DAS WIRTSCHAFTSMAGAZIN ZUR DIGITALISIERUNG

DIGITALE WELT

SCIENCE MEETS INDUSTRY

Ausgabe 1 ▪ Januar ▪ Februar ▪ März ▪ **2021**

Cyber Security

Vom Dark Web bis zu sicheren Identitäten

Threat Hunting

Wie man Cyberbedrohungen jagt

SICHERHEITSRISIKEN

Die wichtigsten Ursachen und Vorschläge zur Lösung

Deep Fakes

Wie sie die Unternehmens-sicherheit bedrohen

Homeoffice 2.0

Wie man den Arbeitsplatz digital absichert

Der Secunet CTO über die Herausforderungen der digitalen Sicherheit

Dr. Kai Martius

€ 19,50
€ 21,90

Die Digitalisierung ist in vollem Gange.

Daten sind zum wichtigsten Rohstoff unserer Zeit geworden. Die Vorteile neuer Technologien, wie z. B. künstlicher Intelligenz, dem Internet-der-Dinge oder Industrie 4.0, klingen verlockend: Wirtschaft und Verwaltung profitieren von effizienteren, produktiveren Arbeitsabläufen, jeder Einzelne von uns von verbesserten Dienstleistungen und Angeboten. Doch die neue digitale Welt ist in Gefahr. Cyberangriffe werden immer mehr zur Bedrohung für Wirtschaft und Gesellschaft. Da alles mit allem vernetzt ist, werden die Schäden, die durch Angreifer und Cyberkriminelle entstehen, immer größer. Mittlerweile melden drei Viertel der deutschen Unternehmen digitale Attacken. Aber nicht nur die Wirtschaft ist bedroht. Es betrifft jeden Einzelnen von uns. So sind bereits über die Hälfte der Internetnutzer in Deutschland Opfer von Cyber-Kriminalität geworden. Auch Attacken auf die neue digitale Arbeitswelt haben weltweit zugenommen, wie der aktuelle Lagebericht des BSI vom Oktober 2020 verdeutlicht. So wurden im Darknet gehackte Zugangsdaten für Videokonferenzen angeboten. Ungesicherte Server, Laptops und Router bedrohen das Homeoffice zusätzlich.

Die Bedrohungslage sähe jedoch noch sehr viel düsterer aus, hätten wir in den letzten Jahren nicht gewaltige Fortschritte sowohl bei der Erforschung neuer IT-Sicherheitslösungen als auch bei deren Umsetzung in Produkte und Anwendungen erzielt. Die Geschwindigkeit, mit der die Digitalisierung nicht zuletzt durch den Covid-19-Schub vorangetrieben wird, zeigt aber auch sehr deutlich weiteren dringenden Handlungsbedarf auf. Denn es geht nicht nur um mehr Effizienz und Produktivität: Die Verwundbarkeit bisher als sicher geglaubter Infrastrukturen untergräbt das Vertrauen in unsere gesamte moderne Wirtschafts- und Gesellschaftsordnung.

Mir liegt derzeit besonders das Thema „technologische Souveränität“ am Herzen. Souveränität bedeutet selbstbestimmtes staatliches oder aber auch unternehmerisches Handeln. Dies ist nicht mehr möglich, wenn die wirtschaftlichen und gesellschaftlichen Prozesse massiv von Dritten beeinflusst werden können. Das ist etwa dann der Fall, wenn die Funktionsfähigkeit der erforderlichen Technologie gezielt durch Ausspionieren und Manipulieren gestört oder aber auch die Bereitstellung der Technologien gezielt verweigert oder verzögert werden. Jedoch ist es ökonomisch nicht leistbar, alle erforderlichen Informations- und Kommunikationstechnologien (IKT) in Deutschland oder in der EU selbst zu entwickeln. Deutschland wird weiterhin auf nicht-europäische IKT-Produkte und -Dienstleistungen angewiesen bleiben. Es ist daher an der Zeit, Maßnahmen zu ergreifen, um die technologische Souveränität Schritt für Schritt zu erhöhen: Erstens müssen wir unsere IKT-Kompetenzen weiter ausbauen, um mögliche Risiken besser beurteilen zu können und kritische Abhängigkeiten zu reduzieren. Zweitens müssen Prüf- und Zertifizierungsverfahren etabliert werden, um sicherheitskritische Technologien zu beurteilen und beherrschbar nutzen zu können. Und drittens müssen wir in Forschung und Entwicklung investieren, um Zukunftstechnologien wie 6G und Quantencomputing frühzeitig zu gestalten.

Angewandte Cybersicherheitsforschung leistet hier im Schulterschluss mit der Wirtschaft einen wichtigen Beitrag: Forschungsteams entwickeln Sicherheitstechnologien, die IT-basierte Systeme und Produkte verlässlicher, vertrauenswürdiger und manipulationssicher machen. Dazu gehören auch Verfahren des Maschinellen Lernens, die bereits heute viele Bereiche unseres privaten und beruflichen Lebens beispielsweise durch Assistenzfunktionen (u.a. Spracherkennung, Fahrassistenz) prägen. Die Manipulationssicherheit derartiger Verfahren, aber auch das Erkennen von sogenannten Deep Fakes (gefälschte Bilder, Nachrichten, gesprochene Texte) sind technologische und gesellschaftliche Herausforderungen für die Sicherheitsforschung. Das Fraunhofer AISEC widmet sich deshalb mit Nachdruck auch dieser Thematik und entwickelt Verfahren, um Maschinelle Lernverfahren zertifizierbar zu machen, sie angriffsresilienter zu gestalten, aber auch um Deep Fakes effektiv zu erkennen.

Der technologische Wandel war und ist ein stetiger Begleiter des Menschen. Doch noch nie war der Wandel so rasant, so absolut und so durchdringend wie heute durch die Digitalisierung. Die Macht der Daten vermag Lösungen für Herkules-Aufgaben wie Klimawandel, Bevölkerungswachstum und Pandemien in greifbare Nähe rücken. Doch diese Vision wird nur dann Wirklichkeit, wenn wir die Augen nicht vor den Gefahren neuer Technologien verschließen und geeignete Maßnahmen ergreifen, um auf die Bedrohungen zu reagieren. Dazu gehört auch, Angriffe auf Internet, Unternehmensnetzwerke und Homeoffice ernst zu nehmen und uns dagegen zu wehren. Wir benötigen eine neue Sicherheitskultur, die es zu gestalten gilt. Jeder muss hierzu einen Beitrag leisten. Sei es der Staat, der seiner Fürsorgepflicht nachkommen und regulatorische Rahmen für die Wirtschaft, Unternehmen und Verwaltung schaffen muss, um ein Mindestsicherheitsniveau zu gewährleisten, und dabei gleichzeitig die Kräfte des Marktes nicht zu stark regulieren sollte. Oder Unternehmen, die aufgefordert sind, Daten- und Informationssicherheit, aber auch Privatheit, von Anfang an bei der Entwicklung neuer Produkte und Dienstleistungen zu berücksichtigen, und nicht zuletzt die Bürger, die sich ihrer eigenen Verantwortung beim Umgang mit ihren privaten, aber auch den unternehmerischen Daten und beim Einsatz von IT-Systemen bewusst sein müssen.

Prof. Dr. Claudia Eckert

Prof. Dr. Claudia Eckert

Claudia Eckert forscht und lehrt seit über 20 Jahren im Bereich der IT-Sicherheit. Sie hat über 10 Jahre das Fraunhofer SIT in Darmstadt geleitet und zu einem Sicherheitsinstitut aufgebaut. Seit 2009 ist sie Professorin für Sicherheit in der Informatik an der TU München und Direktorin des von ihr gegründeten Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC in Garching bei München mit derzeit über 100 hoch qualifizierten Mitarbeiterinnen und Mitarbeitern. Ihre Forschungsergebnisse wurden in über 160 wissenschaftlichen Publikationen, Zeitschriftenbeiträgen und Büchern international veröffentlicht. Als Mitglied verschiedener nationaler und internationaler industrieller Beiräte und wissenschaftlicher Gremien berät sie Unternehmen, Wirtschaftsverbände sowie die öffentliche Hand in allen Fragen der IT-Sicherheit. In Fachgremien wirkt sie mit an der Gestaltung der technischen und wissenschaftlichen Rahmenbedingungen in Deutschland sowie an der Ausgestaltung von wissenschaftlichen Förderprogrammen auf EU-Ebene.

DIGITALE WELT AUSGABE 1 | 2021

13
DR. KAI MARTIUS
Digitale Vernetzung um jeden Preis? secunet und deren Mission, uns digital zu schützen

16
CYBER SECURITY
Vom Dark Web bis zu sicheren Identitäten

10
DR. MAGNUS HARLANDER
Gefahrenstelle World Wide Web – Was für Risiken im digitalen Äther auf uns lauern

LESEN SIE ONLINE MEHR

Fachbeiträge
Kolumnen
Blogs

Die nächste **DIGITALE WELT** erscheint am 03.03.2021

Cover: Illus_man/Shutterstock, secunet Fotos: Illus_man/Shutterstock, secunet, Privat

DIGITALISIERUNG *in Zahlen*

Die **Corona-Warn-App** *wurde bis Ende Oktober über*

20 Mio.

mal heruntergeladen.

Laut einer **Lenovo-Studie,** *gaben nur* **6 %** *der befragten IT-Manager an, dass bei IT-Entscheidungen die Nutzerinnen und Nutzer im Mittelpunkt stehen.*

Aufgrund der Verfehlung von Finanzzielen und der Ankündigung, das **Geschäft auf Cloudsoftware** *auszurichten, stürzte die* **Aktie von SAP** *um*

21 % *ab.*

Laut einer Studie von **Deloitte Private** *gaben*

42 % *der befragten Manager an, dass* **Cyber Security** *für sie eine lediglich mittlere bis sehr niedrige Priorität besitzt.*

Bis zum Jahresende soll die **Corona-Warn-App** *mit anderen Warn-Apps aus* **16** *verschiedenen Ländern kompatibel sein.*

Allein im Juli dieses Jahres gab es deutschlandweit

100.000 *Hackerangriffe auf klein- und mittelständische Unternehmen sowie Privatpersonen.*

Laut Forschern des **Fraunhofer FKIE** *und der* **RWTH Aachen** *sind*

92 % *der im Internet gefundenen Steuerungen auf Basis des Standards OPC UA nicht ausreichend gesichert.*

Der Bund steuert aufgrund der Krisensituation noch weitere

6,6 Mrd.

Euro zur **Digitalisierung der Schulen** *bei.*

An der **ETH Zürich** *öffnet ein neues Forschungszentrum für Künstliche Intelligenz mit*

29 *Professuren.*

Der **„Cambridge-1" Supercomputer** *von NVIDIA schafft*

400 *Petaflops für AI Performance.*

Foto: 123RF

Was bedeutet Teamstärke für anhaltenden Unternehmenserfolg?

Der Gründer des Start-up Unternehmens kommt gleich auf sein Anliegen:

„Unsere Idee ist wirklich gut, der Businessplan ist akzeptiert, die Finanzierung steht, wir haben auch das Team für die erste Phase zusammen. Es läuft und fängt an richtig Spaß zu machen. Wir arbeiten viel, jeder kann im home-office arbeiten. Bei unseren persönlichen jour-fixes wird auch gekickert, alles cool, aber ich spüre – irgendetwas fehlt uns."

Um zu klären, was fehlen könnte, hilft ein Checkup anhand der folgenden psychologischen Elemente. Wenn sie gelebte Praxis sind, bringen sie ein Team langfristig auch durch stürmisches Fahrwasser ans Ziel.

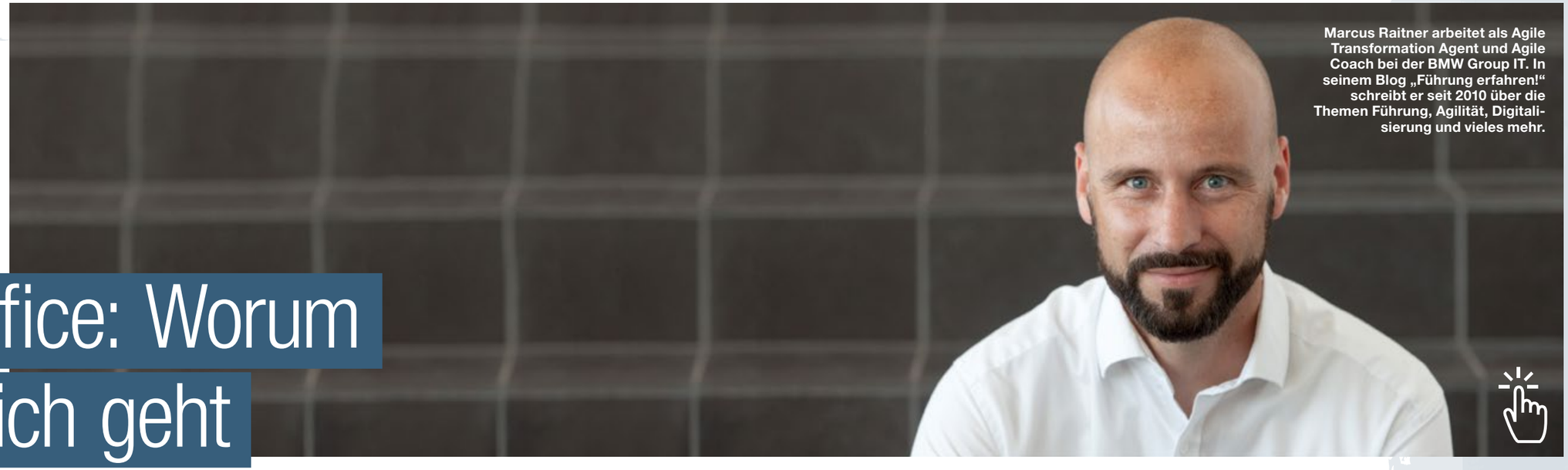
- Und der erste Aspekt sind klare, emotional verankerte Ziele. Ohne sie gibt es keinen Flow. Es gilt sicherzustellen, dass alle im Team das gleiche Ziel-Bild vor Augen haben. Für die Gründer ist das Ziel sonnenklar, aber wirklich auch für alle anderen? Hier hilft die Frage „Wozu machen wir das hier eigentlich?" Die Unterschiedlichkeit der Antworten ist manchmal sehr überraschend.
- Im Alltag gelebte Werte. Bei den Werten glauben manche Gründer, sie seien selbstverständlich alle die gleichen. Allerdings bedeuten z.B. Respekt und Wertschätzung für viele etwas völlig Unterschiedliches. Je nach kulturellem Hintergrund hat z.B. Respekt eine andere Ausdrucksform. Gerade in Teams mit unterschiedlichen kulturellen Hintergründen und einer gemeinsamen „Fremd"Sprache lohnt sich die Diskussion „Was ist unsere gemeinsame Basis und gibt uns Orientierung in unserer Zusammenarbeit?"
- Kommunikation und Feedback-Rituale. Kommunikation ist der Lebensnerv eines jeden Unternehmens. Wir alle wissen, dass es nicht die „richtige" Kommunikation geben kann. Umso wichtiger ist es, Plattformen und Strukturen, Qualität und Quantität immer wieder auf die Waagschale zu legen.
- Führungsqualität – auch emotional, virtuell, interkulturell … Gerade Gründer sind häufig eher technisch orientierte Tüftler oder Vollblut-Unternehmer. Wie gelingt es, neben den faktischen Ergebnissen auch die Bedürfnisse der Menschen im Unternehmen entsprechend zu fördern und zu fordern?
- Deshalb ist das Wissen um die eigenen Stärken und Schwächen, der Blick auf Persönlichkeitsmerkmale und Verhaltensstile nicht nur für alle Teammitglieder, sondern auch für die Köpfe des Unternehmens hilfreich. Bin ich besonders perfektionistisch oder eher detailorientiert unterwegs. Liegen mir die Zahlen, Daten, Fakten am Herzen oder sind es eher die Menschen mit ihren Vorlieben und Fähigkeiten?
- Wenn ich nun weiß, wie ich selbst „ticke", fällt es leichter, Kollegen mit deren Stärken und Schwächen zu respektieren. Gleich und gleich gesellt sich gerne und Unterschiede ziehen sich an. Unterschiedliche Antreiber und Verhaltensstile können das Ergebnis einer Teamleistung deutlich verbessern, gleichzeitig können sie auch Auslöser von Konflikten sein. „Lass uns endlich anfangen, wir haben schon lange genug geredet!" „Bevor wir den Prozess nicht im Detail geplant und alle Eventualitäten berücksichtigt haben, können wir nicht starten!" Im professionellen Mannschaftssport werden Teams nach den Stärken ihrer Spieler zusammengestellt, um möglichst erfolgreich zu sein.
- Im Profisport ist auch mentale Stärke zur Steuerung der Leistung bereits übliche Praxis. Damit ist gemeint, mit der Macht der Gedanken in schwierigen Situationen einen klaren Kopf zu behalten, bestmögliche Leistung zu bringen und auch als Team erfolgreicher zu sein. Für viele Menschen ist es ein besonderes Aha-Erlebnis, wenn sie anfangen zu verstehen, wie sie als Dirigent mentaler Prozesse Einfluss nehmen können. Wie sie sich z.B. für Verhandlungen oder Präsentationen mental aufrüsten können. Oder wie sie in der Zusammenarbeit im Team Kreativität und möglichen Flow mit der Kraft innerer Bilder stärken oder stressige Konflikte einfacher lösen können.

Welche Zutaten für die Teamstärke auch immer fehlen mögen, es lohnt sich, diese für die volle Wirkung des Zaubertranks zu ergänzen. So rüstet sich das kleine gallische Dorf für den Wettkampf mit der Großmacht. Und um das Beste rauszuholen, darf es durchaus mal etwas stressig werden, aber bitte ohne dramatische Dauer-Überanstrengung.

Weiterhin viel Freude und Erfolg!

