwehr von Cyberattacken. Die Cybersecurity-Automatisierung arbeitet dabei nach der Devise, Feuer mit Feuer zu bekämpfen.

**Was ist Cybersecurity-Automatisierung?**

Jeden Tag werden Cyberangriffe zahlreicher und ausgefeilter. Um diese Bedrohungen zu untersuchen, müssen Cyber-Analysten manuelle und sich wiederholende Arbeiten durchführen. Mit Hilfe von Sicherheitssoftware navigieren sich Sicherheitsteams durch Datenwarnungen, um die vielen obskuren Bedrohungen zu finden, über die sie Bescheid wissen müssen. Diese Aufgaben können automatisiert werden.

**Von Anti-Malware bis SOAR**

Die Cybersecurity-Automatisierung ist die maschinenbasierte Ausführung von Sicherheitsaktionen, die Cyberbedrohungen ohne menschliches Eingreifen programmgesteuert erkennen und eingehende Bedrohungen identifizieren, aufkommende Warnungen sortieren und priorisieren, damit zeitnah entsprechende Maßnahmen ergriffen werden können. So überwachen Automatisierungslösungen Intrusion Detection-Systeme, um nach Bedrohungen und Schwachstellen zu suchen. Anti Malware kann so eingerichtet werden, dass sie alle in einem System angemeldeten Geräte automatisch erkennen und scannen. Diese Produkte identifizieren Cyber-Bedrohungen und beseitigen identifizierte Fehler basierend auf den vom Unternehmen festgelegten Sicherheitsprotokollen. Security Orchestration Automation and Response (SOAR)-Produkte automatisieren den Ablauf. Sie wurden entwickelt, um Aktivitäten zwischen verschiedenen Sicherheitstools zu orchestrieren und gleichzeitig spezifische Automatisierungsaktivitäten als Reaktion auf die identifizierten Schwachstellen auszuführen.

**Warum ist Cybersecurity-Automatisierung wichtig?**

Die Digitalisierung von Unternehmens-Netzwerken bietet je Menge Angriffsflächen, die angemessen überwacht und verteidigt werden müssen, um beim Auftreten von Bedrohungen rechtzeitig reagieren zu können. Immer noch verlassen sich Unternehmen auf traditionelle Methoden, um ihre Systeme auf Verhaltensanomalien oder Bedrohungsindikatoren zu untersuchen. Diese sind relativ ineffizient, da große Datenmengen manuell von fehleranfälligen Menschen bearbeitet und verwaltet werden müssen. Dies führt zwangsläufig zu Lücken in der Sicherheits-Infrastruktur, durch die Bedrohungen das Unternehmen infiltrieren können. Die Implementierung einer Cybersicherheitsautomatisierung ist daher ein wichtiger und zuverlässiger Mechanismus, um Unternehmen zu schützen und gleichzeitig durch automatisierte Prozesse eine maximale Verteidigung zu gewährleisten.

Milad Safar, Managing Partner, Weissenberg Group

**Vorteile der Cybersecurity-Automatisierung**
Automatisierung stützt sich auf Technologien der Künstlichen Intelligenz (KI), um die Analysefähigkeiten eines Unternehmens zu erhöhen. Sie eliminiert auch die menschliche Komponente aus dem Prozess, ermöglicht eine schnellere Datenerfassung und macht die Reaktion des Vorfallmanagements zu einem dynamischeren, einheitlicheren und effizienteren Prozess. Außerdem entfallen zeitaufwendige und wiederholbare Aufgaben, so dass sich die Cybersicherheitsexperten auf die Entwicklung anderer Strategien und Initiativen konzentrieren können.

**Technologien der Cybersecurity-Automatisierung**
Funktionen mit geringer Kognition wie Überwachung, Scannen und Reaktion auf Vorfälle auf niedriger Ebene können von Robotic Process Automation (RPA) gehandhabt werden. RPA ermöglicht es, Daten zu erkennen, zu aggregieren und zu extrahieren, während der grundlegende Prozess der Bedrohungssuche und -erkennung durchgeführt wird. Automatisierte Erkennungs- und Alarmreaktionen führen zu einer kürzeren Zeit für die Erkennung von Bedrohungen und die Rückmeldung. RPA hilft bei der Identifizierung exponierter Angriffsflächen, um Sicherheitsrisiken zu mindern, indem es bei der Anwendungs- und Geräteerkennung hilft. RPA bietet damit einen proaktiven 24/7/365-Sicherheitsschutz, im Gegensatz zu Menschen, die aufgrund von Erschöpfung müde werden oder sich mental auspowern.

**Mit KI gegen AML**
Die fortlaufenden Entwicklungen bei Machine Learning (ML) und Natural Language Processing (NLP) werden zudem die Möglichkeiten verbessern, das Verhalten von Bedrohungsakteuren im Kontext von Absicht, Gelegenheit und Fähigkeit des Angreifers zu analysieren. ML kann Massen von Protokoll- und Ereignisdaten von Anwendungen, Endpunkten und Netzwerkgeräten durchsuchen, um schnell Muster aufzudecken und die Ursache von Vorfällen zu ermitteln. Dies ist auch dringend erforderlich, da Kriminelle mittlerweile ihrerseits auch schon Künstliche Intelligenz (KI) einsetzen, um Cyber-Abwehrmechanismen zu analysieren. Zudem kommt auch sogenanntes Adversarial Machine Learning (AML) zum Einsatz, um ein bereits trainiertes Modell zu täuschen, indem es mit bösartigen, manipulierten Daten überflutet wird.

**Möglichkeiten der Cybersecurity-Automatisierung**
Moderne Cyberangriffe sind stark automatisiert. Und nur durch Automatisierung lässt sich das Bedrohungsvolumen reduzieren, Verhaltensweisen besser vorhersagen und damit eine effektive Prävention installieren. Die manuelle Verteidigung gegen automatisierte Cyberangriffe ist wie der Kampf gegen Windmühlen.

**Korrelation von Daten**
Um sich effektiv auf Sicherheitsbedrohungen vorzubereiten, muss eine Vielzahl identifizierter und gesammelter Bedrohungsdaten über alle Angriffsvektoren in der eigenen Infrastruktur sowie globale Bedrohungsinformationen außerhalb der eigenen Infrastruktur ausgewertet werden. Gruppen von Bedrohungen müssen identifiziert werden, um den nächsten Schritt des Angreifers vorhersagen zu können. Dazu ist aber enorme Rechenpower notwendig, um das Bedrohungsvolumen zu skalieren. Das ist manuell nicht möglich. Machine Learning (ML) in Kombination mit der Automatisierung verschiedener Prozesse ermöglicht eine schnellere, effektivere und genauere Datensequenzierung. Dieser Ansatz einer dynamischen Bedrohungsanalyse ist die einzige Möglichkeit, ausgeklügelte und noch nie dagewesene Bedrohungen genau zu erkennen.

**Schnellen Schutz erzeugen**
Sobald eine Bedrohung identifiziert wird, müssen Schutzmaßnahmen schneller erstellt und verteilt werden, als sich ein Angriff im Netzwerke ausbreiten kann. Die Automatisierung kann den Prozess des Erstellens und Implementierens von Schutzmaßnahmen beschleunigen, ohne die Ressourcen zu belasten und ermöglicht es Unternehmen gleichzeitig mit dem Angriff Schritt zu halten. Der Einsatz von Automatisierung bei der Verteilung von Schutzmaßnahmen ist die einzige Möglichkeit, schneller als ein automatisierter und gut koordinierter Angriff vorzugehen und ihn zu stoppen. Mit automatisierter Big-Data-Angriffssequenzierung und automatischer Generierung und Verteilung von Schutzmaßnahmen kann der nächste Schritt eines unbekannten Angriffs genauer vorhergesagt und schnell genug gegen ihn vorgegangen werden, um ihn zu verhindern.

**Erkennen von Infektionen**
Unternehmen müssen schneller vorgehen als der Angreifer selbst. Nur so lässt sich ein Angriff abwehren, bevor Daten das Netzwerk verlassen. Um aber ein infiziertes System oder ein verdächtiges Verhalten zu identifizieren, müssen Daten zeitlich rückwärts und vorwärts analysiert und auf Verhaltensweisen untersucht werden, die darauf hindeuten, dass ein System infiziert wurde. Die Skalierung der manuellen Korrelation und Analyse von Daten im Netzwerk oder in der Cloud ist ein hoffnungsloses Unterfangen. Nur die Automatisierung ermöglicht eine schnelle Analyse, ob ein System im Netzwerk kompromittiert wurde, und eine ebenso schnelle Intervention.

**Kein „nice to have“, sondern ein “Must”**
Angesichts der steigenden Zahl und Schwere von Cyberangriffen mangelt es an erstklassigen Sicherheitstalenten. Cybersecurity-Automatisierung maximiert den

Wert und das Engagement der Sicherheitsanalysten durch die Automatisierung alltäglicher, mühsamer Aufgaben. Mit der Cyberstecurity-Automatisierung können die Reaktion auf Vorfälle und die Dauer des Incidents drastisch verkürzt werden. Cybersecurity-Automatisierung hilft Unternehmen, den Bedrohungen immer einen Schritt voraus zu sein. Die Reaktion auf Vorfälle, die Stunden oder sogar Tage dauern kann, kann auf Sekunden reduziert werden. Das bedeutet, dass Unternehmen sich weniger Bedrohungen aussetzen und auch ihre Kunden besser schützen, während sie gleichzeitig den Ruf und die eigene Zukunft schützen.

Milad Safar

# 1.6 AUTH

## Status quo bei verhaltensbiometrischen Authentifizierungsverfahren

**Dr. Torben Gülstorff, Freier Journalist, Redaktionsbüro Dr. Torben Gülstorff**

Schon länger nutzen Banken und Finanzdienstleister physische biometrische Sicherheitsverfahren, wie Scans des Fingerabdrucks, der Iris oder des Gesichts, um den Online-Zugang und die Online-Transaktionen ihrer Kunden vor unberechtigten Zugriffen zu schützen. Doch auch biometrische Daten können gefälscht werden. Mehr Sicherheit versprechen verhaltensbiometrische Systeme. Doch zwingen Vorgaben zum Datenschutz die meisten Anbieter dieser Lösung zur Arbeit mit anonymisierten Verhaltensdaten. Darunter leidet die Effektivität ihrer Systeme. Ein Problem, das Nutzer von biometrischen Authentifizierungsverfahren, die auf dem Verhalten basieren, nicht kennen.

Cyberangriffe auf digitale Identitäten von Nutzern nehmen zu. Nicht zuletzt das Lagebild Cybercrime 2020 des BKA zeigt genau dieses Phänomen auf. Immer häufiger versuchen Kriminelle über Social Engineering und Dateneinkäufe aus dem Darknet an Anmeldedaten der Nutzer zu gelangen, sich in deren Konten einzuwählen und unrechtmäßige Transaktionen anzuordnen. Klassische Authentifizierungsverfahren die Passwörter, PIN und Token nutzen, genügen hier schon lange nicht mehr. Mehr Sicherheit bietet ein Ansatz, der auf Daten der physischen Biometrie des Nutzers, seinen Fingerabdruck, sein Gesicht oder seine Iris, setzt. Er ist auch wesentlich anwenderfreundlicher als klassische Verfahren. Der Nutzer trägt seine Zugangsberechtigung am Körper, ist freier in seinen Zugangsmöglichkeiten, muss sich nicht mühsam Passwort oder PIN merken. Doch sind auch physische biometrische Daten nur Daten, können entwendet und missbraucht werden. Ein verwandtes biometrisches Verfahren verspricht hier mehr Schutz: die Authentifizierung eines Nutzers anhand seiner Verhaltensmuster.

**Verhaltensbiometrische Verfahren – die sicherere Art der Nutzerauthentifizierung**

Im Gegensatz zum physisch-biometrischen Ansatz werden beim verhaltensbiometrischen Ansatz Nutzer nicht anhand ihrer physischen Merkmale, sondern anhand ihrer Aktivitätsmuster authentifiziert. Der Anschlag einer Taste, das Bewegen und Klicken einer Maus unterscheiden sich von Nutzer zu Nutzer. Sammelt und analysiert man die diesbezüglichen Daten, lassen sich Verhaltensmuster erstellen, die klar einem Nutzer zugeordnet werden können und sich dementsprechend zur Anwendung in einem Authentifizierungsverfahren eignen. Verhaltensbiometrische Verfahren sind sicherer – sowohl als klassische als auch als physisch-biometrische Authentifizierungsverfahren. Drei Vorteile stechen besonders hervor: Erstens können sie im Gegensatz zu Letzteren nicht nur als Gatekeeper, sondern zur kontinuierlichen Überwachung im Hintergrund eingesetzt werden – und so die gesamte Customer Journey des Nutzers vor unerlaubten Zugriffen absichern helfen. Zweitens machen sie es Cyberkriminellen schwerer, gestohlene Daten zu nutzen. Denn Verhaltensprofile werden fortlaufend aktualisiert, um dem Umstand Rechnung zu tragen, dass Nutzerverhalten nun einmal nicht statisch ist. Drittens ermöglichen sie es Banken und Finanzdienstleistern, proaktiv gegen Cyberkriminelle vorzugehen. Betrüger können erkannt und blockiert werden – bevor sie Schaden anrichten. Weitere Vorteile der Technologie sind, dass die Kosten gesenkt und das Nutzererlebnis verbessert werden. Mit der kontinuierlichen Betrugsaufspürung sinkt die Zahl der Arbeitsstunden, die in manuelle Nachforschungen verdächtiger Transaktionen investiert werden; ebenso wie die Zahl der Kontrollen, die den Kunden auf seiner Customer Journey behindern.

**Anonymisierte Verhaltensbiometrie – Datenschutz zu Lasten der Genauigkeit**

Eine Vielzahl unterschiedlicher verhaltensbiometrischer Authentifizierungsverfahren ist mittlerweile erhältlich. Doch haben fast alle Lösungen eine Schwachstelle: die Verhaltensdaten der Nutzer werden in einer Cloud gelagert und verarbeitet. Innerhalb der EU gilt für Unternehmen der Finanzbranche, dass sie ein Outsourcing in die Cloud nur dann durchführen dürfen, wenn sie zuvor die Sicherheit und den Schutz ihrer Daten technisch sichergestellt haben. Dies bedeutet im Regelfall: die Verhaltensdaten werden vor ihrer Weitergabe an den Anbieter anonymisiert. Dadurch verliert das Authentifizierungsverfahren jedoch an Genauigkeit, steigt die Equal Error-Rate (EER) und es bleiben mehr Betrugsversuche unentdeckt.

Einen Ausweg aus diesem Dilemma bietet das verhaltensbiometrische Authentifizierungsverfahren von BehavioSec. Die vom Nutzer erhobenen Verhaltensdaten werden hier zunächst in eine Varianz – eine Verteilung um einen Mittelwert – überführt und erst

danach in einem Verhaltensprofil gespeichert und verarbeitet. Das Verhaltensprofil besteht somit ausschließlich aus Varianzen anwendungsspezifischen Verhaltens – und nicht aus konkreten Daten, die Rückschlüsse auf die Identität des Nutzers geben könnten. Mehr zum Thema Datenschutz erfahren Leser im 2021 Global Data Privacy Regulation of Physical & Behavioral Biometrics Report von BehavioSec.

Das Verfahren kann über On-Premises und über die Cloud betrieben werden. Die Datenübertragung zwischen Kunde und Hersteller erfolgt dabei verschlüsselt; die Speicherung ebenfalls verschlüsselt auf einem separaten, isolierten Konto innerhalb einer VPC-Instanz; das Hosting über ein isoliertes Subnetz. Selbst wenn es einem Angreifer gelingt, sich Zugriff auf die Daten zu verschaffen, kann er sie, da sie ja nur in Form von Varianzen vorliegen, nicht missbrauchen. Das konkrete Nutzerverhalten bleibt ihm verborgen. Selbstverständlich können alle erhobenen Verhaltensdaten vor ihrer Speicherung und Bearbeitung auch noch zusätzlich anonymisiert werden; so dass beispielsweise nur noch das Timing eines Tastenanschlags, nicht aber mehr der konkrete Tastenanschlag selbst in die Analyse einfließt. Das Verfahren verliert dann natürlich – wie die oben erwähnten Cloud-basierten Konkurrenzverfahren – an Genauigkeit.