Foto: Privat

Dieses Fachbuch erklärt praxisnah, wie Führungskräfte und Personalverantwortliche ihre Kollegen gesund, leistungsfähig, kreativ und innovativ halten und vor Burnout schützen – in einer digitalen Arbeitswelt voller Stressfaktoren und psychischer Überlastung.



Marcus Raitner arbeitet als Agile Transformation Agent und Agile Coach bei der BMW Group IT. In seinem Blog „Führung erfahren!“ schreibt er seit 2010 über die Themen Führung, Agilität, Digitalisierung und vieles mehr.

Homeoffice: Worum es wirklich geht

Homeoffice ist nur vordergründig eine Frage des Arbeitsorts. Im Kern geht es dabei um das Prinzip der Augenhöhe, um Menschenbilder, Vertrauen statt Kontrolle und ganz grundsätzlich um das Verhältnis zwischen Führungskraft und Wissensarbeiter.

Die Corona-Pandemie hat Homeoffice endgültig salonfähig gemacht. Über Nacht wurde verteilte Zusammenarbeit für sehr viele Wissensarbeiter zum Standard und sie ist auf dem besten Weg auch nach der Krise zum „New Normal“ zu werden. Auch wenn mobiles Arbeiten in vielen Unternehmen vorher prinzipiell schon möglich war, blieb es doch die Ausnahme: Eine zweitklassige, grundsätzlich verdächtige und daher explizit zu rechtfertigende Arbeitsform und daher nichts für echte Höchstleister. Vielerorts herrschte vor Corona ein ausgeprägter Präsenzkult und dessen Credo lautete: Echte Arbeit findet nur im Büro und unter Aufsicht statt.

Dieses Credo gerät nun sogar in deutschen Traditionskonzernen zunehmend ins Wanken. „Wir haben gesehen, wie produktiv und effektiv das mobile Arbeiten sein kann. Da haben sich einige Vorurteile in Luft aufgelöst“, stellte Jochen Wallisch, ein führender Manager im globalen Personalbereich von Siemens, fest. Die Konsequenz aus dieser Lehre zog Siemens mit einem weitreichenden Vorstandsbeschluss, der das mobile Arbeiten an zwei bis drei Tagen pro Woche zum weltweiten Standard für rund 140.000 Mitarbeiter machen soll. (ZEIT Online vom 16.7.2020)

Auch die Allianz musste binnen weniger Tage alles ins Homeoffice verlegen und sämtliche Reisen absagen. Und es funktionierte erstaunlich gut. So gut, dass der Allianz-Chef Oliver Bäte glaubt, mit einem massiven Ausbau des mobilen Arbeitens 50% der Reisekosten und langfristig ein Drittel der Büroflächen einsparen zu können. Seine ganz persönliche Erfahrung mit der Arbeit im Homeoffice deckt sich mit der Beobachtung vieler anderer Wissensarbeiter: „Ich bin manchmal erheblich produktiver.“ Damit das auch so bleibt, hat Oliver Bäte angekündigt, auch künftig teilweise von zu Hause zu arbeiten. (Manager Magazin vom 2.7.2020)

Ein Beschluss in der Dimension wie bei Siemens hat Signalwirkung, weil durch den dadurch gesetzten Rahmen prinzipiell und unmissverständlich die Gleichwertigkeit von Homeoffice herausgestellt wird. Wichtiger noch ist aber das Vorbild eines Oliver Bäte bei der Allianz, der als Chef selbst auch mal zu Hause in Ruhe arbeitet. Beides zusammen wirkt Wunder.

> *Knowledge workers cannot be managed as subordinates; they are associates. They are seniors or juniors but not superiors and subordinates.*
> Peter F. Drucker, Management’s New Paradigm, 1998

Homeoffice ist tatsächlich nur vordergründig eine Frage des Arbeitsorts. Im Kern geht es dabei um Selbstbestimmung und Augenhöhe. Es geht um Menschenbilder, Vertrauen statt Kontrolle und ganz grundsätzlich um das Verhältnis zwischen Führungskraft und Wissensarbeiter, welches Peter Drucker so oft thematisierte. Letztlich geht es darum, wer über Homeoffice und mobiles Arbeiten entscheidet. Solange wie bisher vielerorts üblich das letzte Wort bei einem Vorgesetzten liegt, für den Homeoffice am Freitag oder Montag einem verlängerten Wochenende gleichkommt, wird sich mobiles Arbeiten nicht durchsetzen. Und solange die Führungsriege fleißig das Narrativ des Kapitäns auf der Brücke nährt, werden auch die besten Absichtserklärungen verpuffen.

Darum braucht es auch neue Spielregeln, die einen Ausgleich der Interessen auf Augenhöhe ermöglichen. So wie beispielsweise bei SAP, wo die 22.000 Mitarbeiter in Deutschland schon seit 2018(!) weitgehend frei entscheiden können, ob sie im Büro, im Café, zu Hause oder auch im Schwimmbad ihre Arbeit verrichten. Die Neuerung der damaligen Regelung war insbesondere die Feststellung, dass es generell erwünscht ist, dass Führungskräfte mobiles Arbeiten ermöglichen. Damit wird die Beweislast umgekehrt. Der Mitarbeiter ist in der Frage nach mobiler Arbeit nicht mehr abhängiger Bittsteller, sondern gleichwertiger Partner in einer gemeinsamen Abwägung der Interessen. Den vorbildlich schlanken Prozess zur Abstimmung beschreibt Personalchef Cawa Younosi so: „Der Mitarbeiter und die Führungskraft einigen sich formlos, das geht per Mail, per SMS oder per Kalendereintrag.“ (FAZ vom 2.3.2018)

> *Whether you think you can, or you think you can’t – you’re right.*
>
> Henry Ford

Es geht also. Bei manchen Unternehmen ging es auch schon vor Corona. Bei vielen anderen geht es jetzt plötzlich und das in unvorstellbarer Geschwindigkeit. Und bei anderen geht es möglichst schnell zurück zum vorherigen Präsenzkult. Die Quittung für diese verpasste Chance erhalten letztere dann in ein paar Jahren, wenn Unternehmen ohne eine vernünftige Regelung von Homeoffice basierend auf Augenhöhe und Selbstbestimmung auf dem Arbeitsmarkt zurückfallen und schlicht nicht mehr konkurrenzfähig sein werden. Auch wenn es sich gerade mitten in der Krise nicht so anfühlt, aber es gilt immer noch: „War for talent is over – talent won.“

Foto: Privat

Das Buch zum Manifest für menschliche Führung. Erhältlich als Taschenbuch und E-Book bei Amazon

Gefahrenstelle World Wide Web

Was für Risiken im digitalen Äther auf uns lauern

Dr. Magnus Harlander im Gespräch

Die derzeitige Situation am Arbeitsmarkt hat viele Alltäglichkeiten unseres Berufslebens verändert. Für viele ist das eigene Heim zum Arbeitsplatz mutiert. Doch das birgt – gerade durch die Vernetztheit unseres Lebens – auch einige Risiken. Magnus Harlander ist Vorstand der ISAR AG und hat über vorherige Funktionen in anderen Bereichen zahlreiche Erfahrungen über das Thema Sicherheit im Internet erhalten.

Das Internet ist – neben vielen guten Aspekten – ein virtueller, nahezu undefinierbarer und nicht begrenzbarer Raum, der die Möglichkeit von Verbrechen fördert. Von Trojanern, Phishing, Malware, Computer-Viren, Scareware, Ransomware oder Zombie-Computern haben wir alle schon mal gehört. Vor welchen Gefahren würden Sie einen 0815-Anwender gerne besonders warnen?
Ich denke, aktuell sind für die Endgeräte-Nutzer Ransomware und Phishing von Zugangsdaten immer noch die größte Gefahr. Allerdings ist inzwischen jeder Haushalt zu einem kleinen Rechenzentrum von netzfähigen Devices herangewachsen, denen es in der Regel an jeglicher Robustheit gegen Angriffe mangelt und die auch ihr Leben lang – und das kann sehr lang sein – nie aktualisiert werden.

Wie hat sich diese Palette an Gefahren im Laufe der letzten Jahre verändert? Gibt es Gefahren, die heute gar keine mehr sind? Was sind Gefahren, die Sie in Ihrem Metier am „interessantesten“ finden?
Der klassische Virus - egal ob als Exe, Zip oder Word Macro - wird von den meisten Virenscannern ganz gut beherrscht. Sehr viel heikler ist targeted Malware, weil die den Virenscanner-Herstellern nicht bekannt wird, Übertragung über verschlüsselte Wege, weil die zentralen Virenscanner da nicht greifen, und die riesige Angriffsbasis von anfälligen embedded Devices (Wlan-Router, Waschmaschinen, Lampen, Heizung, Steuerungen, Rasenmäher,...) im Haushalt, unterwegs und in der Industrie.

Je mehr sich unser Alltag digitalisiert und im World Wide Web vernetzt, umso wichtiger wird das Thema Sicherheit. Wie bewerten Sie die generelle digitale Sicherheitslage in Deutschland?
Die Bundesregierung und das BSI versuchen, die Sicherheitsstandards durch Regulierung vor allem in den öffentlichen Bereichen und im Bereich der kritischen Infrastruktur hoch zu halten. Das ist nur ein mühsames Unterfangen und lässt zudem viele kleinere Organisationseinheiten außen vor, weil sie durch die Regulierung gar nicht erfasst werden.

Der niederländische Journalist Huib Modderkolk hat jüngst in seinem Buch „Der digitale Weltkrieg“ die These aufgestellt, dass der nächste Weltkrieg schon längst digital am Laufen sei: Die Rede ist vom Einfluss russischer Hacker auf den amerikanischen Wahlkampf, von Edward Snowden und anderen Whistleblowers und dem florierenden Online-Geschäft zahlreicher Drogenbarone. Was ist dran an Modderkolks These und wie kann man dem entgegenwirken?
Ich denke, an der These ist schon was dran. Alle Staaten rüsten ihre digitalen Offensiv-Kapazitäten auf. Technisch ist da vor allem in Deutschland und Europa wenig dagegen zu machen, weil wir in den allermeisten Kerngebieten der IT (Software, Hardware, Netze, Plattformen, Cloud) keinerlei Souveränität mehr ausüben können. Da haben die Chinesen und vor allem die USA einen zu großen Vorsprung. Daher bleibt uns eigentlich nur der diplomatische Weg, nach digitalen Abrüstungsvereinbarungen zu streben.

„Sauber aufgesetzte VPNs mit eigenen Hardware- oder Software-Clienten, sauberes Keymanagement, Isolation und Trennung von Geschäfts- und Privat-IT, wiederum mittels Hard- oder Softwarekomponenten, sind nun angesagt.“

Wo es ein Bedürfnis nach Sicherheit gibt, da lauert irgendwo Gefahr. Vielleicht ganz grundsätzlich gefragt: Was macht das Internet für Verbrechen so lukrativ?
Ganz klar: Weil die Attribution, d.h. die Identifikation und der Zugriff auf die Täter so kompliziert ist, weil das Internet inzwischen fast überall präsent und lebenswichtig geworden ist, und weil es so wunderbar skaliert, sodass kriminelle Geschäftsmodelle abgehen wie die Post.

Seit Dezember 2018 funktioniert kontaktloses Bezahlen wie Apple Pay auch in Deutschland. Gerade in Zeiten der Corona-Pandemie haben solche Dienstleistungen an Beliebtheit dazugewonnen. Allgemein gesprochen ist eine Verschiebung unserer alltäglichen Finanzgeschäfte ins Internet zu beobachten. Doch wie sicher ist unser „digitales“ Geld überhaupt? Wie reagieren Banken auf das erhöhte Sicherheitsrisiko?
Von digitalem Geld reden wir aktuell ja noch nicht, wenn man Bitcoin und Co. mal außen vor lässt. Es geht um digitale Prozesse. Die Standards sind hier inzwischen schon recht hoch. Allerdings sind in diesen Prozessen auch sehr viele Beteiligte involviert: Banken, Provider, Geschäfte, Handyhersteller, Softwarehersteller und nicht zuletzt der Kunde. Das macht es anfällig für Schwachstellen. Es muss einfach alles klappen, damit nichts dabei schief geht. Jeder Beteiligte - auch und vor allem der Kunde oder Endbenutzer - muss hier seinen Beitrag leisten.

Was ist an folgender These dran: Eine Oma wird eher durch einen Enkelkinder-Trick beraubt, als dass ihr Online-Banking-Konto entleert wurde.
Das sehe ich nicht so, weil für den Enkelkinder-Trick muss jemand in persona an der Tür klingeln. Phishing-Angriffe, um Online-Banking anzugreifen, skalieren viel besser.

Eine Verschiebung zu mehr digitalem Leben ist durch das lockdownbedingte Homeoffice festzustellen. Wenn ich am Schreibtisch zu Hause mit meinem privaten Laptop über mein hauseigenes WLAN im Internet mit meinen Arbeitskollegen korrespondiere, wer oder was fungiert als digitale Polizei? Was für Systeme gibt es, um unsere Sicherheit im Internet bestmöglich zu gewährleisten? Sind solche Systeme hardwarebasierend, softwarebasierend oder beides? Welche Rolle spielen Kategorien wie „Menschen“, „Moral“ und „Gesetze“?
Die Homeoffice-Offensive wird von vielen Mitarbeitern sehr begrüßt. Es wurde auch sehr schnell realisiert, und da es um den Fortbestand der Unternehmen und der Geschäftstätigkeit ging, hat man dabei sicherlich nicht auf jeden sicherheitstechnisch gebotenen Aspekt geachtet. Jetzt geht es darum, das schnell in Ordnung zu bringen. Sauber aufgesetzte VPNs mit eigenen Hardware- oder Software-Clienten, sauberes Keymanagement, Isolation und Trennung von Geschäfts- und Privat-IT, wiederum mittels Hard- oder Softwarekomponenten, sind nun angesagt. Und natürlich Schulung der Nutzer, weil sie nun eben weit außerhalb der ehemals gut geschützten Firmen-Brandmauern agieren.

Viele Windows-User kennen die Notwendigkeit von Anti-Virus-Softwareprogrammen. Wie sinnvoll sind solche Anwendungen? Was sind gute, was sind schlechte Anti-Virus-Programme? Sollten andere Betriebssysteme auch auf dieses Angebot zurückgreifen?
Virenscanner sind inzwischen obligatorisch, und ein Verzicht darauf oder die Vernachlässigung von Updates ist einfach fahrlässig. Aber sie sind kein Allheilmittel und müssen durch eine Vielzahl anderer Maßnahmen ergänzt werden. Am wichtigsten dabei sind Vernunft und Aufmerksamkeit der Nutzer. Auch Nicht-Windows Betriebssysteme können von Malware-Angriffen betroffen sein, sodass man auch dort über solche Schutzmaßnahmen nachdenken sollte.
Windows ist aber schon ein besonderer Fall.

„Security Laptops“ sind eigens für den Diplomaten- oder Geheimdienst angefertigte Geräte, die eine maximale Sicherheit versprechen. Was macht solche Geräte so sicher und wie sind sie trotzdem verwundbar?
Diese Geräte achten auf strikte Trennung der vertraulichen Daten sowie der Systembestandteile in Soft- und Hardware. Sie nutzen starke und gut gemanagte Verschlüsselungstechniken und sind durch hoch kompetente Prüfstellen und das BSI geprüft, zertifiziert und zugelassen. Aber natürlich gilt auch hier: Einhundertprozentige Sicherheit gibt es nicht, außer in totaler Isolation, d.h.: kein Netz, kein Datenaustausch, keine Schnittstellen.

Virtuelle private Netzwerke, sog. „VPNs“, sind hingegen eine populärere Alternative, um im privaten und öffentlichen Raum anonym zu surfen. Wie sieht der Markt hier aus? Was sind gute, was sind schlechte VPNs? Garantieren VPNs aber wirklich meine Anonymität?

Eigentlich sind VPNs ja zur Verschlüsselung und nicht zur Anonymisierung gedacht. Anonymität bieten sie nur für die IP-Adresse, wofür auch ein einfacher Proxy ausreicht. Allerdings können die Dienstanbieter inzwischen über Cookies u.ä. Verfahren die Nutzer sowieso viel besser identifizieren als über IP-Adressen. Also sollte man sich darauf nicht so verlassen und genauso auf seine Cookies und Freigaben von Datenschutzpolicies achten, wenn man anonym bleiben will. 100%ige Anonymität gibt es aber eben auch nicht.

Moderne Technologien wie Quantencomputer und Künstliche Intelligenz revolutionieren derzeit unseren Alltag. Einige Experten merken mahnend an, dass Quantencomputer alsbald in der Lage sein können, bestimmte Verschlüsselungssysteme zu knacken, mit denen heute sichere Nachrichten oder andere Systeme gehandhabt werden. Teilen Sie diese Sorge?

Die Basis unserer gesamten IT-Sicherheits-Infrastruktur sind mathematische Verfahren, die alle irgendwann durch einen Quantencomputer gebrochen werden können. Dafür gibt es die theoretischen Grundlagen schon sehr lange, man muss nur so ein Ding bauen. Dabei gibt es aber aktuell große Fortschritte. Daher ist es höchste Zeit, über Alternativen nachzudenken und vor allem sie auch ins Feld zu bringen. Erfahrungsgemäß dauert es Dekaden, bis man etablierte Technik in der Fläche austauscht. Für Kryptotechnik gilt das besonders.

Könnte man im Gegenzug nicht gerade die enorme Leistungsfähigkeit des Quantencomputers und die Intelligenz von KI einsetzen, um noch bessere Sicherheitssysteme zu entwickeln?

In der Tat gibt es auch Forschung zu sog. Quanten-Key-Distribution, also die Verteilung von Keys mittels quantenmechanischer Methoden. Das hat mit Quantencomputern nichts zu tun, kommt aber aus derselben Ecke. KI wird tatsächlich heute schon eingesetzt, um Malware zu erkennen oder seltsames Verhalten von Systemen im Netz zu detektieren.