Beste Ergebnisse lassen sich nun einmal nur mit der Speicherung und Verarbeitung nicht anonymisierter Daten erzielen. Denn so kann Nutzerverhalten nicht nur genauer, sondern auch kontextbasierter analysiert werden. Standort, IP-Adresse, Endgerät, Uhrzeit und weitere Kontextfaktoren können dann mit den verhaltensbiometrischen Faktoren verknüpft und zu einer kontextbasierten Verhaltensbiometrie erweitert werden. Wird die Lösung On-Premises eingesetzt, verbleiben alle Verhaltensdaten vor Ort und werden allein auf den Servern gespeichert sowie verarbeitet. Beim Abgleich der Verhaltensdaten eines Nutzers mit seinem Profil finden nicht allein dessen gespeicherte Varianzen, sondern auch Big Data-Analyseergebnisse zu den Varianzen in der Cloud gespeicherter Verhaltensgruppen Berücksichtigung. Das Ergebnis: eine noch geringere EER und ein signifikant beschleunigtes Training von Neuprofilen.

**Fazit**

Dank dieser innovativen Herangehensweise arbeiten verhaltensbiometrische Technologien deutlich effizienter – und sicherer – als konkurrierende verhaltensbiometrische Verfahren. Die Bedrohungslage bleibt dynamisch. Unternehmen werden ihre Schutzmaßnahmen deshalb ausbauen müssen.

Dr. Torben Gülstorff

## Mehr als eine digitalisierte Unterschrift – Was steckt hinter der elektronischen Signatur?

Wie lassen sich Geschäfte und Dienstleistungen sicher und rechtsverbindlich im digitalen Raum abwickeln? Das ist keine neue Frage, doch im Zuge der Pandemie wurde sie nochmals dringender. Vor die Wahl gestellt, digital anbieten oder gar nicht anbieten, suchen Unternehmen nach Alternativen zur klassischen Unterschrift auf Papier. Mario Voge, Lead Strategic Growth Manager Europe bei Swisscom Trust Services, zeigt, wie elektronische Signaturen hier helfen und beleuchtet deren technischen Hintergrund.

Es gibt eine Vielzahl von Dokumenten, die unterschrieben werden müssen, seien es Arbeitsverträge, Kreditanträge oder im medizinischen Bereich beispielsweise Rezepte. Das führt oft dazu, dass Dokumente per Post hin und hergeschickt werden, was Zeit und Kosten bedeutet. Oder es wird auf Behelfslösungen zurückgegriffen, wie das Einscannen unterschriebener Papiere. Das ist im Zweifel und bei späteren Prüfungen nicht rechtssicher. Mit der elektronischen Signatur gibt es eine Alternative, die sich direkt in digitale Prozesse einbinden lässt. Eine flächendeckende Verbreitung hat sie bisher noch nicht gefunden, aber der Druck zur Nutzung und die Nachfrage steigen immens. Das liegt einerseits an der fehlenden Bekanntheit, andererseits gibt es immer noch rechtliche Bedenken und Sorgen in Bezug auf die Zukunftsfähigkeit. Mit den hohen Hürden, die der Gesetzgeber vorgibt und der modernen Krypto-Technik, die heute zur Verfügung steht, sind diese aber unbegründet.

**Rechtliche Anforderungen an elektronische Signaturen**

Für den Rechtsraum der Europäischen Union werden elektronische Signaturen in der eiDAS-Verordnung definiert. Vereinfacht gesagt, unterscheidet diese zwischen den drei Stufen einfache, fortgeschrittene und qualifizierte elektronische Signatur. Wichtig zu wissen ist hierbei, dass nur die qualifizierte elektronische Signatur (QES) einer händischen Unterschrift gleichgestellt ist. Im Zweifel muss sie vor Gericht auch widerlegt und nicht bewiesen werden. Die QES ist in der eIDAS-Verordnung definiert als „eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht“. Für die fortgeschrittene elektronische Signatur muss wiederum gelten: „Sie ist eindeutig dem Unterzeichner zugeordnet. Sie ermöglicht die Identifizierung des Unterzeichners. Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann. Sie

ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann."

**Erstellung von Signaturen in der Praxis**

Für die Erstellung einer elektronischen Signatur wird aus dem zu signierenden Dokument ein Hashwert (Komprimat) nach einem kryptografischen Algorithmus gebildet. Im nächsten Schritt wird in einer sichereen auditierten Umgebung ein Schlüsselpaar mit zwei Schlüsseln (einer davon ist öffentlich, der andere privat) generiert. Mit dem privaten Schlüssel wird die Signatur (Willensbekundung) ausgeführt und der öffentliche Schlüssel wird mit den Nutzerdaten angereichert und mit einer Bestätigung durch einem Trust Service Provider (Trust Center) bestätigt, dass sog. Zertifikat.. Dabei wird sowohl der mit dem privaten Schlüssel signierte Hash als auch der öffentliche Schlüssel, inkl. dem Zertifkatan das Dokument „geheftet" und können mit diesem verschickt werden. Der Dabei hat der Empfänger die Möglichkeit, die Authentizität der Signatur und Integrität des Dokumentes durch den öffentlichen Schlüssel im angehefteten Zertifikat zu prüfen. Sollte beispielsweise das Ausgangs-dokument verändert werden, würde sich auch der Hashwert ändern – der öffentliche Schlüssel ist nicht mehr in der Lage, das Dokument zu entschlüsseln.

Swisscom Trust Services bietet ein Dreieck aus elektronischer Signatur, ID und Key. Unter der ID versteht man dabei die digitale Identität, die eindeutig identifiziert werden soll. Der Key ist das Sicherheitswerkzeug, mit dem die Willensbekundung durchgeführt wird (wie beispielsweise das Smartphone) und die Signatur ist schließlich das Ergebnis nach dem Auslösen dieser Willensbekundung.

**Die Technik im Hintergrund**

Das Kernstück der QES bildet auf der technischen Seite die in der eIDAS-Verordnung vorgegebene qualifizierte elektronische Signaturerstellungseinheit, die durch die Aufsichtsstelle des jeweiligen EU-Staates auditiert werden muss. Das ist konkret ein Hardware-Sicherheitsmodul (HSM), in dem Schlüssel erzeugt und sicher verwahrt werden können. Diese Technologie mit höchsten Sicherheitsstandards ist beispielsweise auf dem Gebiet der Kredit- und Debitkartenausgabe schon lange etabliert und erprobt.

Das hohe Sicherheitsniveau durch HSM ist nötig, da die elektronische Signatur auf asymmetrischer Kryptografie mit einem öffentlichen und einem privaten Schlüssel basiert (s.o.). Dieses Verfahren setzt einerseits voraus, dass der private Schlüssel unter allen Umständen geheim bleiben muss, in einer hochsicheren zertifizierten (auditierten) Umgebung aufbewaht wird. Daher wird er im HSM abgelegt, dass durch physische Trennung einen starken Schutz gegen Angriffe von außen aufweist – im Gegensatz zu alternativen Software-Lösungen. Auf der anderen Seite müssen die Algorithmen, die die Beziehung zwischen privatem und öffentlichen Schlüssel herstellen, entsprechend komplex sein. Ansonsten könnte der private Schlüssel aus dem öffentlichen errechnet werden.

**Gefahr durch Quantencomputer?**

Dass Verschlüsselungsalgorithmen geknackt werden, ist eine nicht unrealistische Gefahr, so geschehen beim Hash-Verfahren SHA-1. Um diesen Vorfall einzuordnen muss man bedenken, dass der Algorithmus schon relativ alt ist und bereits als „angeschlagen" galt. Nichtsdestotrotz benötigte die Entschlüsselung mehr als 6.500 CPU-Jahre und nochmal 100 GPU-Jahre – eine technologische Kraftanstrengung also. Aktuell werden aber an verschiedenen Stellen Quantencomputer entwickelt. Bis diese in der Praxis verfügbar sind, werden noch einige Jahre vergehen, doch bereits heute steht fest, dass ihre Rechenleistung konventionelle Supercomputer in den Schatten stellen wird. Frei nach Murphys Gesetz ist davon auszugehen, dass Quantencomputer früher oder später auch für Angriffe auf kryptografische Verfahren genutzt werden. Algorithmen, die heute noch als sehr sicher gelten, könnten dann binnen Minuten oder gar Sekunden geknackt werden. Darauf muss man sich bereits heute vorbereiten und auf dem Gebiet der sogenannten Post-Quanten-Kryptografie wird auch intensiv geforscht. Lösungen, die quantensichere Algorithmen verwenden, sind auch bereits auf dem Markt erhältlich.