„KI wird tatsächlich heute schon eingesetzt, um Malware zu erkennen oder seltsames Verhalten von Systemen im Netz zu detektieren.“

Noch ein Ausblick in die Zukunft: Glauben Sie wegen des Sicherheitsrisikos an eine Renaissance des Analogen oder ist die Verlagerung unseres Alltags ins Digitale unausweichlich? Wie werden wir letzteres aber ohne große Sicherheitsprobleme schaffen?

Die Zukunft ist digital. Das ist für mich ganz klar. Allerdings sind wir gut beraten, die Systeme, Plattformen und Technologien, die sich in den vergangenen Jahrzehnten einfach über den Markt etabliert haben, auf ihre Gesellschaftstauglichkeit zu überprüfen. Ich denke da z.B. an die zunehmende Polarisierung von Gesellschaften durch die in sozialen Medien genutzten Algorithmen, die Filterblasen mit ganz üblen Auswirkungen erzeugen.

Interview: Hannes Mittermaier

Dr. Magnus Harlander

Foto: Privat

Dr. Magnus Harlander hat an der TU-München und am Lawrence-Berkeley-Lab studiert und in Physik promoviert. Noch während der Promotion hat er 1992 im Team die genua GmbH gegründet, einen führenden Anbieter von Sicherheitslösungen für das anspruchsvolle Segment. Viele Netze von Bundeseinrichtungen und international agierenden Großunternehmen werden von den weltweit einzigartig hoch zertifizierten Komponenten von genua geschützt. Nach dem Verkauf des Unternehmens an die Bundesdruckerei engagiert sich Magnus Harlander als Vorstand der ISAR AG nun als Investor, Business Angel und Berater im Bereich nachhaltiger Startups und Projekte. Als Vorstand der Harlander-Stiftung, Vorstandsvorsitzender des SV-Heimstetten, Handelsrichter am Landgericht München und Vorstandsmitglied des Münchner Kreises hat er zudem ein weites Feld ehrenamtlicher Tätigkeiten.

Digitale Vernetzung um jeden Preis?

secunet und deren Mission, uns digital zu schützen

Dr. Kai Martius im Gespräch

Kai Martius ist Chief Technical Officer von secunet, Deutschlands führendem Cybersecurity-Unternehmen. Seit Jahren befasst er sich mit dem bestmöglichen Schutz von Daten, IT-Infrastrukturen und digitalen Identitäten. Secunet hat sich darauf spezialisiert, für besondere Sicherheitsansprüche im Netz zu sorgen – zum Beispiel bei der Geheimhaltung von wichtigen Informationen oder bei der Vernetzung von Produktionsanlagen von Industrieunternehmen. Außerdem sorgt secunet dafür, dass Patientendaten geschützt im digitalen Gesundheitsnetz unterwegs sind und dass Nutzer der elektronischen Steuererklärung ELSTER sich sicher anmelden und zweifelsfrei authentifizieren können. Wo steuern wir mit der digitalen Revolution hin? Und was für einen Preis müssen wir dafür in puncto Sicherheit bezahlen?

„Im Großen spricht man von digitaler Souveränität. Sie ist ein Faktor, der der digitalen Determination entgegenwirkt.“

Das Internet ist ein Raum, der prinzipiell keine physischen Grenzen kennt. Wie global sehen Sie das Problem der Internetsicherheit? Wie arbeiten Sie mit der Bundesrepublik Deutschland zusammen? Wie mit noch größeren Institutionen?

Cyberkriminelle oder auch Hacker in staatlichem Auftrag können grundsätzlich von überall auf der Welt angreifen. Bedrohungsszenarien für die Internetsicherheit oder ganz allgemein für die Informationssicherheit müssen wir daher immer global denken. Auch unser Angebot richten wir weltweit aus. Industrieunternehmen profitieren von unseren Lösungen, egal, wo sie ihren Sitz haben. Wir arbeiten für zahlreiche Behörden anderer EU-Staaten. Unsere Wurzeln liegen allerdings klar in Deutschland: Seit 2004 sind wir IT-Sicherheitspartner der Bundesrepublik. Alle Bundesministerien und mehr als 20 DAX-Konzerne zählen zu unseren Kunden.

Und wie steht es um die Sicherheitslage in Deutschland im Vergleich zu anderen EU-Ländern; wie im globalen Vergleich?

Hier muss man differenzieren: Der Bereich der öffentlichen Verwaltung in Deutschland ist hinsichtlich der IT-Sicherheit stark reguliert, für die Bundesverwaltung gelten strikte Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). Daher wird viel in Cybersicherheit investiert. Das Schutzniveau der Behörden in Deutschland ist entsprechend hoch.

Im weitgehend unregulierten privatwirtschaftlichen Bereich sieht das anders aus: Hier gibt es größtenteils deutliches Verbesserungspotenzial. Das gilt für Deutschland und auch für andere Länder. Ein Sonderfall sind die kritischen Infrastrukturen, zum Beispiel Energie- und Wasserversorger. Cyberangriffe auf diese Betriebe können schwerwiegende Folgen für die gesamte Gesellschaft haben. Daher bestehen in Deutschland seit 2015 gesetzliche Regelungen für die IT-Sicherheit kritischer Infrastrukturen, und folglich ist bei deren Sicherheitsniveau auch ein Aufwärtstrend zu beobachten.

Die Corona-Krise hat viele zum Homeoffice gebracht. Steigen damit auch die potenziellen Gefahren einer Virtualisierung unseres Alltags, der wiederum dadurch lukrativer wird für Verbrechen? Was können wir als User konkret dagegen tun?

Auch mobile Arbeitsplätze können sehr gut abgesichert werden, sodass keine Sicherheitseinbußen gegenüber einem stationären Arbeitsplatz im Büro entstehen. Schon vor der Corona-Krise haben wir das für viele unserer Kunden getan – gerade für solche, die mit besonders schützenswerten Daten arbeiten. Dabei nutzen wir die Sicherheitsarchitektur SINA, die wir ursprünglich im Auftrag des BSI entwickelt haben. Sie besteht unter anderem aus Netzwerkkomponenten, die den gesamten Datenverkehr spionage- und manipulationssicher verschlüsseln, sowie sehr sicheren Clients wie zum Beispiel Laptops. Je nach Gefährdungslage bei dem konkreten Auftraggeber gilt es, ein angemessenes Schutzniveau zu finden, sodass Aufwand und Nutzen in einem gesunden Verhältnis stehen. Wird das Schutzniveau zu niedrig angesetzt, haben Hacker natürlich leichtes Spiel.

Auch als User können Sie eine Reihe von Dingen tun, um unterwegs oder im Homeoffice keine unnötigen Sicherheitsrisiken einzugehen. Sie sollten zum Beispiel sichere Passwörter einsetzen und ihren Computer immer sperren, wenn Sie ihn verlassen. Es empfiehlt sich, sämtliche Sicherheitsupdates zeitnah einzuspielen, falls das nicht zentral von der Unternehmens-IT gesteuert wird. Wichtig ist außerdem, dass Sie keine Software nutzen, die von Ihrem Arbeitgeber nicht vorgesehen ist, zum Beispiel Cloudspeicher, Chatdienste oder Videokonferenzprogramme. Andernfalls entsteht eine Schatten-IT mit Risiken, die für die Unternehmens-IT schwer zu bekämpfen sind, weil sie sie gar nicht kennt. In unseren Security-Awareness-Seminaren, die wir für Kunden abhalten, steigen wir tiefer in diese Themen ein.

„Auch als User können Sie eine Reihe von Dingen tun, um unterwegs oder im Homeoffice keine unnötigen Sicherheitsrisiken einzugehen.“

Sie haben die Industrie 4.0 erwähnt – was sind hier die besonderen Herausforderungen und welche Lösungen bieten Sie konkret an?

Wenn Sie bedenken, dass Maschinen im Industrieumfeld oft länger als 30 Jahre in Betrieb sind, können Sie sich die Herausforderungen vorstellen: Eine digitalisierte und vernetzte Produktion ist extrem wichtig für zukunftsfähige Geschäftsmodelle, aber die Maschinen sind in vielen Fällen dafür schlichtweg zu alt. Wie bekommen die Betreiber diese Maschinen trotzdem sicher mit modernen Plattformen vernetzt? Mit secunet edge haben wir dafür eine Gesamtlösung im Portfolio, die auf dem Konzept des Edge Computing basiert: Die Lösung setzt dezentral an der einzelnen Maschine an, vernetzt sie und sichert sie ab. Darüber hinaus fungiert die Lösung als sichere Plattform, auf der diverse Connectivity-Anwendungen laufen können. So können die Betreiber zum Beispiel sichere Fernwartung umsetzen, mit einer Monitoring-Komponente Angriffe erkennen und vieles mehr. Dieses Konzept ist übrigens nicht nur für alte Maschinen, sondern auch für neue interessant: Es ist flexibel erweiterbar, sodass auch künftige Anforderungen abgedeckt werden können, die auch in neuen Maschinen – die wieder eine jahrzehntelange Laufzeit haben werden – noch nicht berücksichtigt sind.

Digitale Forensik ist ein neuer Fachbegriff, der in der Kriminalistik derzeit grassiert. Was versteht man darunter und welchen Beitrag leisten Sie als Unternehmen?

Digitale Forensik kommt dann zum Zug, wenn ein Cyberangriff erfolgreich war. Betroffenen Unternehmen bieten wir Forensik-Dienste an. Im Mittelpunkt steht dabei die Aufklärung des Sicherheitsvorfalls. Dessen Ursprung ist stets ein einzelnes kompromittiertes System, der sogenannte „Patient Zero“. Dieses System muss in vielen Fällen erst ermittelt werden. Dann erzeugen die Experten eine Eins-zu-eins-Kopie, um die Beweismittelkette zu erhalten, und analysieren anschließend die Kopie.

Zur digitalen Forensik gehört auch, als Unternehmen auf ein solches Szenario vorbereitet zu sein – das maximiert die Erfolgsaussichten im Ernstfall. Secunet bietet unter dem Stichwort „Forensic Readiness“ Workshops an, in denen Strukturen, Prozesse und Entscheidungsbäume festgelegt werden. Besonders wichtig sind ein gemeinsames Verständnis bei den beteiligten Personen sowie klare Rollen und Entscheidungskompetenzen.

Nehmen wir an, dass das Auto von morgen, die Straßenbahn, der Computer an der Arbeit, mein Smartphone, meine Bank, meine intelligente Brille etc. mit dem Internet verbunden sind. In diesem digitalisierten Umfeld, in das ich mich zunehmend mehr begebe, besteht die Gefahr einer digitalen Determination. Wie bewerten gerade Sie aus ethischer Sicht die Frage nach einer möglichen Einschränkung unserer Handlungsfreiheit durch die digitale Überhand?

Neue Technologien werden immer auch mit Skepsis betrachtet – das ist bei der digitalen Transformation, einer tiefgreifenden Umwälzung, natürlich nicht anders. Aber Sie sprechen durchaus eine Gefahr an, die wir ernst nehmen sollten.

Grundsätzlich gilt auch für die digitale Welt: Wir sind nur so unfrei, wie wir uns machen. Das fängt im Kleinen an: An Ihrem Smartphone sollten Sie bewusst und sorgfältig die Dienste auswählen, die Sie auch wirklich nutzen möchten, und die anderen deaktivieren. Im Großen spricht man von digitaler Souveränität. Sie ist ein Faktor, der der digitalen Determination entgegenwirkt. Digitale Souveränität bedeutet, die Hoheit über die eigenen Daten zu behalten – um sich vor Cyberkriminalität, Spionage und ähnlichem zu schützen, aber auch um in besonders sensiblen Bereichen unabhängig von den weltweit dominanten IT-Anbietern zu sein. Nur wer jederzeit weiß, wo seine Daten liegen und wer Zugriff darauf hat, kann auch entscheiden, was damit passiert. Das ist ein wichtiges Thema für Privatpersonen, aber auch für Unternehmen, Behörden und andere Organisationen. Bei secunet haben wir es uns daher zur Aufgabe gemacht, digitale Infrastrukturen zu schützen – weil wir unsere Kunden in die Lage versetzen wollen, digital souverän zu handeln und innovativ zu sein.

Ein Beispiel: Cloud Computing ist eine Technologie, die besonders stark mit dieser Frage verknüpft ist. Wir kennen das aus dem Privatleben: Wir nutzen Cloud-Angebote, weil sie praktisch sind. Aber wir haben manchmal ein schlechtes Gefühl dabei, weil wir nicht wissen, wo die Daten landen und ob sie nicht doch für Zwecke verwendet werden, die uns nicht gefallen. Für Behörden und Unternehmen, die mit besonders sensiblen Daten umgehen, haben wir dieses Dilemma mit secustack gelöst, einem Joint Venture von secunet und der Firma Cloud&Heat. SecuStack bietet ein vertrauenswürdiges Cloud-Betriebssystem – SecuStack – Made in Germany, basierend auf der Open Source Software „OpenStack“. Die Kernfunktion ist eine durchgängige Verschlüsselung der Daten in einer OpenStack-Umgebung mit den gleichen Sicherheitsbausteinen, die secunet seit vielen Jahren im Hochsicherheitsbereich einsetzt. Das ermöglicht es überhaupt, auf Basis prüfbarer Software eigene Cloud-Infrastrukturen für sensible Daten aufzubauen, so Cloud Computing zu nutzen und trotzdem souverän mit diesen Daten umzugehen.

Welche biometrischen Lösungen bietet Ihr Unternehmen an? Wie steht es um die Sicherheit meiner Daten, wenn ich mein Smartphone mit meinem Gesicht entsperre oder meine Bankzahlung via Fingerabdruck erledige?

Wir beschäftigen uns seit vielen Jahren intensiv mit Biometrie und ihrer Zuverlässigkeit und liefern zum Beispiel die Technologie, mit der an Flughäfen elektronische Reisepässe und Personalausweise automatisiert geprüft werden. Dabei nimmt das System ein Gesichtsbild der Reisenden auf und vergleicht es mit dem Bild auf ihrem elektronischen Identitätsdokument. Eine Vielzahl intelligenter Mechanismen sorgt dafür, dass Betrugsversuche keine Chance haben.

Die biometrischen Funktionen eines Smartphones sind auf jeden Fall ein besserer Schutz des Gerätes im Vergleich zu einer PIN oder gar keinem Zugriffsschutz. Die Bequemlichkeit der Nutzung ist zudem ein großer Vorteil, damit Anwender ihr Gerät überhaupt schützen. Allerdings sind die Mechanismen in den Smartphones weniger sicher gegen Angriffe als unsere Gesichtserkennung in den Grenzkontrollsystemen – denn bei diesen geht es ja auch um einen höheren Sicherheitsanspruch.

Was halten Sie von der Idee eines gänzlich digitalen Personalausweises?

Grundsätzlich spricht aus meiner Sicht nichts dagegen, ein digitales Abbild des Personalausweises für bequemere Identifikationsverfahren zu nutzen. Dieses sollte allerdings weiterhin an ein physisches Dokument gekoppelt sein, um bei Bedarf auch unabhängig von einer Smartphone-Funktion Identitätsprüfungen durchführen zu können.

Welche Rolle kann die enorme Leistungsfähigkeit eines Quantencomputers für die Datenverschlüsselung und andere kryptographische Verfahren spielen?

Der Quantencomputer ist eine große Chance für die effiziente Bearbeitung von Algorithmen, insbesondere im Kontext von Optimierungsfunktionen. Allerdings ist er gleichzeitig eine große Gefahr für herkömmliche Verschlüsselungsverfahren, da insbesondere für heutige asymmetrische Verfahren bereits Quantencomputer-Algorithmen existieren, die diese in sehr kurzer Zeit brechen. Aber es gibt durchaus Methoden, die sich quantenmechanische Effekte zunutze machen. Der Quantenschlüsselaustausch (QKD, Quantum Key Distribution) beruht auf quantenmechanischen Prozessen, die nachweislich sicher gegen Quantencomputer-Algorithmen sind.

Oder ist es umgekehrt: Kann gerade diese Leistungsfähigkeit eine neue Methode sein, um gängige Datenverschlüsselungssystem zu knacken?

Ja, für die herkömmliche Kryptographie sind Quantencomputer ganz klar eine Gefahr. Viele Verschlüsselungsverfahren basieren auf mathematischen Einwegfunktionen, die in eine Richtung leicht berechnet werden können, in die andere Richtung aber für heutige Computertechnik praktisch unmöglich zu berechnen sind. Quantencomputer werden aber künftig das bisher Unmögliche möglich machen. Daher sind Experten – auch bei secunet – seit einigen Jahren dabei, die Kryptographie gewissermaßen neu zu erfinden. Das Forschungsgebiet nennt sich Post-Quantum-Kryptographie. Wir sind dabei schon weit vorangekommen, es gibt bereits Quantencomputer-resistente Verschlüsselungsverfahren. Sie basieren auf anderen, komplexeren mathematischen Problemen als die herkömmlichen Methoden. Aktuell gilt es, diese Verfahren zu evaluieren und praxisbezogene Hindernisse aus dem Weg zu räumen. Dazu beteiligen wir uns an internationalen Standardisierungsprozessen des National Institute of Standards and Technology (NIST) und der Internet Engineering Task Force (IETF), um frühzeitig unsere Produkte dafür zu ertüchtigen. Bereits im Jahr 2021 werden wir erste Produkte mit Post-Quantum-Kryptographie auf den Markt bringen.

Zuletzt ein Ausblick: Ist der Fortgang ins Digitale konstant steigend oder wird es auch wieder eine Renaissance des Analogen geben? Oder anders gefragt: Welche Bereiche unseres alltäglichen Lebens werden – aus Ihrer Sicht – von einer Digitalisierung verschont bleiben müssen, weil sie im Äther des Internets nicht funktionieren würden?

Aus meiner Sicht wird alles, was sich digitalisieren lässt, auch digitalisiert werden. Die digitale Welt bietet einfach zu viele Vorteile, um dieses Potenzial ungenutzt zu lassen. Als das papierlose Büro noch eine Zukunftsvision war, konnten sich viele nicht recht vorstellen, dass es einmal Realität werden würde. Heute zeigt nicht zuletzt die Corona-Krise, dass unzählige Homeoffice-Arbeitnehmer recht gut ohne Papierakten auskommen – und sie meist auch nicht vermissen.

Zudem entwickelt sich die Leistungsfähigkeit der Technologien unentwegt weiter bei tendenziell sinkenden Kosten – und der Automatisierungsgrad steigt stetig. Die viel beschworene „Künstliche Intelligenz“ ist z. B. nichts anderes als eine datenbasierte, automatisierte Programmierung – in diesem Fall von neuronalen Netzen. Damit scheint der Weg vorgezeichnet, dass digitale Systeme eine gewisse „Autonomie“ entwickeln und zu einer fortwährenden Digitalisierung drängen. Hier müssen wir aufpassen, dass wir immer die Kontrolle behalten, was da genau passiert – sozusagen digitale Souveränität 2.0.

Im privaten Bereich liegen die Dinge aktuell noch etwas anders: Schallplatten und gedruckte Bücher haben ihre Fans, weil Menschen mit diesen Medien positive Emotionen oder Erinnerungen verbinden. Allerdings gehört die Zukunft auch hier digitalen Formaten. Die analogen Inseln im digitalen Meer werden noch eine Weile Bestand haben, aber sicher nicht ewig.

Interview: Hannes Mittermaier

Dr. Kai Martius

Dr. Kai Martius ist seit 2015 CTO von secunet und wurde im Juni 2019 in den Vorstand berufen. Er verantwortet die Bereiche Technologie/Entwicklung, Produktmanagement und Zertifizierung. Zuvor leitete er von 2007 bis 2015 den Geschäftsbereich Hochsicherheit/Public Sector. Bereits seit 1999, dem Jahr seiner Promotion in der Elektrotechnik an der TU Dresden, war er bei secunet für verschiedene Themen in der Beratung und Produktentwicklung verantwortlich.

Dr. Martius zählt zu den maßgeblichen Architekten der Sicherheitslösung SINA und besitzt darüber hinaus umfangreiche Erfahrungen in der Konzeption, der Umsetzung und dem Einsatz von Sicherheitsprodukten im Behördenumfeld.

Fotos: secunet

1. CYBER SECURITY

Cyber Security hat in den letzten Jahren eine enorme Welle an Popularität erfahren. So zählt es heute zu den meist behandelten Themen im Geschäftsumfeld. Diese Beliebtheit ist einfach zu begründen, denn beim Thema Sicherheit geht es um uns alle betreffende Faktoren: Vertrauen, Angst vor Betrug und monetäre Tätigkeiten. Die zunehmende Verlagerung unserer täglichen Aktivitäten ins Internet hat dem Thema eine zusätzliche Aufmerksamkeit gegeben. Doch wenn heute von Cyber Security geredet wird, ist es schwierig, das Thema überhaupt greifbar zu machen. Wie ist Cyber Security definiert, was ist Internetsicherheit, Informationssicherheit oder Datenschutz?

Die unterschiedlichen Ebenen, mit denen Cyber Security assoziiert wird, heben einerseits das Interesse, verkomplizieren den Gegenstand aber auch. So ist Cyber Security selbstverständlich technischer Natur, aber ebenso hat es eine organisatorische Dimension: Nur wenn eine Maßnahme auch sinnvoll 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 schließlich auch eine menschlich-soziale: Der Anwender muss die Maßnahmen wollen, darf keine Berührungsängste haben und soll sie insbesondere auch verstehen.

Selbst innerhalb dieser skizzenhaft vorgestellten Ebenen tritt nun eine schwierige Kompromissfindung auf, die sich zwischen „Wähle zwei: Sicherheit, Nutzbarkeit, Kosten" auffächert. Was heißt das? Eine sichere und meist einfach zu bedienende Lösung ist oft teuer, umgekehrt ist eine einfach zu bedienende und günstige Lösung oft nicht sicher. Und drittens: Eine günstige und sichere Lösung ist oft nur schwer zu verwenden. Sowohl für Unternehmen als auch für Privatanwender gilt es nun, einen möglichst nutzungseffektiven Weg zu beschreiten.

Ebenso facettenreich wie das Thema Cyber Security sind die einzelnen Beiträge dieser Ausgabe selbst. Sie enthalten unter anderem allgemein orientierte 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 **1.790.000 Mal** geklickt*

Beiträge zum Thema **CYBER SECURITY** erhielten **355.000** Klicks.

	Autor I Thema
#1	**Nicolas Ehrschwendner I** Trügerische Sicherheit: Datenverlust trotz RAID **Seite 77**
#2	**Nicolas Ehrschwendner I** Defekte RAID-Datenträger – ungeahntes Datenmissbrauchsrisiko! **Seite 77**
#3	**Robert Blank I** Die sieben Todsünden des Security Policy Change Managements **Seite 33**
#4	**Roland Messmer I** Threat Hunting: Die Jagd nach Cyberbedrohungen **Seite 48**
#5	**Detlev Weise I** IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich **Seite 78**

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 30. November 2020.**

INHALT

The Power of Industrial Cybersecurity

Hier geht es zu weiteren Fachbeiträgen

Dr. Andreas Kind

Since decades operational environments like factories, train systems, energy networks and city infrastructures have been equipped with dedicated communication and control technology that addresses the specific needs for timing, reliability, availability, and safety. Such operational technology (OT) for industrial equipment, assets, processes and events is increasingly combined with information technology (IT). Strictly isolated before, OT domains are now being connected with the back and middle office for business process integration and analytics. Furthermore, IT best practice and technology components are increasingly being applied in the OT domain, such as certificate-based authentication and secure communication.

This industrial digitalization opens new attack vectors for operational environments – but has also created new approaches for holistic security concepts for human-cyber-physical systems that address all system actors and the full lifecycle of system components. Unfortunately, too often publications focus on individual security incidents. Like folklore, stories about attacks on operational IT (no matter whether observed in the field or only in laboratory conditions) are passed down and shared broadly, while ignoring the actual advances in industrial cybersecurity. In this article we, thus, want to highlight new powerful developments in industrial cybersecurity for converged OT/IT environments, particularly in the context of machine and device identities.

Human-cyber-physical Systems

In general, cyber-physical systems connect the processes of physical devices and machines with computing technology. The conditions of the physical processes are measured by sensors, then provided as input to a controller that evaluates the input according to a digital model of the physical process. The output of the controller is a modification that is applied to the physical process via an actuator. This control loop often runs autonomously following real-time requirements, which make human interaction impossible. Operational personnel are, however, needed to configure and manage the control loop with a human-machine interface (HMI), which can be in the form of a monitoring or engineering system.

Human-cyber-physical systems [1] are potentially vulnerable to cybersecurity attack vectors on the social level, targeting the mental model of the operational personnel in front of the HMI as well as on the digital level, targeting the digital model and controller (Figure 1). In the latter cases, the approach of an attacker is to enforce a disconnect between the mental model (i.e., what the operator thinks is happening) from what is actually happening in the digital and physical world. In the former case, the approach is to enforce a disconnect between the digital model (i.e., what the control system has as dynamic representation of the physical processes) from what is actually happening in the physical world. In both cases, the larger objective of an attacker is, typically, to influence the operation of the physical processes (e.g., hold a factory production, stop a train, cause a blackout). This is sometimes also achieved by simply overloading or breaking systems, for instance in the form of a denial-of-service attack.

The security requirements in human-cyber-physical systems often differ from IT security requirements, which gravitate around confidentiality, integrity, and availability. In operational technology systems, safety and the continuity of operation have generally highest priority. Of course, safety often also depends on integrity and availability. The general threat and risk modeling methodology as well as the sets of security controls, that can be implemented to bring security risks into acceptable levels, are similar for IT and OT systems.

Industrial Cybersecurity today

Ten years after Stuxnet [2], industrial cybersecurity has advanced significantly. The Stuxnet computer worm was aimed at industrial control systems, particularly ones that control centrifuges to separate uranium-235 from uranium-238 isotopes. The worm was introduced to target environments via an infected memory stick. It then propagated across the network, looking for a process control portal (HMI) to modify the portal to give wrong commands to the process controller while pretending to the operator normal system operation. This first major attack against industrial infrastructures (and others that followed) triggered broad awareness and led in multiple areas to advancements in industrial cybersecurity:

Organizational measures: Cybersecurity ownership and responsibility are today anchored at highest management levels in industrial companies, typically in the form of a Chief Cybersecurity Officer (CCSO). In addition, processes are established to enable visibility, define and enforce governance, educate employees and management as well as to provide response capabilities and transparency internally and externally, e.g., computer and product emergency response teams (CERTs). These organizational measures helped tremendously to build, protect, defend and generally manage critical infrastructures with higher safety and security levels today.

Frameworks and standards: In the last decade, the ICT industry has developed frameworks and standards (formal and de-facto) in industrial cybersecurity consisting of collections of security technologies, controls, policies, concepts, guidelines, best practices, and risk management approaches. Some exist already for a longer time but are broadly applied only recently. The most relevant frameworks and requirement standards are:

ISA/IEC 62443 [3] is the most comprehensive standard for security management of plants, facilities and industrial systems. The standard applies to manufacturers, integrators and operators with their specific requirements and defines four security levels that determine security measures accordingly. Initially focused on industrial production, IEC 62443 is already being applied also in other verticals, such as rail or power systems.

NERC-CIP [4] was developed by the North American Electric Reliability Corporation (NERC) as a set of Critical Infrastructure Protection standards, mostly aimed at the bulk electric system, which includes generation and transmission. NERC-CIP standards are regularly enforced by the Federal Energy Regulation Commission.

ISO/IEC 27001 [5] specifies a management system that is intended to bring information security under explicit management control. Enhancements for security controls in specific industry verticals are available in the ISO 27000 series.

NIST published guidelines and frameworks addressing cybersecurity issues associated with the Internet of Things (IoT) and smart manufacturing. In particular, the Cybersecurity Framework [7], which includes a set of industry standards and best practices to help organizations manage cybersecurity risks, is broadly followed.

MITRE ATT&CK [6] is a knowledge base of adversary tactics and techniques built from real observations. The knowledge base is a foundation for the development of threat models and methodologies in the general cybersecurity community, but with applicability in industrial products and solutions.

For regulatory reasons and for better differentiation on the market, many large manufacturers, integrators and operators are getting certified according to ISA/IEC 62443, NERC-CIP or ISO/IEC 27001. In fact, requests for proposal in the process, energy and transportation industry often ask for such certification.

Laws and regulations: Many countries have issued laws and regulations to protect critical infrastructures against cyber-attacks in sectors such as energy, water, food, health, finance, telecommunication, and transport. These laws and regulations refer to, both, organizational measures as well as frameworks and standards. According to the German Security Law (ITSiG) operators of critical infrastructures are required to establish organizational measures, must implement “state-of-the-art” technology and, furthermore, must report security incidents to the Federal Office for Information Security (BSI). In the US, the Presidential Decision Directive 63 (PDD-63) initiated a program for Critical Infrastructure Protection (CIP) that triggered the NIST Cybersecurity Framework. In Europe, the European Programme for Critical Infrastructure Protection (EPCIP) addresses European critical infrastructure that, in case of fault, incident, or attack, could impact both the country where it is hosted and at least one other European Member State [8]. Worth mentioning in the European context is also the Directive on Security of Network and Information Systems (NIS Directive) [17].

Partnerships: Companies operate today in globalized markets with suppliers, partners and customers in all regions in the world. The security, safety and privacy of industrial products, solutions or infrastructures depend on many stakeholders and cannot be solved by a single company alone. Partnerships, like the Charter of Trust [9] help to keep pace with cybersecurity technology and threats, coordinate actions among businesses and governments and set common trust principles between society, politics, business partners, and customers.

Technology: Security in OT environments has significantly improved over the last ten years. Field-level protocols that had literally no security controls at all, are now revamped with authentication, integrity protection and other security controls. The OPC UA (Open Platform Communications Unified Automation) protocol, broadly used in industrial automation, the Industrial Internet-of-Things (IIoT) and smart city systems, includes client/server authentication, user authorization, integrity and confidentiality of communications as well as auditing of client server interactions. Concerns on network and information security and infrastructure integrity with BACnet, a widely used standard in building automation, are now being addressed by BACnet Secure Connect [11]. PROFINET, a data communication protocol over Industrial Ethernet, will soon have security enhancements [10] according to the defense-in-depth approach described in IEC 62443. A challenge comes with the fact that well established security controls were designed with assumptions not suited for OT environments. For instance, TLS key updates can cause unacceptable side-effects on industrial operation. For power system, a standard series has been developed with IEC 62351 to address specific communication protocols utilized in this domain. The standard incorporates state-of-the-art security mechanisms for authentication, authorization, and secure communication.

Key for the integration of OT and IT environments is that technology can bridge both domains securely. For instance, regulations in transportation demand juridical event recording.

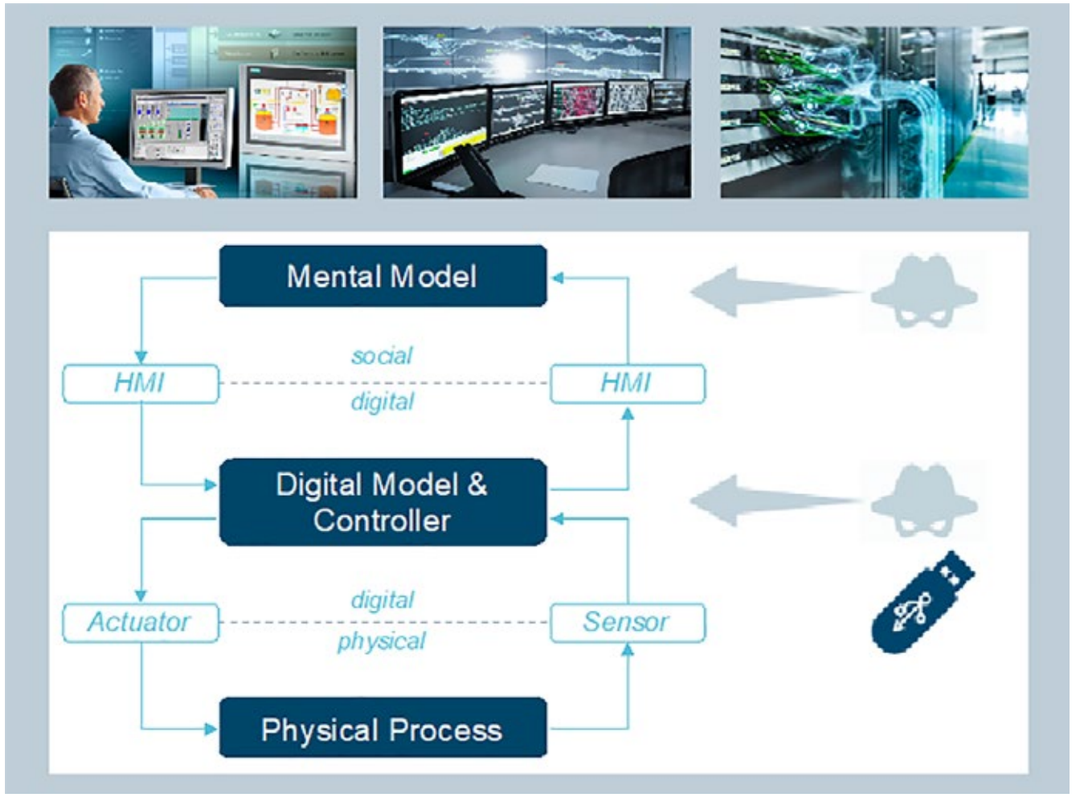


Figure 1: Human-cyber-physical system

Galvanic separation in passive one-way gateways makes sure data can only leave, and never enter, a critical network [12]. Furthermore, various state-of-the-art security technologies (e.g., identity and access management, secure communication, privacy- and confidentiality-preserving techniques) are deployed in industrial cloud infrastructures, such as MindSphere.

Research directions in Industrial Cybersecurity

Industrial cybersecurity is an exciting and relatively new research field. Problem statements and research go far beyond standard IT security due to the involvement of the physical world (e.g., an electricity infrastructure, a hospital, a rail network). The following paragraphs provide evidence about this ongoing research in the areas of identity (Product PKI, Generic Trust Anchor, Zero Touch Onboarding, Zero Trust in OT environments), product lifecycle (DevSecOps, functional agility, penetration testing, industrial asset discovery) as well as in analytics and trust.

A key foundation for many security controls (authentication, signing, encryption, etc.) is identity. In industrial security, the identity of devices and machines is as important as the identity of people. For instance, a device needs an identity during operation for any form of secure communication. But how can the device receive the identity securely from the manufacturer? How can the identity be stored securely on the device? How can the integrator securely and efficiently prepare the device with the identity needed during operation? How can the identity of a device securely be updated or revoked securely? In order to address these questions, research is pursued to build industrial identity solutions based, as much as possible, on existing technologies, such as public key infrastructures (PKI), hardware security modules (HSM) and secure elements. This research goes in the direction of establishing certificate management and digital signature functionality. Such product PKI services are used for securely hosting specific roots and issuing certificate authorities as well as signature keys. A factory can use these services, for instance for issuing "birth certificates" to devices being produced.

A secure element is often used in industrial devices to anchor an unforgeable identity within the device. This can be achieved in the form of a firmware-based trusted platform module, dedicated FPGA, trusted execution environment, physically unclonable function, or hardware security module. However, low-level specifics of secure elements pose challenges for application programmers. Applications could be developed faster and more securely when low-level complexities are hidden by a logical secure element interface. A research direction is, therefore, to define a Generic Trust Anchor interface. An ISO/IEC initiative is currently underway to propose respective specifications [14].