Ein Problem, das vermutlich bislang kaum jemand vor Augen hat, sind veraltende Signaturen. Sind Dokumente, die nach dem heutigen Stand der Technik signiert werden, auch noch in zehn Jahren sicher? Kommt es bis dahin zum Durchbruch der Quantencomputer, muss man diese Frage mit Nein beantworten. Deshalb wird es in Zukunft darauf ankommen, digital signierte Dokumente, die einer Aufbewahrungspflicht unterliegen, regelmäßig nach dem aktuellen Stand zu „re-signieren". Dieses Problem kann allerdings mit dem Anhängen von Zeitstempelservices, auch Long Time Validation (LTV) genannt, gelöst werden. In der Praxis bedeutet das: Erstellte und signierte Dokumente können so auch in 20 Jahren als verbindlich eingestuft und geprüft werden, da zum Zeitpunkt der Unterschrift, der LTV-Bestätigung, die Signatur und alle vorgelagerten Prozesse, also Identifizierung, Schlüsselerzeugung und Zertifikatserstellung, korrekt waren.

Wenn die Sicherheitsmechanismen stets der aktuellen Entwicklung angepasst werden, haben Unternehmen allerdings mit der elektronischen Signatur ein hochsicheres Verfahren zur Verfügung, das die vollumfängliche Digitalisierung von Geschäftsprozessen und Kundeninteraktionen ermöglicht.

Mario Voge

**Mario Voge, Lead Strategic Growth Manager, Swisscom Trust Services**

# Risiko Cloud-Migration: Wie man Zugriffe auf Cloud-Ressourcen absichert und überwacht

**Stefan Schweizer, Vice President of Sales DACH, ThycoticCentrify**

Die Corona-Pandemie – und vor allem der damit verbundene Homeoffice-Boom – hat sich in den vergangenen 12 Monaten als wahrer Cloud-Treiber erwiesen. So setzen heute mehr Unternehmen denn je auf einen Cloud-first-Ansatz und ziehen Cloud-Bereitstellungsoptionen traditionellen On-Premises-Lösungen vor. Wie der aktuelle State of Cloud Report 2021 zeigt, sollen in den kommenden 12 Monaten bereits 55 Prozent aller Workloads in der Cloud ausgeführt werden. Die Anzahl der genutzten Cloud-Apps pro Unternehmen stieg laut Netskope Cloud & Threat Report allein im letzten Jahr um 20 Prozent. So nutzen Unternehmen mit 500 bis 2.000 Mitarbeitern im Durchschnitt 664 verschiedene Cloud-Apps pro Monat.

Die positiven Auswirkungen der Cloud-Initiativen – von einer erhöhten Agilität und Effizienz bis hin zu relevanten Kosteneinsparungen – sind für die Unternehmen dabei meist recht schnell spürbar. Doch bei der Geschwindigkeit, mit der viele von ihnen die Cloud-Migration angegangen sind, treten auch neue Sicherheitsrisiken zu Tage. Privileged Access Management (PAM), das gezielt auf die Herausforderungen der Cloud ausgerichtet ist, hält diese Risiken jedoch gut unter Kontrolle.

**Identitäten sind der neue Sicherheitsperimeter**

Ein Hauptproblem im Zusammenhang mit der raschen Cloud-Einführung ist die daraus resultierende starke Zunahme an privilegierten Accounts und Berechtigungsnachweisen, was es den IT-Teams immer schwieriger macht, diese angemessen zu verwalten und abzusichern. Hinzu kommt, dass immer mehr Mitarbeiter von Zuhause aus arbeiten und die Verwaltung kritischer Infrastrukturen und Entwicklungsplattformen sowie der Zugriff auf ständig neue und aktualisierte Webanwendungen außerhalb der geschützten Unternehmensumgebung stattfinden. Werden diese sensiblen Cloud-Zugriffe ausschließlich über einfache Passwörter geschützt, haben Cyberangreifer leichtes Spiel. Wie der 2021 Data Breach Investigations Report von Verizon ermittelt hat, sind 77 Prozent der Sicherheitsverletzungen in der Cloud kompromittierten Zugangsdaten geschuldet.

Hier bedarf es eines Umdenkens: Unternehmen müssen verstehen, dass traditionelle on-premises-Sicherheitslösungen allein nicht ausreichen, um auch Cloud-Umgebungen angemessen zu schützen, und dass der neue Sicherheitsperimeter in Identitäten und privilegierten Zugriffen selbst liegt. Konzentrieren sich Unternehmen weiterhin darauf, ihre verbleibenden on-premises-Legacy-Systeme einfach in die Cloud zu verlagern, werden sie früher oder später ein böses Erwachen erleben. Wer auch seine Cloud und alle darüber zugänglichen Systeme und Daten geschützt wissen will, muss vielmehr von Anfang an starke Authentifizierungs-, Autorisierungs- und Zugriffskontrollen für Benutzer einbauen, die gemäß deren individuellen Rollen und Aufgabenbereichen definiert werden. Privileged Access Management ist für die Umsetzung dieser Kontrollen von zentraler Bedeutung.

**Die Vorteile von PAM bei der Cloud-Migration**

Für viele Unternehmen ist der Umzug in die Cloud etwas, das sich einfach nicht aufschieben lässt. Insbesondere dann, wenn man davon ausgeht, dass der Großteil der Belegschaft auch weiterhin (teilweise) von zu Hause aus arbeiten wird. Für Security-Teams bedeutet dies, dass sie privilegierte Zugriffe im Rahmen der fortschreitenden Cloud-Migration gezielt adressieren müssen, um sensible Daten weiterhin angemessen zu schützen, Compliance zu gewährleisten und unbefugten Zugriff auf Systeme zu verhindern.

Sichtbarkeit muss dabei das Herzstück der Cloud-Sicherheitsstrategie sein, und diese muss ständig aufrechterhalten werden. Ein gelegentlicher Discovery-Scan von privilegierten Konten reicht längst nicht aus, denn er bietet schlicht nicht die Transparenz, um alle Risiken fortlaufend unter Kontrolle zu halten. Eine kontinuierliche automatisierte Erkennung aller Arten von Cloud-Konten ist für die Teams hier unerlässlich. Nur so kann sichergestellt werden, dass die Berechtigungen richtig konfiguriert sind und eine angemessene Aufsicht besteht.

**Monitoring – Privilegien von Mitarbeitern und Drittanbietern im Blick haben**

Eine weitere wichtige Maßnahme bei der Absicherung von Cloud-Diensten ist das Monitoring. Obwohl die überwiegende Mehrheit der Benutzer vertrauenswürdig ist, sollte das Verhalten derjenigen, die auf sensible Informationen und privilegierte Konten zugreifen, dennoch überwacht und geprüft werden. Dazu gehört unter anderem das Überwachen des Netzwerkverkehrs auf ungewöhnliche Aktivitäten, wie z. B. Zugriffe außerhalb der üblichen Geschäftszeiten, von ungewöhnlichen Orten oder andere ausgehende Aktivitäten. Zudem können Unternehmen gezielt nach Anzeichen für eine Kompromittierung suchen, indem sie zusätzliche dynamisch Sicherheitskontrollen für den privilegierten Zugriff verlangen, wie etwa einen Zero-Trust-Ansatz, der eine kontinuierliche Verifikation erfordert.

Gleichzeitig ist es wichtig, die Überwachung nicht nur auf die eignen Mitarbeiter zu beschränken, sondern auch die Partner im Blick zu haben. Der Großteil der Unternehmen arbeitet heutzutage auf verschiedene Weise mit Drittanbietern zusammen. Dazu zählen externe Auftragnehmer, die an zeitlich begrenzten Projekten arbeiten, fest integrierte Auftragnehmer oder Personal aus der Mitarbeiterüberlassung. Ihre

privilegierten Zugriffe nicht zu überwachen, würde große Sicherheitsrisiken bedeuten.