The deployment of devices in the field includes the secure management of "birth certificates" according to the operator's certificate authority. The proper transition from the manufacturer's to the operator's administrative domain is cumbersome and, unfortunately, often shortcut. Research and standardization (IETF, OPC UA) are addressing this problem with new technology called Zero Touch Onboarding. Devices equipped with a "birth certificate" of the manufacturer can be simply dropped in a target environment. Operational certificates will then be automatically deployed using a registrar service, which is connected with the manufacturer's domain.

Today, the internet and, even more, industrial networks are highly fragmented with many levels of segmented intranets in every organization. Firewalls and network address translation set perimeters that are costly to manage and don't actually bring more security in a world of mobile devices, company merger and acquisition, outsourced cloud services and the Industry 4.0. Zero Trust is a network architecture concept that removes network perimeters. Instead, Zero Trust assumes (i) applications and services can be accessed from anywhere in the internet, (ii) identity and access management can be based on user and device certificates (in combination with behavior-based authentication methods) and (iii) strong endpoint protection and management. While for IT environments Zero Trust has been implemented (e.g., by Google), it is today an open research question whether and how OT environments benefit from Zero Trust. Scenarios from the emerging Industry 4.0 suggest that also in industrial networks perimeters will get dissolved in order to enable multi-party interactions within factories for the benefit of higher production flexibility.

Monitoring and penetration testing of devices in OT environments is often demanded for compliance and is clearly essential for anomaly detection and security related asset management. Due to the heterogeneity of devices and protocol stacks, standard asset discovery technology fails to provide the necessary visibility. Advanced analytics-based detection capabilities, applied mostly passively by observing network traffic, is the focus of research teams in the industry. Similarly, dedicated tooling for industrial penetration testing is developed by research teams [1513].

Industrial products have long lifetimes – sometimes up to 30 years. The design of such products has to include mechanisms for updates, upgrades and patches throughout a very long lifecycle. In this context, research is ongoing how to enable crypto agility [13], such that the cryptographic schemes deployed today can be updated continuously in the future. A concern is that integer factorization, discrete logarithm or elliptic-curve discrete logarithm are soon no longer hard problems for quantum computers. In this case, the security based on these mathematical problems can be broken, unless crypto agility would allow products to switch to quantum-safe cryptography.

Security starts with a threat and risk assessment to understand how an attacker can compromise a system. An important research direction is to provide methods and tools for continuous security assessments and compliance according to industrial security frameworks (e.g., IEC 62443) in agile development (DevSecOps), which is increasingly applied for industrial products and solutions [13].

Analytics, machine learning and artificial intelligence are entering also industrial environments. First robots were equipped with neural engines that improve their ability to pick parts during production. Research is starting in the cybersecurity community how to protect such systems from adversarial attacks, which use inputs to machine learning models that are intentionally designed to cause the model to make a mistake. These models may be part of a digital representation of a physical device (so-called Digital Twin), which can be analyzed for anomalies simultaneously with traditional direct monitoring approaches.

Mostly, OT/IT integration is still confined to a single company, a single trust domain. The next phase of digitalization will go beyond company borders and leverage the synergy within entire ecosystems for new productivity growth. First examples, such as pay-per-use financing of machines, demonstrate the strength of tighter ecosystem interaction for new industrial business models. These examples, however, also show the need for research into new technologies to implement trust and confidentiality for future automated ecosystems.

Conclusions

During the past ten years, businesses and governments have advanced significantly in industrial cybersecurity. This is demonstrated by organizational measures, frameworks and standards, laws and regulations, partnerships and technology. Security is increasingly powerful and pre-configured into the design of products, functionalities, processes, technologies, operations, architectures, and business models [9]. In many ways, security is no longer a non-functional, but a functional requirement in critical infrastructures. However, the race between the good and the bad will continue, and contributions from the research community will be essential for the good to stay ahead also in the future.

References: **[1]** Pacaux-Lemoine, Marie-Pierre, Quentin Berdal, Simon Enjalbert, and Damien Trentesaux. "Towards human-based industrial cyber-physical systems." In 2018 IEEE Industrial Cyber-Physical Systems (ICPS), pp. 615-620. IEEE, 2018. **[2]** Stuxnet, Wikipedia, https://en.wikipedia.org/wiki/Stuxnet **[3]** IEC 62443, Wikipedia, https://de.wikipedia.org/wiki/IEC_62443 **[4]** CIP Standards, North American Electric Reliability Corporation, https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx **[5]** ISO/IEC 27001, Information Security Management, https://www.iso.org/isoiec-27001-information-security.html **[6]** MITRE ATT@CK, https://attack.mitre.org/ **[7]** Cybersecurity Framework, NIST, https://www.nist.gov/cyberframework/framework **[8]** John Perdikaris, Physical Security and Environmental Protection, CRC Press, 2014. **[9]** Charter of Trust, https://www.charteroftrust.com/ **[10]** Security Enhancements for PROFINET, https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet/ **[11]** David Fisher, Bernhard Isler, Michael Osborne, BACnet Secure Connect, A Secure Infrastructure for Building Automation, SSPC 135 IT Working Group, http://www.bacnet.org/Bibliography/B-SC-Whitepaper-v15_Final_20190521.pdf **[12]** Secure your data flows and infrastructure with Siemens Data Capture Unit, https://www.mobility.siemens.com/global/en/portfolio/rail/automation/secure-connectivity.html?sitc=wwmoi10007 **[13]** Moyón, Fabiola & Beckers, Kristian & Klepper, Sebastian & Lachberger, Philipp & Bruegge, Bernd. (2018). Towards continuous security compliance in agile software development at scale. RCoSE '18: Proceedings of the 4th International Workshop on Rapid Continuous Software Engineering, 2018. **[14]** Generic Trust Anchor Application Programming Interface for Industrial IoT Devices, ISO/IEC JTC 1/SC 41, Internet of Things (IoT), 2020. **[15]** FLUFFI (Fully Localized Utility For Fuzzing Instantaneously) – A distributed evolutionary binary fuzzer for pentesters, https://github.com/siemens/fluffi **[16]** Project Aquorypt, https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/aquorypt **[17]** The Directive on security of network and information systems (NIS Directive), European Commission, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Dr. Andreas Kind

Dr. Andreas Kind is Head of Cybersecurity Technology at Siemens, Corporate Technology. He received his Ph.D. degree in computer science from the University of Bath, UK and worked in various positions for IBM Research from 2000 until 2018. Andreas is a Senior Member of the ACM.

Foto: Privat

Machine Learning: Fluch oder Segen für die IT-Security

Michael Klatte

Künstliche Intelligenz (KI) und Machine Learning (ML) zählen zu den meistdiskutierten Themen in der IT-Security. Manche erhoffen sich von ihnen den ultimativen Befreiungsschlag gegen Malware, andere befürchten die Zunahme weiter ausgereifter Cyberattacken. Recht haben beide Seiten.

Abb. 1: Plant Ihr Unternehmen, ML in seine Strategie zur IT-Absicherung zu integrieren?

Abb. 2: KI wird/könnte die Anzahl der Angriffe erhöhen, die mein Unternehmen erkennen und abwehren muss.

Künstliche Intelligenz ist nicht Machine Learning

Nicht erst seit gestern ist die Idee der Künstlichen Intelligenz (KI) bzw. richtiger des Maschinellen Lernens (ML) in aller Munde. Welches Veränderungspotenzial diese Technologien jedoch tatsächlich mit sich bringen, ist in vielen Branchen noch nicht oder nicht umfassend bekannt. Nur eines steht fest: Von der Entwicklung tatsächlicher künstlicher Intelligenz, wie wir sie auf der Kinoleinwand antreffen, sind wir noch weit entfernt.

Die Begriffe Künstliche Intelligenz und Machine Learning werden häufig und fälschlicherweise synonym verwendet. Bei KI geht es um die Idee, dass eine Maschine selbstständig „intelligent“ lernen und agieren könnte, ohne menschliches Zutun und allein auf Basis von Input aus der Umwelt. Machine Learning ist mithilfe von Algorithmen zur Datenverarbeitung in der Lage, bestimmte Aufgaben autark zu bewältigen. Die Lösung basiert dabei auf der Fähigkeit des Rechners, in großen Datenmengen schnell Strukturen und Anomalien zu erkennen und auf die für die Fragestellung wesentlichen Punkte herunterzubrechen (Modellgenerierung). Nichtsdestotrotz wird ML meist als die zentrale Grundlage von KI gehandelt.

ML sorgt für mehr IT-Sicherheit

Maschinelles Lernen und eine seiner Methoden, Deep Learning, sind hingegen technisch ausgereift und bereits seit Jahrzehnten Teil unserer IT-Security-Welt. Gesteigerte Aufmerksamkeit erfahren beide jedoch erst in den letzten Jahren. Sie helfen dabei, Betrugsfälle aufzudecken und kriminelle Machenschaften zu analysieren. Damit tragen sie erheblich dazu bei, neue Lösungen für bestehende Probleme zu finden.

Der Trend Machine Learning ist nicht nur in den Köpfen von Entscheidern, sondern längst in der Realität angekommen. Eine von OnePoll im Auftrag von ESET durchgeführte Studie zeigte, dass:

- 82% der Befragten glauben, dass ihr Unternehmen bereits ein IT-Security-Produkt mit ML-Komponenten im Einsatz hat.
- 80% der Befragten zudem der Ansicht sind, dass ML ihrem Unternehmen hilft oder zukünftig helfen wird, schneller auf Gefahren zu reagieren.
- 76% der Befragten nicht davon ausgehen, dass ML dabei helfen wird, einen Mangel an entsprechend ausgebildetem IT-Sicherheitspersonal in ihrem Unternehmen auszugleichen.

Auch Cyberkriminelle gehen mit der „intelligenten“ Zeit

Die Vorteile von ML haben sich auch in der Cybercrime-Branche herumgesprochen. Immer mehr Hacker verwenden sie dafür, potenzielle Opfer beziehungsweise wertvolles Daten-Diebesgut ausfindig zu machen und auszunutzen. Gleichzeitig lassen sich mit Machine Learning Lücken und Schwachstellen finden, bevor diese geschlossen werden können. Nicht zuletzt greifen Kriminelle auf Maschinelle Lernalgorithmen zurück, um ihre eigene IT-Infrastruktur (z.B. Botnetze) zu schützen.

Unternehmen, die Machine Learning in größerem Umfang nutzen, werden hierdurch für Angreifer teils besonders attraktiv. Durch Verunreinigung von Inputdatensätzen beispielsweise sorgen sie dafür, dass eigentlich einwandfrei funktionierende Systeme fehlerhafte Ergebnisse und nicht der Realität entsprechende Bilder der Datenlage produzieren. Chaos, Betriebsstörungen und teils irreparable Schäden sind die Folge.

Malware mit ML im Herzen: Emotet

Ein Beispiel aus der Praxis, das anscheinend auf maschinellem Lernen basiert, ist die im Moment kursierende Schadsoftware Emotet. Diese wird eingesetzt, um andere unerwünschte Anwendungen, z.B. Banking-Trojaner, automatisch auf den Rechner des Opfers herunterzuladen. Dank Machine Learning ist Emotet dabei in der Lage, seine Opfer ganz gezielt auszuwählen. Gleichzeitig ist es erstaunlich gut darin, der Entdeckung durch Forscher, Botnet-Tracker und Honeypots zu entgehen.

Für seine Angriffe sammelt Emotet Telemetriedaten potenzieller Opfer und sendet diese zur Analyse an den C&C-Server des Angreifers. Im Gegenzug erhält es vom Server Befehle oder Binärmodule. Auf Basis dieser Daten wählt die Software nur diejenigen Module aus, die seinem Auftrag entsprechen. Ebenso scheint sie in der Lage zu sein, echte menschliche Akteure von virtuellen Maschinen und automatisierten Umgebungen, wie Forscher und Ermittler sie nutzen, zu unterscheiden.

Besonders auffällig ist dabei die Fähigkeit Emotets, den Unterschied zwischen legitimen und künstlichen Prozessen zu lernen. Dabei werden letztere zunächst akzeptiert, aber innerhalb weniger Stunden auf eine Blacklist gesetzt. Während von den Rechnern „echter“ Opfer aus Daten versendet werden,

So erkennt ESET Malware

Die Verarbeitung eines Malware-Samples durch die ESET Engine erfolgt in mehreren Schritten:

1. Statische Code-Analyse, bei der die Features des Samples extrahiert und so für die Deep Learning-Algorithmen bereitgestellt werden.
2. Emulation als Teil einer dynamischen Analyse. Ergebnis sind die sogenannten DNA-Gene, die dann als Grundlage für Klassifikationsmodelle und einen weiteren Deep Learning-Algorithmus dienen.
3. Währenddessen wird das fragliche Element in einer Sandbox ausgeführt und einer erweiterten Speicherprüfung zugeführt. Das Ergebnis wird für den Vergleich mit bekannten und regelmäßig upgedateten Hashes von sauberen und schädlichen Samples verwendet.
4. Die Ergebnisse der vorangegangenen Schritte werden durch ein neuronales Netz oder andere Auswertungsverfahren vektorisiert und konsolidiert.
5. All diese Informationen werden dann genutzt, um eine abschließende Entscheidung darüber zu treffen, ob das Sample als „sauber", „potenziell unerwünscht" oder „schädlich" klassifiziert wird.

fällt der Schadcode auf Rechnern/Bots auf der Blacklist in eine Art Schlafmodus und stellt jegliche schädliche Aktivität ein.

Derartige Abläufe wären ohne Automatisierung kaum realisierbar. Die hinter Emotet stehenden Angreifer müssten massiv Ressourcen aufwenden, um die Malware zu steuern. Die ESET Experten nehmen daher an, dass Emotet mit maschinellen Lernalgorithmen arbeitet – das Verhalten der Malware ließe sich so mit einem Bruchteil der Ressourcen und wesentlich schneller implementieren.

Selbst Angreifer können nicht zaubern – auch nicht mithilfe von maschinellem Lernen. Auch schädliche Anwendungen haben Grenzen. Dies zeigt sich am Beispiel des Stuxnet-Wurms, der selbst in stark gesicherte Netzwerke eindringen und sich schnell sehr weit verbreiten konnte. Gerade dieses aggressive Verhalten sorgte jedoch auch dafür, dass Sicherheitsexperten auf den Wurm aufmerksam wurden, seine Funktionsweise analysierten und Schutzlösungen entsprechend verstärken konnten.

Ähnlich könnte es Schadsoftware ergehen, die auf ML basiert. Mit zunehmender Menge erfolgreicher Angriffe werden auch solche Schädlinge immer auffälliger und können leichter unschädlich gemacht werden.

Maschinelles Lernen und IoT

Von Beginn an war das Internet of Things (IoT) beliebtes Ziel von Angreifern. Seitdem steigt die Menge an Routern, Überwachungskameras und anderen smarten Geräten immer schneller an. Vielfach sind diese Geräte jedoch extrem unsicher und können oft mit einfachsten Mitteln ausspioniert oder anderweitig missbraucht werden. Typisch sind werkseitig gesetzte oder unsichere Passwörter oder über Jahre bekannte Schwachstellen.

Mithilfe von ML-Algorithmen sind Angreifer noch besser in der Lage, Profit aus diesen Problemen zu schlagen, beispielsweise können sie:

- bisher unbekannte Schwachstellen in IoT-Geräten finden und Unmengen an Daten über Traffic und Nutzerverhalten sammeln, welche dann für das Training von Algorithmen zur Verbesserung von Tarnmechanismen genutzt werden können.
- Standardverhalten und -prozesse bestimmter, rivalisierender Malware lernen, um diese bei Bedarf zu entfernen oder für eigene Zwecke zu missbrauchen.
- auf Basis von Millionen geleakten Passwörtern jedes Jahr Trainingssets mit den effektivsten Passwörtern erstellen. So werden sie in Zukunft noch einfacher in vergleichbare IoT-Geräte eindringen.

Mensch und Maschine als Team können Hacker besiegen

Maschinelles Lernen ist im Kampf gegen Cyberkriminalität von großer Bedeutung, vor allem in Bezug auf die Malware-Erkennung. Anhand riesiger Datenmengen wird ML daraufhin trainiert, digitale Schädlinge korrekt in „gutartig" und „bösartig" zu unterteilen. So lassen sich auch neue und unbekannte Elemente automatisch einer der beiden Kategorien zuordnen. Dazu werden Massen an Inputdaten benötigt – wobei jede Information richtig kategorisiert sein muss. Anders als vielfach dargestellt ist es keineswegs garantiert, dass ein Algorithmus neue Elemente korrekt labelt, nur weil er vorher mit großen Datenmengen gefüttert wurde. Die menschliche Verifizierung im Vorfeld und eine Endkontrolle bei fragwürdigen Ergebnissen bleibt zwingend notwendig.

Im Gegensatz zur Maschine ist der Mensch in der Lage, aus Kontexten zu lernen und kreativ zu agieren. Das ist etwas, zu dem kein noch so weit entwickelter Algorithmus fähig ist. Professionelle Malware-Autoren sind beispielsweise in der Lage, den tatsächlichen Zweck ihres Codes geschickt zu verschleiern. So lassen sich beispielsweise ein bösartiger Code in einzelnen Pixeln einer sauberen Bilddatei oder Codeschnipsel von Schadsoftware in einzelnen Dateien unbemerkt verstecken. Erst wenn die einzelnen Elemente an einem Endpoint zusammengefügt werden, entfaltet sich das schädliche Verhalten. Ist der ML-Algorithmus dann nicht in der Lage, das zu identifizieren, fällt er im Zweifel eine falsche Entscheidung. Ein menschlicher Virenjäger erkennt aufgrund seiner Ausbildung, Erfahrung und einer Portion Bauchgefühl die Gefahr. Daher ist es erforderlich, dass Mensch und Maschine zusammenarbeiten, um aktiv schädliche Aktivitäten zu verhindern.