Eine weitere essenzielle Maßnahme, um das Missbrauchsrisiko zu minimieren und widerstandsfähiger zu werden, ist das Einschränken von Zugriffen nach dem Just-in-Time-Prinzip. Das bedeutet, das Zugriffe nur ein einem eng begrenzten und für den jeweiligen Benutzer definierten Zeitraum, und niemals dauerhaft, gewährt werden. Viel zu viele Unternehmen halten Privilegien viel zu lange aufrecht, versäumen es, Passwörter und Konten auslaufen zu lassen und Privilegien zu löschen, wenn diese nicht mehr gebraucht werden, z.B. wenn Projekte enden oder Mitarbeiter ausscheiden. Das Gewähren von dauerhaftem privilegiertem Zugriff verstößt gegen das Least Privilege-Prinzip und birgt unkontrollierbare Risiken. Deshalb empfiehlt sich der Einsatz von PAM-Lösungen, die es Unternehmen ermöglichen, privilegierten Zugriff in Echtzeit oder aber nur bei Bedarf zu gewähren.

**Die eigenen Cloud-Verantwortlichkeiten im Blick behalten**

Bei der Absicherung der Cloud ist es zudem wichtig, die eigenen Verantwortlichkeiten genau zu kennen. Viele Unternehmen sind sich nicht bewusst, dass die meisten Cloud-Fehlkonfigurationen und inkonsistenten Kontrollen rechtlich gesehen die Schuld des Nutzers sind, nicht die des Cloud-Anbieters. Nur in seltenen Fällen kann es zu einer Mithaftung kommen, so dass es auch im Interesse des Cloud-Anbieters liegt, ihren Kunden bei der Umsetzung von Security-Best-Practices zu helfen. Die Hauptverantwortung liegt jedoch tatsächlich auf den Schultern des Unternehmens. Sie müssen dafür sorgen, dass Zugriffe und Berechtigungen für jede Identität und jedes System, das mit Cloud-basierten Systemen interagiert, angemessen verwaltet und geschützt werden.

Zu diesen Systemen können kritische Anwendungen oder Datenbanken gehören, die in der Cloud gespeichert sind, Plattformen für die Anwendungsentwicklung oder Tools, die von den Business- oder Technik-Teams verwendet werden. Unter Berücksichtigung dessen sollte der Cloud-Zugriff mit denselben PAM-Richtlinien, -Prozessen und -Lösungen, die für das gesamte Unternehmen verwendet werden, eingebunden und geprüft werden.

Dabei müssen die Unternehmen auch Veränderungen im Blick haben und in ihre Sicherheitsstrategie einplanen. Das zeigt auch der vermehrte Einsatz von Cloud-Services: So nutzen Unternehmen heute durchschnittlich etwa 2.000 Cloud-Dienste und damit bereits 15 Prozent mehr als noch im letzten Jahr, was hauptsächlich auf das Wachstum von SaaS zurückzuführen ist.

So schnell digitale Transformationsprojekte derzeit an Tempo gewinnen, so gut kann PAM hier helfen. In DevOps-Unternehmen, in denen eine breite Palette an Cloud-Ressourcen kontinuierlich und in großem Umfang erstellt, verwendet und wieder lahmgelegt wird, unterstützt PAM durch die Automatisierung der schnellen Erstellung, Archivierung, Abfrage und Rotation von Secrets.

**Fazit**

In Zeiten einer verschärften Bedrohungslandschaft und zunehmender Cyber-Angriffe kann PAM die Arbeit von IT- und Security-Abteilungen erheblich vereinfachen. So verschafft PAM nicht nur einen besseren Überblick über hybride On-Premises- und Multi-Cloud-Umgebungen, Daten und Infrastrukturen sowie Privilegien im Allgemeinen. Ein gut durchdachtes PAM ermöglicht es auch, granulare Kontrollen, die eine kontinuierliche Authentifizierung und sichere Autorisierung unterstützen, über verschiedene Umgebungen hinweg einzurichten und umzusetzen. Gleichzeitig sorgt eine starke PAM-Strategie für eine klarere Auditierbarkeit, indem sie die Einhaltung von Vorschriften und Compliance erleichtert.

Inmitten der ständigen Transformation, die durch Covid-19 noch stärker vorangetrieben wird, und die den Einsatz von immer mehr Cloud-Diensten forciert, kann PAM Unternehmen eine zusätzliche wertvolle Sicherheitsebene bieten. Indem präzise gesteuert wird, was Benutzer in Cloud-Plattformen, -Diensten und -Anwendungen sehen und tun können, können Unternehmen die Angriffsfläche reduzieren und letztlich die Herausforderungen der Cloud-Sicherheit meistern.

Stefan Schweizer

# 1.7 USE CASES

## Gesundheitswesen: Wie Unternehmen ihre Cybersecurity während der schnellen Digitalisierung sicherstellen

Das Gesundheitswesen befindet sich schon seit einiger Zeit inmitten der digitalen Transformation – die COVID-19 beschleunigt den Einsatz von Cloud-Services und digitalen Tools zusätzlich. Eine weitere Veränderung der Branche: Immer mehr digital native sogenannte „Health-Tech"-Unternehmen drängen auf den Markt und ermöglichen die Digitalisierung gesundheitlicher Dienstleistungen.

Die Vorteile der digitalen Transformation sind in der Branche unumstritten, dennoch wird gerade das Gesundheitswesen immer mehr zum Angriffsziel von Cyber-Attacken. Besonders in diesem Bereich können Cyber-Angriffe gravierende Folgen haben: Neben den Auswirkungen auf das angegriffene Unternehmen oder Institution, können ebensolche Attacken im Zweifelsfall

zu Verzögerungen bei der medizinischen Versorgung oder gar zum Verlust von Menschenleben führen.

Seit Beginn der COVID-19-Pandemie ist das Gesundheitswesen noch stärker in den Fokus der Hacker gerückt, um die anfällige Phase gezielt auszunutzen. Ein Beispiel aus den USA: Das U.S. Department of Health and Human Services berichtete vor Kurzem einen Anstieg von 50 Prozent bei den Verstößen gegen die Cybersecurity von Krankenhäusern und Netzwerken von Gesundheitsdienstleistern – dies deutet auf eine verstärkte Ausrichtung auf die Gesundheitsbranche hin. In Düsseldorf legte im September 2020 ein Ransomware Angriff das Universitätsklinikum lahm und führte zum Tod einer Patientin.

Die IT-Systeme des Gesundheitswesens sind einem erhöhten Sicherheitsrisiko ausgesetzt, denn immer mehr Endanwender setzen auf Technologien wie Telemedizin oder spezielle Gesundheits-Apps – und teilen damit sensible, persönliche Daten. Darüber hinaus besteht ein Großteil der medizinischen Infrastruktur aus veralteten und heterogenen Systemen mit offensichtlichen Sicherheitseinschränkungen.

**Vishal Salvi, Chief Information Security Officer & Head of Cyber Security Practice, Infosys**

Aber auch die Branche selbst ist ein attraktives Ziel für Cyber-Angriffe: Gesundheitsdienstleister bieten vermehrt Telemedizin, Apps, Services und vernetzte Endgeräte an und generieren damit große Datenmengen an sogenannten Protected Health Information (PHI). Diese sensiblen Daten werden im Dark Web hoch gehandelt. Und auch hochwertige Assets wie die Forschung und Entwicklung von Impfstoffen sind wertvolle Ziele für kommerzielle und politische Zwecke.

Das Gesundheitswesen ist ohne Zweifel systemrelevant und eine kritische Dienstleistung. Sowieso schon am Anschlag müssen Gesundheitsorganisationen und Dienstleiser mitten in der Pandemie ihre Sicherheit verbessern und die Cybersecurity stärken. Während die meisten Cybersicherheitslösungen branchenunabhängig sind, gibt es bestimmte Nuancen, die die Gesundheitsbranche berücksichtigen muss.

**IT-Hygiene**

Organisationen des Gesundheitswesens müssen einen „Null-Toleranz-Ansatz“ in Sachen IT-Hygiene verfolgen und dabei für die notwendigen Systeme und Steuerung beim Risikomanagement von Dritten sorgen. Dabei müssen die vorhandenen Richtlinien für Hochrisikosysteme wie Lebenserhaltungssysteme oder sensible Assets wie Impfstoffversuche drastisch verschärft werden.