ML ist nur Teil einer komplexen Sicherheitsstrategie

ML ist in der IT-Security seit den 1990er-Jahren ein wichtiger Sicherheitsbaustein. Wenn das letzte digitale Jahrzehnt etwas gelehrt hat: Für komplexe Probleme gibt es keine einfachen Lösungen. Das gilt besonders für den Cyberspace, wo sich die Bedingungen binnen weniger Minuten verändern können. In der heutigen Geschäftswelt wäre es unklug, sich nur auf eine Technologie zu verlassen, um eine widerstandsfähige Cyberabwehr aufzubauen. IT-Entscheidungsträger müssen erkennen, dass ML zweifellos ein wertvolles Instrument im Kampf gegen Cyberkriminalität ist, aber eben nur ein Teil der gesamten Sicherheitsstrategie eines Unternehmens sein sollte. Und dazu zählt nach wie vor die fachliche Expertise von echten Menschen: den Sicherheitsbeauftragten und Administratoren.

Fazit

Dank Big Data und verbesserter Rechnerleistung ist Machine Learning (ML) in den letzten Jahren zum Mittel der Wahl für unzählige Anwendungsgebiete geworden – darunter IT-Security. Doch die Welt der Internetsicherheit befindet sich im stetigen Wandel. Es ist deshalb unmöglich, sich ausschließlich mit ML-Algorithmen gegen die sich häufig ändernden Gefahren zu schützen. Mehrschichtige Lösungen, kombiniert mit talentierten und qualifizierten Mitarbeitern, werden der einzige Weg sein, den Hackern immer einen Schritt voraus zu sein.

Michael Klatte

Seit fast 20 Jahren beschäftigt sich Michael Klatte mit dem Thema IT und insbesondere der IT-Sicherheit. Regelmäßig publiziert er seine Artikel in deutschsprachigen Fachmagazinen und Online-Portalen. Für ESET ist er seit 2008 tätig und veröffentlicht Fachartikel im ESET-Blog „WeLiveSecurity".de.

Foto: Privat

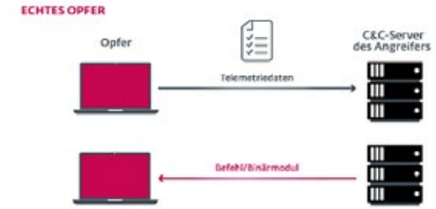


Abb. 3: Der infizierte Rechner eines Opfers übermittelt Telemetriedaten an den C&C-Server des Angreifers und erhält Befehle oder Binärmodule.

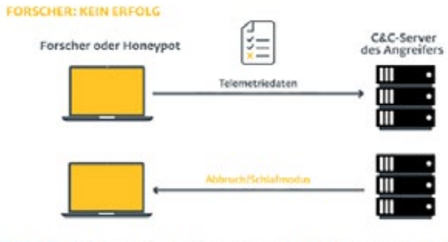


Abb. 4: Der Rechner eines Forschers (Honeypot) versendet gefälschte Telemetriedaten an den C&C-Server und erhält den Befehl, in den Schlafmodus zu gehen bzw. abzubrechen.

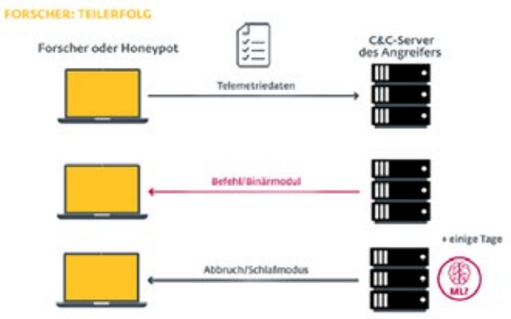


Abb. 5: Der Rechner eines Forschers (Honeypot) sendet künstlich erzeugte Telemetriedaten an den C&C-Server des Angreifers und erhält im Gegenzug Befehle oder Binärmodule. Binnen weniger Tage wechselt Emotet jedoch auch hier in den Schlafmodus.

Cybersicherheit in Industrieanlagen

Dirk Loomans, Marko Vogel

Mit der Digitalisierung steigt auch die Vernetzung in Industrieanlagen und diese geraten somit immer mehr in das Blickfeld von Hackern. Die meisten Anlagen wurden bereits vor langer Zeit installiert, als Cybersicherheit noch kein großes Thema war. Dies wird den meisten nun zur Bedrohung, denn Cybersicherheit hat mittlerweile hohe Priorität für jede erfolgreiche Industrie-4.0-Strategie.

Mit Cybersicherheit den neuen Herausforderungen standhalten

In der Vergangenheit waren die IT und die OT örtlich vollständig voneinander getrennt, das bedeutet, dass jeder Bereich eigenständig arbeitete und über eigene Kommunikationsprotokolle verfügte. Ein Cyberangriff von innen oder außen war praktisch nicht durchführbar. Heute ist aus Effizienz- und Kostengründen (IoT, Industrie 4.0) eine fortgeschrittene internetprotokollbasierte Vernetzung von ICS-Systemen zu beobachten (z. B. IT, Service Provider), was dazu führt, dass Cyberangriffe sowohl von innen als auch von außen viel wahrscheinlicher werden. Die Herausforderung besteht nun darin, trotz steigender Digitalisierung das zuverlässige Produzieren der Industrieanlagen garantieren zu können und selbst bei Cyberangriffen richtig zu reagieren. Zudem sind sich viele Unternehmen der Gefahren nicht bewusst, welchen ihre Anlagen durch Cyberangriffe ausgesetzt sind. Fehlendes Wissen kann dazu führen, dass Unternehmen ihre Anlagen noch nie auf Angriffe überprüft haben, da es an Sensibilisierung für das erhöhte Risiko von Angriffen und deren potenziellen Auswirkungen zu mangeln scheint. Dies bietet die Gelegenheit, sich mittels unterschiedlicher Angriffsarten, sei es gezielt oder ungezielt, Zugriff auf das System zu verschaffen, um die Produktion zu stören, ganzheitlich lahmzulegen oder interne Daten abzufangen oder zu verschlüsseln, mit der Absicht, Unternehmen zu erpressen. Die Herausforderung für die OT, welche in die neue Welt der IT eingedrungen ist, besteht nun darin, diese zu verstehen und ihr Wissen von eingespielten Systemen nun mit der „wackligen Komponente“ IT zu verbinden; denn dort passieren die Angriffe. In Zukunft wird es immer mehr digitale Fabriken geben, in denen alles miteinander vernetzt sein wird. Um die Funktionalität dieser garantieren zu können, ist ein ausgereiftes Cybersicherheitssystem absolut notwendig, da die Gefahr von Cyberangriffen stetig steigt und somit ein wirtschaftliches Risiko für Unternehmen darstellt.

Welche Probleme treten auf?

Oft dauert es viel zu lange, bis der Angreifer im Netzwerk bemerkt wird, da keine Vorkehrungen zur Cybersicherheit getroffen wurden. Produktionsnetzwerke, welche in den meisten Fällen nur Prozesse und Maschinen anstoßen, sind, sobald sie eingerichtet sind, fast frei von menschlichem Zugriff. Dies müsste dazu führen, dass bei einem Cyberangriff auf das System oder die Industrieanlagen, der missbräuchliche Zugriff direkt bemerkt werden kann. Jedoch sind die Systeme in den meisten Fällen nicht in der Lage, jene zu erkennen und zu melden, beziehungsweise reagieren sie erst dann, wenn der Angreifer schon längere Zeit im System ist. Die OT beschäftigt sich zwar mit Sicherheit, jedoch liegt hier der Fokus auf dem reibungslosen und sicheren Arbeiten der Anlagen. Denn Industrieanlagen wurden bislang so gebaut, dass Prozesse richtig aufgezogen wurden und die Produktion fehlerfrei funktioniert. Oft wurde der Aspekt der Einbindung eines Cybersicherheitssystems ignoriert, denn eine Schwierigkeit besteht zum Beispiel darin, die Sicherheitsupdates in den Industrieanlagen einzuspielen, ohne dass es zu einem Produktionsausfall kommt. Die Anlagen sind Tag und Nacht in der Produktion im Betrieb, was es erschwert, den richtigen Zeitpunkt der Aktualisierung zu finden, um garantieren zu können, dass alle Komponenten nach dem Update weiterhin reibungslos funktionieren. Angriffe auf Industrieanlagen sind in erster Linie riskant, da dort bei Manipulation oder durch das Eindringen in das System im schlimmsten Fall Menschenleben in Gefahr sein können. Es gilt nicht, sich erst nach einem Angriff Gedanken zur Sicherheit zu machen, sondern sein Unternehmen so aufzustellen, dass es gar nicht erst zu einem erfolgreichen Angriff kommt oder nur zu einem milderen Verlauf. Wenn das Unternehmen eine direkte Meldung bei Eintritt des Angreifers in das System erhält, kann es schneller handeln und den Angreifer im Produktionsnetzwerk lokalisieren und sperren. Ein weiteres Problem, welches das Einspielen eines Cybersicherheitssystems auf bestehende Industrieanlagen erschwert, ist die Tatsache, dass die Maschinen in Realtime laufen müssen, um die Produktion aufrecht zu erhalten.

Die häufigsten OT-Sicherheitsbedrohungen

Durch das Verknüpfen der OT mit der IT kommen auch gleichzeitig weitere Sicherheitsbedrohungen auf die Industrieanlagen zu. Zu den erwähnten Bedrohungen, wie dem Eindringen von Malware durch beispielsweise Hardware oder Wechselmedien, kommt auch menschliches Versagen hinzu, welches durch schlechtes Training, zu schnelles Arbeiten, Missachten der Sicherheitsvorkehrungen oder Trägheit ausgelöst werden kann. Durch die Anbindung an das Internet steht die OT noch weiteren Sicherheitsrisiken gegenüber. Unter anderem kommt es vermehrt zu DDoS-Angriffen und Attacken durch IoT-Botnets, welche versuchen, die Industrieanlagen lahmzulegen. Meist besteht die Abwehr dieser Angriffe darin, einen Dienstleister mit der Abwehr zu beauftragen, wenn keine eigenen Cybersicherheitssysteme in den Anlagen installiert sind. Cyberkriminelle nutzen IoT-Botnets vermehrt für ihre Angriffe, um eine Vielzahl an Bots mithilfe von C&C-Software (Command and Control) mit für gewöhnlich schädlichen Aktionen zu beauftragen. Durch IoT-Botnets muss der Angreifer nicht mehr länger über Fachwissen verfügen, um eigene Botnets aufzubauen, sondern kann stattdessen für seine Cyberangriffe auf bereits verfügbare Botnets zurückgreifen. Neben dem bereits bekannten Eindringen von Malware durch externe Hardware und Wechselmedien kommt es durch die Internetanbindung auch zur Bedrohung durch Malware Injection. Dies kann sowohl vom Internet als auch dem eigenen Intranet ausgehen. Eine weitere OT-Sicherheitsbedrohung sind kompromittierende Cloud-Komponenten, auf die unberechtigt zugegriffen wird, um dort gespeicherte Daten und Prozessabläufe auszuspähen oder zu manipulieren. Neben den bereits genannten Bedrohungen gibt es selbstverständlich noch eine Vielzahl mehr, welche Unternehmen vor Herausforderungen stellen. Sowohl die Wahrnehmung als auch die Annahme, bereits ausreichende Sicherheit zu gewährleisten, führt dabei oft zu einer dramatischen Fehleinschätzung, wie beherrschbar die Risiken rund um das Industrial Internet of Things, innere Bedrohungen oder das steigende Wissen und die wachsenden Fähigkeiten der Angreifer sind. Als Beispiel mag Stuxnet dienen, ein bösartiger Computerwurm, welcher 2010 erstmals entdeckt wurde und sich vermutlich seit mindestens 2005 in der Entwicklung befindet. Stuxnet zielt auf Überwachungs-, Kontroll- und Datenerfassungssysteme ab und wird für die Verursachung beträchtlicher Schäden am iranischen Atomprogramm verantwortlich gemacht.

Die Herausforderung der IT/OT-Konvergenz

Das primäre Ziel eines industriellen Steuerungssystems ist seine Verfügbarkeit und Funktionalität. Während die IT sich auf die transaktionale Interaktion zwischen Mensch und Anwendung fokussiert, beschäftigt sich die OT weitestgehend mit der ereignisbasierten Interaktion zwischen Bedingungen und Prozesssystemen. Bislang konzentrierte sich die IT nicht darauf, die Reaktionszeiten auf Millisekunden zu reduzieren, da menschliche Prozesse in der Regel Prozessverzögerungen tolerieren. Die OT hingehen, welche Regelkreise erzeugt, kann durch eine Verzögerung von Millisekunden schon eine Prozessverzögerung hervorrufen und somit im schlimmsten Fall ein Menschenleben aufs Spiel setzen. Die Herausforderung der IT/OT-Konvergenz ist es, eine geeignete Cybersicherheitsstrategie zu entwickeln, um das gemeinsame Funktionieren sicher zu gestalten. Denn um die Fabriken von morgen sicher zu gestalten, gilt es nun, die unterschiedlichen Sicherheitsanforderungen, einerseits das Unterstützen menschlicher Arbeitskräfte und ihrer Aktionen und andererseits das Senden direkter Steuerungsbefehle an industrielle Prozesse, zu kombinieren. Fehlende Eigenverantwortung und mangelndes Management von Cyberrisiken stellen Unternehmen vor eine neue Herausforderung. Denn die mangelnden Kenntnisse über Cybersicherheit, fehlendes allgemeines Cyberbewusstsein von Mitarbeitern und ein Mangel an Secure-By-Design bei Produkten und Ökosystemen erschweren es Unternehmen, durch das Zusammenführen von IT und OT eine risikoangepasste Cybersicherheitslösung zu implementieren. Durch eine unzureichende OT-Cybersicherheit und ungenügende Datenschutzressourcen, eine fehlende Überwachung der Identifizierung von Sicherheitsereignissen und das unzureichende Anlageninventar und Systemlebenszyklusmanagement wird die OT vor neue Herausforderungen gestellt. Die fehlende Identifizierung und das Management von Schwachstellen sind zwei der Hauptprobleme, wenn es um die Eindämmung des Risikos von Cyberangriffen auf Industrieanlagen geht.

Eine Architektur zur Identifizierung der Sicherheitskontrollen und -muster

Eine Sicherheitsarchitektur ist in erster Linie die Praxis des Entwurfs von Computersystemen zur Erreichung von Sicherheitszielen. Durch diese wird die Störung eines Systems erschwert und die Erkennung einer Kompromittierung der Anlage erleichtert.

Eine logische Architektur für ein OT-Netzwerk, die zur Identifizierung der Sicherheitskontrollen und -muster verwendet werden sollte, besteht aus vier verschiedenen Zonen – der Sicherheitszone, Zellen-/Bereichszone, Herstellungszone und Unternehmenszone. Das sogenannte Purdue Model liefert einen anschaulichen Überblick über das komplizierte Automatisierungsnetz. In der Unternehmenszone läuft der unterstützende (Geschäfts-)Betrieb eines Unternehmens ab, welcher aus der Sicht des Anlagennetzes als äußerst unsicher gilt. Darunter folgt die Herstellungszone. Diese umfasst den Herstellungsbetrieb und die Herstellungskontrolle vor Ort. Hierzu gehören unter anderem das Bereitstellen jeglicher Systeme, Dienste

Quelle: KPMG in Deutschland, 2020

und Anwendungen, die für das Industrienetz notwendig sind. In der Zellen-/Bereichszone befinden sich die Systeme, die zur Überwachung und Steuerung der speziellen Prozessführung verantwortlich sind. Sie beinhaltet außerdem auch die Systeme, welche unmittelbaren Einfluss auf die Ausführung und Steuerung des physischen Prozesses haben. Diese arbeitet in Echtzeit, wodurch eine Störung auf dieser Stufe zu einer direkten Beeinträchtigung des automatisierten Prozesses führt. In der Sicherheitszone gilt es, den (arbeits)sicheren Betrieb zu gewährleisten.

Unterschied zwischen IT und OT

Obwohl IT und OT immer weiter zusammenwachsen, gibt es zwischen den beiden jedoch erhebliche Unterschiede. Während sich die IT mit Maßnahmen zum Schutz vor Maleware schon seit Langem beschäftigt und einen hohen Reifegrad erlangt hat, wird die Umsetzung von Schutzmaßnahmen im OT-Umfeld durch die mangelnde Flexibilität beim Ändern der zugrunde liegenden IT-Installationen erschwert und geradezu unmöglich gemacht. Durch regelmäßige technologische Aktualisierungen liegt der Lebenszyklus in der IT bei 3–5 Jahren, während die OT der Industrieanlagen mit einer Lebensdauer von 10–25 Jahren teilweise sehr alte Sicherheitslücken ohne jegliches Sicherheitskonzept aufweisen. Diese Sicherheitslücken entstehen oftmals durch das „Einfrieren“ des verwendeten IT-Betriebssystems, ohne die Möglichkeit der Durchführung von (Sicherheits)Updates. Die Anforderungen an Verfügbarkeit und Funktionalität eines industriellen Steuerungssystems erschweren so die Verwaltung von Änderungen, da die Maschinen kontinuierlich und in Echtzeit arbeiten und jede Millisekunde entscheidend ist. Dies ist auch der Fall, um das Risiko des Verlusts von Menschenleben zu verringern und den reibungslosen Produktionszyklus garantieren zu können. Im Vergleich ist die Umsetzung von Schutzmaßnahmen in der IT weniger kompliziert, da dort Verzögerungen und Auszeiten toleriert werden und die Kenntnisse zum Schutz vor Angriffen deutlich weiter ausgebaut sind. In der IT ist die Wahrscheinlichkeit, dass Menschenleben in Gefahr gebracht werden, geringer, denn das Risiko bezieht sich in erster Linie auf den Verlust von Daten und die Verletzung der Vertraulichkeit.

Wirksamer Schutz vor Cyberbedrohungen

Die Vernetzung von Sensoren, Maschinen und Fahrzeugen bietet eine weite Angriffsfläche für Cyberkriminelle. Angreifer schleusen beispielsweise ein Gerät in eine IIoT-Infrastruktur ein, welches vorgibt zu diesem Netz zu gehören, da dort Maschinen und Anlagen der Produktion unverschlüsselt über WLAN kommunizieren. Durch das eingeschleuste Gerät lässt sich das System manipulieren, lassen sich Daten sammeln oder wird im schlimmsten Fall die Produktion gestört.

Durch eine Public Key Infrastructure (PKI) kann die notwendige Sicherheitstechnologie für den Austausch sicherer Daten in einer vernetzten Umgebung bereitgestellt werden. Die PKI schafft eine Vertrauensbasis in OT- und IIoT-Umgebungen und stellt sicher, dass nur autorisierte Komponenten im Netzwerk agieren können. Um einen wirksamen Schutz vor Cyberbedrohungen aufzubauen, sind im Allgemeinen folgende fünf Säulen für Sicherheitsanforderungen im Industrieumfeld zu beachten.

1. **Governance und Strategie:** Der Aufbau und die Führung eines Cybersicherheitssystems kann mithilfe des Plan-Do-Check-Act-Zyklus die kontinuierliche Verbesserung von Produkten und Prozessen herbeiführen. Das Modell dient zur Umsetzung von Veränderungen und ist eine wichtige Voraussetzung für die kontinuierliche Verbesserung von Prozessen, denn das Unternehmen kann hierdurch wiederkehrende Fehler vermeiden und somit Prozesse optimieren.
2. **Risikomanagement:** Um effektives Risikomanagement betreiben zu können, verfolgt die zweite Säule der OT-Cybersicherheit das Prinzip „Accept-Treat-Tolerate-Transfer“ (Akzeptieren-Behandeln-Tolerieren-Übertragen). Um Risiken korrekt einschätzen zu können, gilt es, diese in unterschiedliche Stufen einzuordnen. Beispielsweise kann die Fähigkeit, etwas gegen manche Risiken zu unternehmen, eingeschränkt sein oder die Kosten für das Ergreifen der Maßnahmen stehen in keinem Verhältnis zum gewonnenen Nutzen. In diesem Fall ist „Tolerate“ ein wichtiger Faktor, mit dem das Risiko von Angriffen oder Ähnlichem konsequent überwacht wird, sodass das Management bereit ist zu reagieren, falls es zu einer Eskalation kommt. Hier werden sogenannte Toleranzniveaus bestimmt, um die Ausmaße des jeweiligen Risikos auf den einzelnen Ebenen festzulegen und abzuschätzen, wie die Entscheidungen diese beeinflussen können. Die meisten Risiken fallen jedoch in den Bereich „Treat“. Hier handelt es sich um den Einsatz von Maßnahmen zur Verringerung der Eintrittswahrscheinlichkeit und nicht unbedingt um die Vermeidung eines Risikos. Der Schaden soll so auf ein akzeptables Maß begrenzt werden. Um in Zukunft auf ähnliche Risiken vorbereitet zu sein, ist es daher wichtig, über das bereits Gelernte zu reflektieren und festzustellen, was geändert werden muss, und diese Erkenntnisse dann auf ähnliche oder gleiche Risiken zu übertragen, um diese zu beseitigen.
3. **Sicherheitsintegration:** Cybersicherheit ist die Summe aus Sicherheit und Zuverlässigkeit. Aus diesen beiden Komponenten gilt es, eine erfolgreiche Cybersicherheitsstrategie in bereits bestehende Industrieanlagen zu integrieren, ohne den laufenden Prozess zu unterbrechen oder im schlimmsten Fall lahmzulegen, um einen wirtschaftlichen oder menschlichen Schaden für das Unternehmen zu vermeiden.
4. **Sicherheitsimplementierung:** Die erfolgreiche Implementierung eines Sicherheitskonzeptes funktioniert nur durch eine holistische Betrachtung des Gesamten. Erst das Einbeziehen von Menschen, Prozessen und Technologie in die Sicherheitsimplementierung ermöglicht es, alle Komponenten abzudecken, um eine Industrieanlage gegen Angriffe zu schützen. Der Menschenteil der Gleichung repräsentiert die Bedürfnisse der Benutzer – auch wenn diese nur einen geringen Zugriff auf die verwendeten Prozesse haben, dürfen sie nicht vergessen werden. Prozesse beziehen sich in diesem Zusammenhang auf Geschäftsziele, die berücksichtigt werden müssen, um erfolgreiche Veränderungen im Unternehmen voranzutreiben. Die Technologie steht für die Implementierung, welche die höchsten Kosten verursacht, dabei jedoch den geringsten Ertrag für das Unternehmen liefert, allerdings bei einem Angriff die notwendigen Maßnahmen bereitstellt, um größere Schäden zu vermeiden. Menschen, Prozesse und Technologie müssen deshalb aufeinander abgestimmt sein, damit eine effektive und ganzheitliche Sicherheitsimplementierung erfolgen kann.
5. **Sicherheitsoperation:** Die fünfte Säule folgt dem Muster „Erkennen-Antworten-Wiederherstellen“. Je nach aufkommendem Risiko wird der Angriff erkannt, es wird mit der geeigneten Sicherheitsoperation reagiert und am Ende zu einem Normalzustand zurückgekehrt, um den Regelbetrieb wiederherzustellen.

Die Cybersicherheit der zukünftigen Industrieanlagen

Die Digitalisierung und Verbindung aller Komponenten untereinander – vom Lieferanten bis zum Kunden – wird in Zukunft Realität sein. Durch die gegenseitige Verbindung wird ein Cyberangriff von innen oder außen erhebliche Auswirkungen auf die gesamte Lieferkette und gleichzeitig einen großen Einfluss auf die Wirtschaftlichkeit von Unternehmen haben, da bei einem Angriff oder einer Manipulation nicht nur der Produktionszyklus, sondern die gesamte Lieferkette gestört werden kann. Um dies weitestgehend einzudämmen, sollen die einzelnen Komponenten in Zukunft mit der Fähigkeit ausgestattet werden, beispielsweise ihre Log-Daten an ein zentrales System (z. B durch Integration in ein SCADA) zu schicken, das dann auf Vorfälle reagieren kann. Dies, zusammen mit einer durchdachten IT-/OT-Sicherheitsarchitektur wie oben skizziert, ermöglicht es, Angriffe auf die OT früh genug erkennen und schadensminimierend reagieren zu können. Bis dahin kann der Weg ein weiter sein.

Dirk Loomans

Der Diplom-Physiker besitzt langjährige Erfahrung in der Beratung mittelständischer, international agierender Industrieunternehmen. Zudem lehrt er als Professor für Wirtschaftsinformatik an der Hochschule Mainz und arbeitet als Gutachter für die Europäische Kommission im Förderprogramm HORIZON 2020.

Marko Vogel

Der Diplom-Ingenieur berät seit über 18 Jahren Industriekunden zu Cyber-Sicherheitsthemen. Er verantwortete zahlreiche Cyber-Transformationsprogramme, um den Schutz kritischer Informationen zu verbessern und die Reaktionsfähigkeit auf einen Cyberangriff zu optimieren.

Fotos: Privat

1.1 SICHERE IDENTITÄTEN

Sieben Wege Ihr Konto vor Hackerangriffen zu schützen

Mit Corona hat sich das Home-Office für viele Unternehmen zur neuen Norm in der Arbeitswelt entwickelt. Sicherer ist die IT deshalb jedoch nicht geworden. Die Angriffe auf Mitarbeiterkonten und Online-Accounts zeigt diese Gefahr nur allzu deutlich.

IT-Sicherheit in Remote-Arbeitsumgebungen ist für Unternehmen keine leichte Aufgabe. Wenn der Umstieg ins Home-Office dann auch noch notgedrungen und in kürzester Zeit realisiert werden soll, nimmt das digitale Risiko für Mitarbeiter gänzlich neue Dimensionen an. Jeder Arbeitsrechner, der an private oder öffentliche Wi-Fi-Netzwerke angeschlossen wird, vergrößert automatisch die Angriffsfläche für Cyberangriffe. Und jedes neue Tool aus der Cloud, birgt Sicherheitsrisiken. In der Regel werden daher Anwendungen von der Unternehmens-IT einer genauen Überprüfung unterzogen ehe sie dem Mitarbeiter zur Verfügung gestellt werden. Während der Corona-Krise in den letzten Wochen und Monaten fehlte dafür jedoch in vielen Fällen schlichtweg die Zeit.

Hier geht es zu weiteren Blogbeiträgen

Sicher „Zoomen“ oder doch lieber telefonieren?

Zoom ist hierfür ein Paradebeispiel. Das Videokonferenz-Portal erlebte mit Corona einen Boom und verzeichnete allein im März einen Anstieg des täglichen Datenverkehrs um 535%. Zwar dauerte es nicht lange bis kritische Stimmen auf die mangelhaften Sicherheitsmaßnahmen und Datenschutzrichtlinien der Lösung aufmerksam machten. An der weiteren Verbreitung sowohl im privaten als auch beruflichen Umfeld änderten diese berechtigten Einwände nur wenig. So nahmen im April pro Tag bis zu 300 Millionen Nutzer weltweit an Zoom-Videokonferenzen teil.

Zoom steht nur exemplarisch für eine Reihe von Lösungen, die von Mitarbeitern eigenmächtig und ohne Abstimmung mit der IT heruntergeladen werden und als Schatten-IT den Sicherheitsverantwortlichen in Unternehmen Kopfzerbrechen bereitet. Das Risiko von unkontrollierten IT-Assets ist groß. Fehlt das korrekte Setup und die Integration in eine ganzheitliche Sicherheitsstrategie (inkl. Sicherheits- und Versionsupdates), ist es nur eine Frage der Zeit bis Cyberkriminelle Sicherheitslücken der Anwendungen ausnutzen. Zumal das Sicherheitsbewusstsein bei vielen Usern zu wünschen übrig lässt. Welche Konsequenzen beispielsweise eine schlechte Passworthygiene haben kann, lässt sich erneut an Zoom demonstrieren. Im April tauchten im Dark Web sowie auf kriminellen Marktplätzen die Anmeldeinformationen für mehr als eine halbe Million Zoom-Konten auf. Zoom selbst war jedoch nicht gehackt worden. Die zum Verkauf stehenden Passwörter stammen aus früheren Datenleaks, die nun von Cyberkriminelle erneut herangezogen werden, um Angriffe auf Online-Accounts zu starten.

123 – und das Konto ist gehackt

Das systematische und automatisierte Wiederverwenden von einmal geleakten Passwort/Login-Kombination – auch als Credential Stuffing bekannt – ist für Hacker mit relativ wenig Aufwand verbunden. Das liegt zum einen daran, dass die Kreativität von Anwendern bei der Vergabe von Passwörtern gelinde gesagt „verbesserungswürdig“ ist. Auf Platz eins der beliebtesten deutschen Passwörter 2019 steht so nicht zum ersten Mal die Zahlenkombi „123456“. Zum anderen vergeben viele Anwender immer wieder ein und dasselbe Passwort für unterschiedliche Online-Accounts. In den USA trifft das auf zwei von drei Internetnutzern zu. Wirklich überraschend ist diese unschöne und höchst gefährliche Angewohnheit nicht. Wer im Netz beruflich oder privat unterwegs ist, muss zwangsläufig Zugangsdaten für Konten einrichten – im Durchschnitt sind es 191 Passwörter. Die Mehrfach-Nutzung eines Passworts mag demnach nur zweckmäßig erscheinen, zu entschuldigen ist diese Praxis aber nicht (Stichwort Passwort Manager). Passworthygiene – also starke und einmalig verwendete Passwörter, die in regelmäßigen Abständen geändert werden – gehört deshalb auch zu den absoluten Grundvoraussetzungen der IT-Sicherheit.

Ungebetene Gäste im eigenen Online-Account

Werden solche Richtlinien auf Unternehmensseite nicht genügend forciert, ist es nur eine Frage der Zeit bis Konten gehackt und geleakte Zugangsdaten zum Verkauf im Dark Web angeboten werden. Für Unternehmen kann das teuer werden. Allein in den USA beliefen sich 2017 die Schäden von Account Takeover Fraud (ATO) auf über 5,1 Mrd. Dollar. Für Cyberkriminelle gehört ATO zum Standardrepertoire. Haben Sie erst einmal Zugriff auf ein Konto, lassen sich sensible Daten für Phishing-Angriffe sammeln oder für Erpressungen nutzen (Sextortion). In anderen Fällen dienen die Accounts nur als Basislager, um das Netzwerk von Unternehmen weiter zu infiltrieren, Malware einzuschleusen oder die technische Infrastruktur des Anwenders zu nutzen (Botnet). Standen anfangs vor allem E-Commerce Webseiten und Bankkonten im Visier der Angreifer, sieht sich mittlerweile jede Plattform, die eine Registrierung erfordert, dem Risiko von Identitätsdiebstahl ausgesetzt. Mit Corona und Home-Office sind nun Video-Konferenz-Plattformen wie Zoom ins Visier geraten.

Die Zahl der exponierten Zugangsdaten im Open, Deep und Dark Web steigt kontinuierlich. Der Threat Intelligence-Experte Digital Shadows führt so in seiner Datenbank über 16 Mrd. geleakte Anmeldeinformationen. Das Analystenteam stieß bei seiner Recherche zudem auf eine neue Masche beim Verkauf von sogenannten Combolisten. Gewöhnlich handelt es sich dabei um lange Textdateien, die Millionen von Benutzernamen- und Passwortkombinationen enthalten. Bekanntestes Beispiel ist die 2017 entdeckte „The Anti Public Combo List”, die mehr als 562 Mio. Zugangsdaten enthielt und sich aus unterschiedlichen Datenleaks wie Adobe, Dropbox, LinkedIn und Yahoo zusammensetzte. Seit 2019 finden sich im Dark Web auch Combolists-as-a-Service (CaaS): Akteure können ein Abonnement für nur 50 US-Dollar abschließen und erhalten damit 30 Tage lang Zugriff auf eine Liste an Zugangsdaten – darunter auch Daten von Amazon, Ubisofts Uplay und Netflix.

Credential Stuffing & Bot-Technologie

Zu Recht stellt sich die Frage, ob das geleakte Netflix-Passwort eines Mitarbeiters wirklich ein Sicherheitsrisiko für dessen Unternehmen darstellt. Statistisch gesehen ist die Erfolgsquote von Credential Stuffing tatsächlich eher gering. Ein Angreifer müsste sein Glück bei 1.000 Konten versuchen, um einmal mit dem richtigen Passwort einen Volltreffer zu landen. Dass sich das Geschäft trotzdem lohnt, liegt an der schieren Masse an exponierten Anmeldeinformationen sowie dem Einsatz moderner Credential-Stuffing-Tools und Bot-Technologie.

Vereinfacht ausgedrückt ist ein Bot eine Software, die über das Internet mit anderen Webseiten und Endgeräten interagiert. Mehrere Bots lassen sich zu einem Netzwerk zusammenschließen (Botnet) und können Hunderte, Tausende oder Zehntausende von Anmeldeversuchen gleichzeitig auf ein Konto starten. Damit können Cyberkriminelle Kontoübernahmen und Identitätsdiebstahl hochgradig optimieren und automatisieren. Da die Anmeldeversuche scheinbar von verschiedenen Gerätetypen und IP-Adressen kommen, helfen auch die Sicherheitsmaßnahmen von Webanwendungen nur wenig (z. B. Sperren der IP-Adressen bei mehrfach erfolgloser Anmeldung). Dass ein Credential Stuffing-Angriff stattfindet verrät meist nur die Zunahme des Gesamtvolumens der Login-Versuche.

Sieben Sicherheitsmaßnahmen gegen ATO

Wie lassen sich solche Angriffe also stoppen und Kontoübernahmen und Identitätsdiebstahl verhindern? Die eine Lösung gibt es dafür nicht. Unternehmen sollten vielmehr unterschiedliche und ineinandergreifende Sicherheitsstrategien implementieren und ganzheitlich durchsetzen – sowohl im Home-Office als auch am Arbeitsplatz vor Ort.

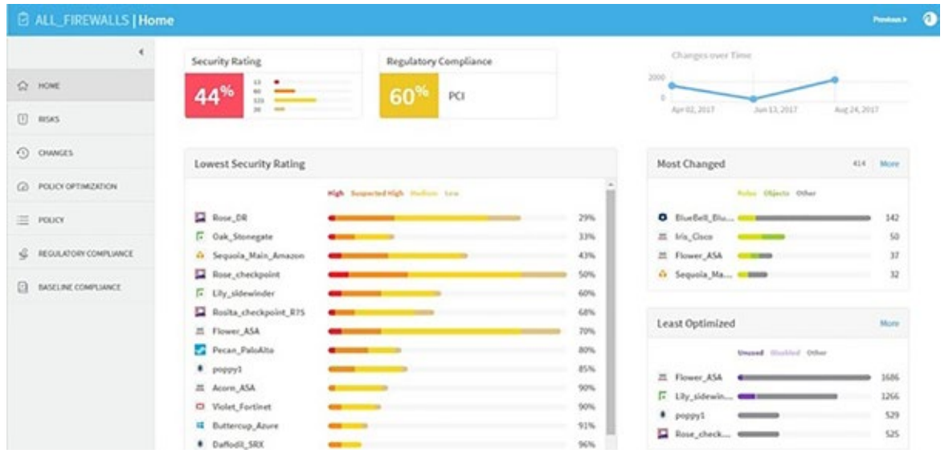
1. Monitoring von Zugangsdaten von Mitarbeitern. Es gibt eine ganze Reihe an kostenlosen Tools, Webseiten und Services, die Unternehmen beim Monitoring von digitalen Risiken zur Seite stehen. Auf der Webseite HaveIBeenPwned können Anwender schnell und unkompliziert nach Datenleaks fahnden – beispielsweise der Email-Domain eines Unternehmens. Andere Monitoringtools scannen das Open, Deep und Dark Web nach exponierten Daten und melden Datenschutzverstöße und aktuelle Bedrohungen.
2. Monitoring des Unternehmens- und Markennamens. Wer sich online bewegt, sieht sich automatisch digitalen Risiken ausgesetzt, das gilt für den einzelnen Anwender genauso wie für Unternehmen. Die fortlaufende Beobachtung von Bedrohungen rund um Webseite, Social Media, Kundenportal und Online-Shop, kann dabei nicht nur das Risiko von Kontoübernahmen minimieren, sondern auch Reputationsschäden und Markenmissbrauch (Spoof Domains) verhindern. Eine einfache Form des Monitorings stellen Google Alerts dar, die richtig konfiguriert gute Indikatoren für drohende ATO-Versuche liefern.