Organisationen sollten sich strikt an die Software- und Hardware-Security halten, indem sie etwa für aktuelle Anwendungen und Betriebssysteme sorgen, veraltete oder nicht unterstützte medizinische Geräte austauschen und Sicherheitsmaßnahmen für remote vernetzte Geräte implementieren.

**Zero Trust-Modell**

Mit der zunehmenden Verbreitung der Telemedizin und der vermehrten Remote-Arbeit von Fachkräften im Gesundheitswesen reicht es nicht mehr aus, ausschließlich die Sicherheit der Perimeter zu gewährleisten – vielmehr benötigen Unternehmen neue, belastbare Modelle, die an die neue Umgebung angepasst sind.

Organisationen des Gesundheitswesens sollten generell nur limitiert Privilegien vergeben. So erhalten beispielsweise ausschließlich Personen Zugriff auf Daten, die sie für die Erledigung ihrer Aufgaben benötigen. Darüber hinaus sollten nur notwendige Anwendungen für den Remote-Zugriff freigegeben werden. Mithilfe von Netzwerksegmentierung können Firmen außerdem sicherstellen, dass geschäftskritische Systeme – etwa zur Lebenserhaltung oder für Forschung und Entwicklung – vom restlichen IT-Setup separiert sind.

**Datensicherheit**

Unternehmen sollten sich auf Datenminimierung konzentrieren. Auf diese Weise werden nur unbedingt notwendige Daten gesammelt, verarbeitet und (wenn möglich) anonymisiert. Um die Sicherheit sensibler Daten wie PHI sowie Forschungs- und Entwicklungs-Assets sowohl im Ruhezustand als auch bei der Übertragung zu gewährleisten, müssen Unternehmen automatisierte Systeme zur Datenidentifizierung und -klassifizierung sowie zur Vermeidung von Datenverlusten aufbauen.

Die Gesundheitsbranche muss zudem auch strengere Datenzugriffskontrollen einführen. Diese beschränken den Zugriff nur auf die Einzelperson und den Gesundheitsdienstleister sowie gegebenenfalls auf eine Regierungsbehörde, um die kommunale Gesundheitsversorgung wie im Fall von COVID-19 zu verwalten. Hochentwickelte Verschlüsselungsstandards sowie Data Masking-Lösungen und regelmäßige Kontrollen gewährleisten darüber hinaus, dass nur autorisierte Benutzer Zugriff erhalten.

**Secure by Design**

Moderne Unternehmen müssen sicherstellen, dass Cybersecurity bereits in der Entwicklungsphase berücksichtigt wird (Security by Design) und nicht erst im Nachhinein. Dies erfordert die Etablierung sicherer Kodier-Richtlinien und die Einführung von Praktiken wie DevSecOps.

Ebenso ist ein fortlaufendes Compliance-Management mit Echtzeit-Patching und Fokus auf Bedrohungen, Schwachstellen, Risiken und Vorfällen essenziell. Auch die Mitarbeiter müssen involviert werden: Nur mit einem fundierten Verständnis und Sensibilität für IT-Security können Mitarbeiter Sicherheitsrisiken intuitiv entschärfen – eine starke Security-Unternehmenskultur rundet dies ab.

**Compliance und Risk Management**
Das Ökosystem des Gesundheitswesens besteht aus einer Vielzahl von Partnern und Anbietern innerhalb der Wertschöpfungskette. In dieser vernetzten – aber ungleichen – Struktur muss jeder Beteiligte individuell für Cybersecurity sorgen.

Unternehmen müssen effektive Partner-Risikomanagement-Programme entwickeln und implementieren, um Daten zu sichern und vor Cyberangriffen zu schützen. Dies kann durch eine Bewertung der Sicherheitslage von Partnern erreicht werden, gefolgt von einer risikobasierten Partnersegmentierung sowie der Definition an „Zero-Trust"-Prinzipien in Sachen Konnektivität und Zugriffsmanagement für Partner.

**Managed Detection und Response**
Die Cyber-Bedrohungslandschaft entwickelt sich stetig weiter. Dies führt dazu, dass fast jeden zweiten Tag neue Bedrohungen auftauchen. Daher ist ein gut definiertes Playbook für die schnelle Erkennung von Bedrohungen und Sicherheitsverletzungen und die Reaktion darauf entscheidend.

Organisationen des Gesundheitswesens müssen KI-Systeme mit Machine Learning und Verhaltensanalysen einsetzen, um Anomalien und Bedrohungen proaktiv zu erkennen und schnelle Sandboxing- und Wiederherstellungsprozesse zu entwickeln. Nur dann können sie sich „cyber-resilient" (widerstandsfähig) aufstellen und schützen.

Vishal Salvi

## Cyber-Risiko Lieferkette: Warum die Cybersecurity Ihrer Partner auch Ihre Angelegenheit ist

Die Zahl der Cyberangriffe auf Industrieanlagen aller Größenordnungen nimmt seit Jahren deutlich zu. Dabei erstreckt sich das Risiko über die gesamte Lieferkette. Eine Studie mit 150 Cybersecurity- und IT-Fachleuten in mittelständischen und großen Unternehmen der Fertigungsindustrie hat unlängst gezeigt, dass jede zweite OT-Infrastruktur für Cyberangriffe anfällig ist. 53 Prozent der Befragten gaben zudem an, dass ihr Unternehmen in den letzten 12 bis 24 Monaten bereits von einem Cyberangriff oder einem anderen Sicherheitsvorfall betroffen war, der auch die OT-Netzwerke beeinträchtigte.

Moderne Lieferketten sind längst komplizierte, miteinander verflochtene Partnernetzwerke. Und wenn ein Partner kompromittiert wird, hat dies Auswirkungen auf alle Partner in der Lieferkette. Die Auswirkungen eines Angriffs auf einen First-Tier-Lieferanten können dabei genauso verheerend sein, wie ein Angriff auf die eigenen Systeme: Ganze Produktionslinien können ausfallen, was erhebliche Kosten verursacht, sich negativ auf den Umsatz auswirkt und den Ruf des Unternehmens schädigt.

Seit Jahren nutzen Angreifer Schwachstellen in der Lieferkette als Sprungbrett, um andere Unternehmen zu infiltrieren. Vielleicht erinnert sich so mancher noch an den Datenvorfall beim US-amerikanischen Handelsunternehmen Target vor knapp zehn Jahren. Hier haben Angreifer gestohlene Zugangsdaten eines Klimaanlagen-Herstellers genutzt, um auf das Netzwerk von Target zuzugreifen und sich lateral zu bewegen. Das Ergebnis: Millionen gestohlener Kundendaten, inklusive Zahlungsinformationen. Ein paar Jahre später sahen wir mit der Ransomware NotPetya einen weiteren hochkarätigen Angriff auf die Lieferkette, der zunächst Software einer ukrainischen Buchhaltungsfirma infizierte. Im weiteren Verlauf wurden multinationale Unternehmen getroffen und es entstand ein geschätzter Gesamtschaden von 10 Milliarden US-Dollar. Und erst kürzlich ermöglichte die Kompromittierung der SolarWinds Orion-Software und die SUNBURST-Backdoor Angreifern den Zugang zu zahlreichen Unternehmen und Behörden auf der ganzen Welt. Das Ausmaß und die Auswirkungen dieses Angriffs sind derzeit noch nicht abzusehen.

**Yaniv Vardi, CEO, Claroty**

**Maßnahmen der Industrie**
Cybersicherheit in der Lieferkette wird mittlerweile als bedeutendes Thema von Führungskräften und Sicherheitsverantwortlichen in (nahezu) allen Branchen wahrgenommen. Entsprechend ergreifen Behörden, Branchenverbände und Regulierungsbehörden Maßnahmen, um das Risiko zu minimieren. Als ein Impfstoff für COVID-19 in greifbare Nähe rückte, gab IBM eine Warnung vor unbekannten Bedrohungsakteuren heraus, die auf die Lieferkette für den Impfstoff COVID-19 zielen. Die Security-Experten wiesen dabei besonders auf die gestiegenen Fähigkeiten von Angreifern sowie die Dringlichkeit und Schwere des Lieferketten-Risikos hin und mahnten, die Gefährdung von OT-Umgebungen zu reduzieren. Ab Juli 2024 werden neue Cybersecurity-Vorschriften für die Automobilindustrie für alle in der Europäischen Union produzierten Neufahrzeuge verpflichtend sein. Entsprechend sind derzeit neue Cybersicherheitsstandards zur Etablierung von „Cybersecurity by Design" über den gesamten Lebenszyklus eines Fahrzeugs in der Entwicklung.

**Was Sicherheitsverantwortliche tun können**
Cyber-Risiken in der Lieferkette sind kompliziert und erstrecken sich über den gesamten Lebenszyklus eines Produkts – von der Entwicklung über die Herstellung, den Vertrieb und die Lagerung bis hin zur Wartung. Je umfangreicher und komplexer der Lebenszyklus ist, desto mehr Angriffsmöglichkeiten und Chancen, ein schwaches Glied in der Kette zu finden und auszunutzen, gibt es. Und da Lieferketten oft global sind und mehrere Ebenen von Lieferanten umfassen, liegt

die Verantwortung für die Sicherheit nicht bei einem einzelnen Unternehmen. Jeder Partner muss hier involviert sein, wodurch die Reduzierung von Cyber-Risiken in der Lieferkette eine besondere Herausforderung darstellt. Deshalb dürfen Führungskräfte bei der Erstellung von Business-Continuity-Plänen nicht nur ihr eigenes Unternehmen im Auge behalten. Sie müssen auch die Sicherheitsmaßnahmen ihrer unmittelbaren Zulieferer im Blick haben und einbeziehen, wie diese ihrerseits das Risiko mit ihrem erweiterten Netzwerk von Zulieferern verwalten und mindern. Diese fünf Schritte können dabei helfen:

**Kommunikation und Bewertung:** Das Management dieses kritischen Risikos beginnt mit der Festlegung der internen Verantwortung für das Procurement und die Überprüfung der Prozesssicherheit eines Partners. Hierbei müssen sowohl die Rechtsabteilungen als auch Technologie- und Fachabteilungsleiter in allen Geschäftsbereichen einbezogen werden. Führungskräfte benötigen verlässliche Bedrohungsdaten hinsichtlich der Angriffe auf die Lieferkette, um fundierte Entscheidungen über die Risiken für das Unternehmen zu treffen. Beschaffung und Datensicherheit müssen deutlich und effektiv an Partner und Stakeholder kommuniziert werden.

**Detaillierte operative Transparenz:** Dedizierte industrielle Cybersicherheitslösungen sind in der Lage, OT-spezifische Herausforderungen, wie den Mangel an standardisierter Technologie, die Verwendung proprietärer Protokolle und eine geringe Toleranz gegenüber Unterbrechungen kritischer Prozesse, zu adressieren. Eine Plattform, die kontinuierlich Bedrohungen im gesamten OT-Netzwerk überwacht und erkennt, sich mit dem bestehenden Sicherheitsnetzwerk Ihres Unternehmens verbindet und auch eine Verbindung zu allen Zugangspunkten mit Ihren Partnern in der Lieferkette herstellt, erweitert diese Transparenz auf alle relevanten Partner.

**Konsistente Cybersicherheitsstandards:** Halten Sie sich über neue Vorschriften (etwa das geplante IT-Sicherheitsgesetz 2.0) und Standards sowie neue Warnmeldungen auf dem Laufenden. Folgen Sie branchenspezifischen Empfehlungen und setzen Sie diese zügig um.

**Steigende Awareness:** Angesichts der kritischen Bedrohungslage hat sich das Bewusstsein vieler Führungskräfte und Vorstandsmitglieder für die Notwendigkeit von effektiver industrieller Cybersicherheit entwickelt, um so Produktivität, Verfügbarkeit, Zuverlässigkeit und Safety zu gewährleisten. Als Sicherheitsverantwortlicher sollten Sie den Moment nutzen, um funktions- und abteilungsübergreifende Unterstützung aktueller und zukünftiger industrieller Cybersicherheitsinitiativen zu erhalten.

**Kollaborativer Ansatz:** Ihre Lieferkette ist ein integraler Bestandteil des Ökosystems Ihres Unternehmens. Deshalb muss sie auch in Ihr Sicherheitsökosystem integriert werden und genauso effektiv geschützt werden, wie ihre „internen" Systeme. Cloud-basierte Lösungen vereinfachen die sichere Konnektivität mit wichtigen Partnern in der Lieferkette. Außerdem können sie die Sicherheit verbessern, einfacher aktualisiert und neue Funktionen schneller hinzugefügt werden. In manchen Branchen ist eine Cloud-Transformation aufgrund gesetzlicher Vorgaben noch nicht umsetzbar. Dennoch ist es auch hier möglich, Benchmarks festzulegen sowie Berichte und Erkenntnisse über Schwachstellen und die jeweiligen OT-Netzwerk-Sicherheitslevel mit den Partnern in der Lieferkette auszutauschen.

Wir sehen, dass die Cybersicherheit der gesamten Lieferkette eine gemeinschaftliche und durchaus herausfordernde Aufgabe ist, die nur durch Zusammenarbeit bewältigt werden kann. Glücklicherweise gibt es Maßnahmen, die jedes einzelne Unternehmen ergreifen kann, um das Risiko zu reduzieren. Es ist höchste Zeit, dies jetzt schnell anzugehen.

Yaniv Vardi

**Marcus Raitner ist überzeugt, dass Elefanten tanzen können. Als Agile Coach begleitet er deshalb Unternehmen auf ihrer Reise zu mehr Agilität und menschlicher Lebendigkeit. In seinem Blog „Führung erfahren!“ schreibt er seit 2010 über die Themen Führung, Agilität, Digitalisierung und vieles mehr.**

# Das postpandemische Büro als Ort der inspirierenden Begegnung

Kurzfristig hat die Corona-Pandemie die Arbeitswelt kräftig aufgerüttelt. Die spannende Frage ist nun in dieser Endphase der Pandemie, ob der Impuls ausreichend war, um langfristig die Arbeitswelt zu revolutionieren. Was wird bleiben von Remote Work und Homeoffice, wenn wir gelernt haben mit diesem Virus zu leben wie mit anderen auch? Werden wir dann wieder zum Status quo und in unsere präpandemischen Großraumbüros zurückkehren? Warum sollten wir das wollen?

Vor Corona fand „echte“ Arbeit nur im Büro statt, während Homeoffice die tolerierte Ausnahme für Mitarbeiter ohne Karriereambitionen war. Zu Hause zu arbeiten war immer ein wenig anrüchig und verdächtig. Seit fast zwei Jahren arbeiten nun die meisten Wissensarbeiter vornehmlich im Homeoffice oder gleich ganz woanders. Und es funktioniert für viele erstaunlich gut.

Nicht von der Hand zu weisen und mittlerweile lieb gewonnen sind zudem die Vorteile einer vorrangig verteilten Arbeitsgestaltung. Wer weniger Zeit auf dem Weg zwischen Home und Office verbringt, hat mehr Zeit für Work und Life. Und wenn Home gleich Office, ist Work gleich Life. Aus Work-Life-Balance wird Work-Life-Integration. Und das ist gut so, denn das Familienleben findet eben nicht nur vor 7:30 Uhr und nach 18:30 Uhr statt. Keine bahnbrechende Erkenntnis, aber gerade für viele Männer doch eine ganz neue Erfahrung.

Das Büro als den Ort, wo die Akten lagern und daher dort die Arbeit stattfinden muss, gibt es ohnehin schon lange nicht mehr. Über die letzten Jahrzehnte wurde die Arbeit immer digitaler. Trotzdem war der Zugriff auf diese digitalisierte Arbeit anfangs nur im Büro möglich, weil nur dort die Infrastruktur, der PC, das Netzwerk, der Zugang zum Mainframe, etc. war. All das ist mit flächendeckend schnellem Internet nun seit 10 bis 15 Jahren auch passé. Es gibt also rein technisch keinen Grund mehr, das Büro aufzusuchen. Die Arbeit kann an jedem beliebigen Ort mit Internet erledigt werden.

Es tritt nun eine andere Funktion des Büros in den Vordergrund. Wir Menschen sind nicht nur Maschinen für Wissensarbeit, sondern soziale Wesen. Wir unternehmen gerne etwas gemeinsam und wir inspirieren uns dabei gegenseitig. Der wichtigste Ort im Büro war deshalb vielleicht immer schon die Cafeteria. Die dort stattfindenden zufälligen Begegnungen und das mal kurze und mal längere Gespräch sind oft der entscheidende Zündfunke für eine neue Idee oder wenigstens das Schmiermittel für einen reibungsfreien Ablauf der Arbeit.

Vor Corona war diese soziale Komponente des Büros als Ort der kreativen menschlichen Begegnung zwar ganz angenehm, wurde aber eher als schmückendes Beiwerk gesehen. Jetzt, wo wir alles digitalisiert haben und an jedem Ort mit Internetanschluss arbeiten können, stellen wir fest, dass uns genau diese soziale Komponente stark verkümmert. Menschliche Begegnungen lassen sich nur schwer digitalisieren.

Das postpandemische Büro wird also zum Ort der inspirierenden menschlichen Begegnungen werden müssen. Menschen werden künftig das Büro viel weniger zum reinen Arbeiten aufsuchen oder um die Arbeit zu koordinieren. All das lässt sich virtuell viel angenehmer bewerkstelligen. Der wichtigste Grund für einen Besuch im Büro wird nach dieser Zeit der sozialen Distanz die Begegnung und der Austausch mit Kollegen sein. So wie früher am Ende eines Arbeitstags im Büro die Erschöpfung dominierte, sollte es künftig die Inspiration sein. Das Büro hat als reine Legebatterie für Wissensarbeiter jedenfalls ausgedient.

Gefragt sind jetzt Gestaltungskonzepte, die Lust auf Begegnungen machen und gemeinsame Kreativität fördern. Ein guter Anfang wäre vielleicht eine zentrale Cafeteria für lose Gespräche umringt von Ecken mit Whiteboards und Flipcharts für die spontane Vertiefung von Gesprächen. Vielleicht gibt es dann in der Nähe dieser modernen Agora auch größere Räume, wo Trainings, Vorträge oder ähnliches geboten wird. Ein attraktives Konzept, wo ich mir sicher sein kann, dass sich mein Weg ins Büro lohnt, weil ich inspiriert nach Hause gehen werde, könnte jedenfalls auch so manche sich anbahnende Vorschrift zu zeitweiser Anwesenheit im Büro ersetzen. Die Mitarbeiter werden kommen, weil es sich für sie lohnt und nicht weil es angeordnet wurde.

Foto: Privat


**Das Buch zum Manifest für menschliche Führung. Erhältlich als Taschenbuch und E-Book bei Amazon**

# FACHBEIRAT

**Patric Fedlmeier**
CIO Provinzial Rheinland

**Dr. Norbert Gaus**
Executive VP SIEMENS

**Dr. Sandro Gaycken**
Direktor ESMT

**Dr. Michaela Harlander**
Vorstand ISAR AG

**Dr. Markus Heyn**
GF Bosch

**Dr. Markus Hoffmann**
Google Quantum-AI

**Manfred Klaus**
Sprecher der GF Plan.Net

**Andrea Martin**
CTO IBM

**Dr. Niko Mohr**
Partner McKinsey

**Dr. Christian Plenge**
BL Messe Düsseldorf

**Frank Rosenberger**
Group Director TUI

**Dr. Ralf Schneider**
CIO Allianz Group

**Stephan Schneider**
Manager Vodafone

**Michael Zaddach**
Flughafen München

# IMPRESSUM

**REDAKTION**

**Chefredaktion** Claudia Linnhoff-Popien (V. i. S. d. P.)
**Chef vom Dienst** Robert Müller
**Fachbeirat** Patric Fedlmeier, Dr. Norbert Gaus, Dr. Sandro Gaycken, Dr. Michaela Harlander, Dr. Markus Heyn, Dr. Markus Hoffmann, Manfred Klaus, Andrea Martin, Dr. Niko Mohr, Dr. Christian Plenge, Frank Rosenberger, Dr. Ralf Schneider, Stephan Schneider, Michael Zaddach
**Redaktion** Steffen Illium, Hannes Mittermaier, Claudia Huber
**Redaktionsassistenz** Katja Grenner, Catarina Ilg, Emilia Maierhofer
**Mitarbeiter dieser Ausgabe** Thomy Phan
**Schlussredaktion** Hannes Mittermaier

**ANFRAGEN AN DIE REDAKTION**

redaktion@digitaleweltmagazin.de

**GRAFIK**

**Layout** Stefan Stockinger, www.stefanstockinger.com

**ANZEIGEN**

**Ansprechpartner**
redaktion@digitaleweltmagazin.de
Es gilt die gültige Preisliste, Informationen hierzu unter www.digitaleweltmagazin.de/mediadaten

**KOSTENLOS ERHÄLTLICH**

www.digitaleweltmagazin.de/magazin/
Ebenfalls online über SpringerLink (Berlin, Heidelberg, New York) erhältlich.
Alle Artikel werden von GoogleScholar indexiert.

**HERAUSGEBER**

Prof. Dr. Claudia Linnhoff-Popien, Institut für Informatik, Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 München,
Tel. +49 89 2180-9153, www.digitaleweltmagazin.de

**RECHTE**

DIGITALE WELT

# CALL FOR CONTRIBUTION

## für den DIGITALE WELT-Blog

Platzieren Sie Ihre Digitalthemen von morgen auf der Plattform von heute mit bislang über **2.810.000*** Beitragsaufrufen:

**digitaleweltmagazin.de/category/blog**


### Werden Sie Autor!

Ihre Vorteile im Überblick:

- ✓ Teilen Ihres Fachwissens mit einer breiten digitalen Leserschaft
- ✓ Potenzielle Veröffentlichung im **DIGITALE WELT** Magazin
- ✓ Bekanntheitssteigerung Ihres Unternehmens Mediale Positionierung von gezielten, für Sie relevanten Digitalthemen
- ✓ Aktive Beteiligung am aktuellen Dialog zur Digitalisierung
- ✓ Multiplier Effekt durch die Verbreitung über Social Media
- ✓ Profilschärfung und Positionierung gezielter Unternehmensvertreter

### Aktuelle Blog-Rubriken:

Quantum Computing, Human Resource, Machine Learning, Affective Computing, Internet of Things, Cyber Security, Blockchain u.v.a.m.

**INTERESSE GEWECKT?**

Melden Sie sich bei der **DIGITALE WELT**-Redaktion via E-Mail unter **redaktion@digitaleweltmagazin.de**

*Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/category/blog veröffentlicht und erzielten dabei die oben genannte Klickzahl im Zeitraum 01. August 2017 - 15. November 2021.

# Digitale Stadt München e.V.

**Jetzt Mitglied werden!**

Stand: Sept. 2019

## Digitale Stadt München e.V.:

Der Verein „Digitale Stadt München e.V.“ ist ein branchenübergreifendes Netzwerk im Umkreis der Digitalmetropole München. Als lebendige Plattform vernetzt er seine Mitglieder im Rahmen von drei Formaten:

### DigiTalk

DigiTalks sind unsere regelmäßigen Themenabende. Unsere Mitglieder öffnen ihre Türen und laden zu einem aktuellen Thema der digitalen Transformation ein. Lernen Sie das Unternehmen kennen und erfahren Sie dessen Herausforderungen und Lösungsansätze.

### AGs

Die Arbeitsgruppe „Smart City“ hat beispielsweise das Ziel, die Stadt München zu einer intelligenten Metropole zu entwickeln. Zu diesem Zweck werden Potenziale aus Wissenschaft und Wirtschaft identifiziert, um sie in das urbane Leben zu integrieren.

### DIGICON

Die DIGICON ist großer Treffpunkt, wenn jährlich 350 namhafte Experten und Entscheider zusammenkommen, um sich über aktuelle Themen der Digitalisierung auszutauschen.

**Kontakt: Geschäftsstelle des Vereins „Digitale Stadt München e.V.“, Oettingenstraße 67, 80538 München**
**geschaeftsstelle@digitalestadtmuenchen.de 089/ 2180-9259 oder -9171**
**Mitglied werden unter: https://digitalestadtmuenchen.de/mitglied-werden/**