Stefan Bange ,
Country Manager DACH ,
Digital Shadows

3. Monitoring von Zugangsdaten von Kunden. Was für Daten von Mitarbeitern gilt, trifft auch auf Kundendaten aus dem Online-Shop, Abonnenten des Newsletters oder Geschäftspartnern zu. Unternehmen sollten hier vorsorglich Kommunikationsstrategien entwerfen, um im Ernstfall betroffene Anwender schnell und transparent über Datenleaks aufklären zu können.
4. Online-Firewall für Webanwendungen. Kommerzielle und Open-Source-Firewalls, wie ModSecurity, helfen, Angriffe auf Zugangsdaten zu identifizieren und zu blockieren.
5. Sicherheitsbewusstsein schärfen. Cybersicherheit ist die Aufgabe eines jeden Mitarbeiters. Dementsprechend vehement sollten Unternehmen intern Aufklärungsarbeit über digitale Risiken, Bedrohungsakteure und Betrugsmaschen betreiben. Dazu gehören Schulungen, die zeigen warum eine gute Passworthygiene auch im Eigeninteresse von Anwendern nötig ist, sowie einfache Leitfäden und Best Practices. Darüber hinaus muss klar sein, wie im Ernstfall zu reagieren und wer über Vorfälle benachrichtigt werden soll.
6. Monitoring von Credential Stuffing-Tools. Um zu verstehen welche Sicherheitsmaßnahmen gegen ATO und Credential Stuffing greifen, ist es notwendig, die eingesetzten Tools und Technologien der Angreifer zu kennen. Credential Stuffing-Tools haben sich in den letzten Jahren kontinuierlich weiterentwickelt. Als eines der beliebtesten Tools unter Hackern gilt SentryMBA, das mittlerweile in der Lage ist, Sicherheitskontrollen wie CAPTCHAs zu umgehen.
7. Zwei-Faktor-Authentifizierung (2FA). Um eine zusätzliche Barriere zu schaffen und Angreifer auszubremsen, wird neben dem Passwort ein weiterer Faktor in den Authentifizierungsprozess mit aufgenommen. Am bekanntesten sind hier zufällig generierte SMS-Token, die an das Smartphone des Anwenders geschickt werden und laut Google automatisierte Bot-Attacken zu 100% blockieren. Auch 96% der großangelegten Phishing-Kampagnen sowie 76% von gezielten Angriffen (Spear Phishing) lassen sich auf diese Weise entschärfen. Trotzdem gelten SMS-Token zu Recht als die unsicherste 2FA-Variante, denn die Token können auf ihrem Weg aufs Handy abgefangen werden.

Wie beim Einbruch in ein Haus, lässt sich auch das Konto von Anwender auf unterschiedliche Weise knacken: Entweder man verschafft sich gewaltsam Zutritt, oder man sucht nach dem Ersatzschlüssel unter der Fußmatte. Unternehmen, die ihre Mitarbeiter und Kunden vor Kontoübernahmen schützen wollen, müssen sich deshalb nicht hinter einer Batterie an Passwörtern und Sicherheitsmaßnahmen verschanzen. Zu einfach sollten sie es den Angreifern jedoch auch nicht machen. Der Schlüssel für eine effektive Strategie liegt eher darin, die richtige Balance zwischen Sicherheit und Datenschutz auf der einen, sowie Praxistauglichkeit und Nutzerfreundlichkeit auf der anderen Seite, zu finden.

Stefan Bange

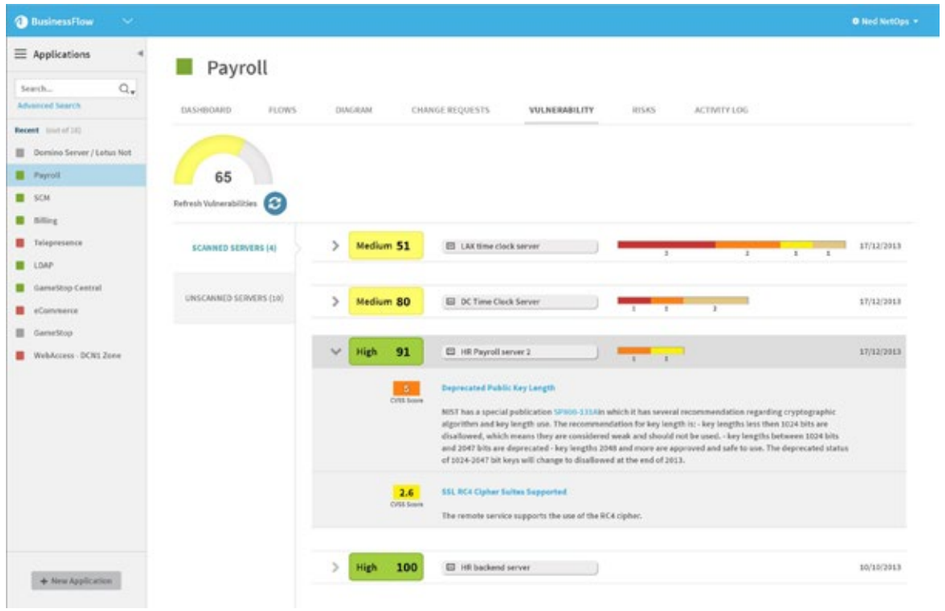


Die sieben Todsünden des Security Policy Change Managements

Die Verwaltung ständig wachsender Netzwerksicherheitsrichtlinien wird nicht einfacher. IT- und Cybersicherheit sind mit immer mehr Bedrohungen, der zunehmenden Komplexität und gestiegenen Anforderungen an Sicherheit und Anwendungskonnektivität konfrontiert. Viele Unternehmen versäumen es jedoch, ihren Ansatz für das Management von Sicherheitsrichtlinien anzupassen, um mit diesen Herausforderungen Schritt zu halten. In den letzten Jahren haben sich sieben „Todsünden“ des Security Policy Managements herausgebildet, die in fast jeder Organisation zumindest teilweise stattfinden. Ein genauer Blick im eigenen Unternehmen lohnt sich.

1. Kein Fokus auf die Geschäftsanwendungen: Wenn ein Verantwortlicher für IT-Sicherheit über Netzwerksicherheit nachdenkt, ist er oft schnell dabei, einen netzwerkzentrierten statt eines anwendungszentrierten Ansatzes zu wählen: Das heißt, er konzentriert sich auf die IP-Adressen, Ports, Protokolle, VPN-Tunnel usw. Das bedeutet allerdings, den Weg und nicht den Zweck zu betrachten. Die Dokumentation konzentriert sich entsprechend oft auf diese Elemente der Infrastruktur. Der Grund, warum der Netzzugang gewährt wurde, erscheint dann als nachträglicher Gedanke im Kommentarfeld, falls er überhaupt nachvollzogen werden kann. Oft denken die Verantwortlichen erst viel später darüber nach, was die wichtigste Frage sein sollte: Warum gibt es diese Regel überhaupt? Welche Geschäftsanwendung unterstützt sie?
2. Keine Bereinigung der Firewall-Regeln für stillgelegte Anwendungen: Wenn ein Unternehmen eine Anwendung bereitstellt, erstellt die Netzwerksicherheit Regeln und definiert Zugriffsrechte. Wenn jedoch eine Anwendung außer Betrieb genommen wird, geschieht der umgekehrte Schritt selten. Der nicht benötigte und aus Sicht der Sicherheit unerwünschter Zugriff wird beibehalten, weil man befürchtet, dass ein Entfernen zu Problemen führen kann. Der Gedanke scheint zu sein: Wenn es nicht kaputt ist, repariere es nicht. In der Regel ist das Gegenteil der Fall. Die Zugänge, die für keinen Geschäftszweck erforderlich sind, summieren sich und schaffen Unordnung. Dies macht es einem Angreifer viel einfacher, eine erfolgreiche Attacke durchzuführen. Hinzu kommt, dass die Vorbereitung eines Audits erschwert wird.
3. Duldung oder Förderung einer ineffektiven Kommunikation: Die Wartung einer großen IT-Infrastruktur erfordert mehrere Teams: ein Sicherheitsteam zur Definition und Durchsetzung von Richtlinien, ein Operation-Team zur Sicherstellung der Verfügbarkeit und des ordnungsgemäßen Betriebs des Netzwerks sowie ein Anwendungsteam zur Unterstützung der Geschäftsanwendungen. Typischerweise kümmern sich diese Teams sehr wenig um die Arbeit der anderen Teams und sprechen sehr unterschiedliche Sprachen. Die Kommunikation ist entsprechend katastrophal. Dafür gibt es viele Gründe: unterschiedliche Berichtsstrukturen, kulturelle Unterschiede und unterschiedliche Ziele. Das macht es für jedes Team schwierig, das Netzwerk und seine Herausforderungen genauso zu sehen wie die jeweils anderen, wodurch Fehler auftreten und es zu langen Durchlaufzeiten bei der Bearbeitung von Änderungen kommt.
4. Unzureichende oder fehlende Dokumentationen: Die Dokumentation ihrer Arbeit ist für die meisten Experten der unangenehmste Teil der IT-Arbeit, aber sie ist entscheidend. Wenn eine Regel nicht dokumentiert ist, geht das Wissen darüber verloren, warum sie konfiguriert wurde. Daraus folgt die Herausforderung, zu wissen, wie man mit Änderungen

Robert Blank, Regional Sales Manager DACH, AlgoSec



umgeht, die sich auf eine Richtlinie auswirken. Darüber hinaus führt eine schlechte Dokumentation zu sehr umständlichen Audits, weil ein Auditor nicht damit zufrieden sein wird, wenn man ihm sagt, etwas könne nicht nachvollzogen werden, weil der Verantwortliche das Unternehmen verlassen hat. Die Netzwerksicherheit muss zuverlässig beantworten können, warum eine Regel existiert. Der Versuch, das Monate oder Jahre nach der Implementierung herauszufinden, macht noch mehr Arbeit und Umstände als die anfängliche Dokumentation.

5. Kein Recycling bestehender Firewall-Regeln und -Objekte: Ein häufiges Problem. Eine Person ruft alle IP-Adressen für die Datenbank „DB_srv“ auf. Wenige Wochen später erstellt jemand anderes „dbserver“ für die gleichen Adressen und ein paar Monate später erstellt jemand „databasesrv“ – erneut für denselben Zweck. Nicht nur, dass all diese Duplikate Unordnung schaffen, es verwirrt jeden im Team, der versucht herauszufinden, warum es drei Datenbanken gibt, welche Unterschiede zwischen ihnen bestehen und ob sie noch benötigt werden.
6. Wilde Änderungen zulassen: Jedes Unternehmen hat jene Administratoren, die ohne jeden Prozess oder eine Genehmigung ihre Firewall-Konsole starten und Änderungen vornehmen. Das mag mit den besten Absichten geschehen wie eine Ad-hoc-Änderung, die schnell durchgeführt werden muss. Aber selbst dann können die Auswirkungen verheerend sein. Eine Vielzahl von Organisation erlebt immer wieder, dass es zu Anwendungs- und Netzwerkausfällen kommt, die durch Änderungen an den Sicherheitsrichtlinien verursacht werden, ohne dafür eingerichtete Prozesse einzuhalten.
7. Manuelle Eingabefehler aufgrund „dicker Finger“: Irren ist menschlich, aber ein IT-System wird das nicht verzeihen. Wenn Sicherheitsteams Änderungen manuell codieren oder verarbeiten, laufen sie Gefahr, Fehler zu machen. Diese machen das Netzwerk möglicherweise anfällig für Angriffe oder Ausfälle. Ein Fall ist ein einfacher Tippfehler des Administrators, der versehentlich Port 433 anstelle von Port 443 eingibt, weil er „dicke Finger“ hat. Die Folgen davon können für sein Unternehmen, die Mitarbeiter sowie letztlich die Geschäftsbilanz – im besten Fall – unangenehm sein. Es benötigt allerdings nicht viel, damit eine solche Situation in eine katastrophale Verletzung der IT-Sicherheit resultiert. Ohne eine Möglichkeit, Fehler zu erkennen oder Prozesse zu automatisieren, laufen die Verantwortlichen Gefahr, menschliche Fehler zu machen und Zeit mit Aktivitäten zu verschwenden, die eine Software schnell und zuverlässiger erledigen könnte.

Fazit

Die manuelle Verwaltung von Sicherheitsrichtlinien wird immer schwieriger, weil die Regelkataloge stetig umfangreicher und die Netzwerkinfrastruktur in Unternehmen zunehmend komplexer werden. In vielen Organisationen lässt sich feststellen, dass diese Herausforderung in sieben „Todsünden“ resultiert, deren Minderung Prozesse, Transparenz und Automatisierung erfordert. Diese Schritte in einem Unternehmen zu etablieren, ist aufwendig, aber die notwendige Arbeit ist es wert, da sie sowohl die Sicherheit als auch die Agilität einer Organisation wesentlich verbessern kann.

Robert Blank

Warum sich Hacker in einer zunehmend vernetzten Welt besonders wohl fühlen – und wie man sich gegen sie wehrt

Phishing ist ein Internet-Scam, bei dem sich jemand als vertrauenswürdige Partei ausgibt, um Zugang zu den sensiblen Informationen eines Benutzers wie Kreditkartennummern, E-Mail-Adressen oder Passwörtern zu erhalten. Das heißt, dass zum Beispiel E-Mails versendet werden, die augenscheinlich im Namen des Bankinstituts versendet wurden und den Nutzer auf auffällige Kontoaktivitäten aufmerksam machen möchten. Doch statt der Bank stecken hinter der E-Mail-Betrüger, die durch den Vertrauensvorsprung, den man dem Bankinsitut gegenüberbringt, Zugangsdaten oder persönliche Informationen abfangen wollen.

Gerade aktuell ist die Gesellschaft vornehmlich digital vernetzt. Wenn man daher jemals Zweifel daran hatte, wie sehr das Internet unser Leben beherrscht, wird die Corona-Pandemie, diese ausgeräumt haben. Noch nie waren so viele Menschen von ihren Liebsten getrennt oder haben im Home-Office gearbeitet wie zurzeit. Über das Internet verbunden zu sein, war in den letzten Wochen und Monaten daher von unschätzbarem Wert. Während das soziale Leben nun an das Social Distancing angepasst wird, verlassen sich immer mehr Menschen auf das Internet. Um Freunde oder Familie zu sehen, werden Tablets, Handys oder Computer genutzt. Auch das Arbeitsleben hat sich verändert und findet zunehmend digital statt - Videokonferenz-Apps florieren. Zoom, eine der beliebtesten Apps, erlebte einen enormen Benutzeranstieg von 10 Millionen Benutzer pro Tag im Dezember zu bis zu 200 Millionen User im März 2020.

Der Anstieg der Nachfrage nach Internetanwendungen wurde von Sicherheitsexperten mit Vorsicht wahrgenommen. Damit einher gingen Warnungen, dass die Pandemie von Cyberkriminellen ausgenutzt werden wird. Denn auch Phishing-E-Mails werden zurzeit von einem Thema dominiert: Dem Corona-Virus. Proofpoint fand heraus, dass bis zum 27. März bereits 500.000 Scam-E-Mails, 300.000 verdächtige URLs und 200.000 Anhänge versendet wurden – jeweils mit Inhalten mit Corona-Virus-Bezug.

Besonders in Krisenzeiten sind Phishing-Versuche weit verbreitet, denn sie spielen mit den Ängsten und Sorgen der Menschen. So gab es beispielsweise E-Mails, die angeblich von der Weltgesundheitsorganisation (WHO) versendet wurden und über den aktuellen Ausbruch informieren sollten. Hacker nutzen diese E-Mails, um Malware zu versenden, Bankdaten zu stehlen oder Zugang zu weiteren Accounts zu erlangen.

Doch wie kann man sich davor schützen, Opfer von Phishing-Attacken zu werden? Die einfachste Möglichkeit digitale Identitäten zu verteidigen besteht darin, die Stärke der verwendeten Passwörter zu überprüfen. Das ideale Passwort ist ein Passwort, das aus einer einzigartigen und zufälligen Buchstaben- und Zahlenfolge von ausreichender Länge und Komplexität besteht, um einfachen, automatisierten „Brute-Force“-Angriffen Stand zu halten. Verschiedene Tools können hier unterstützen, um schnell sichere Passwörter zu generieren. Darüber hinaus sollten Passwörter regelmäßig geändert werden, da Verstöße oft monate-, manchmal sogar jahrelang unentdeckt bleiben. Durch das regelmäßige Ändern der Passwörter kann sichergestellt werden, dass Konten weiterhin geschützt sind.

Mit den folgenden fünf Tipps schützt man Aktivitäten im Internet zusätzlich vor Angriffen von Cyberkriminellen:

Emmanuel Schalit, CEO, Dashlane

1. Aktualisierung von Webbrowser und Betriebssystem

Wird ein Browser nicht regelmäßig aktualisiert, läuft er nicht nur langsam, sondern kann für eine Vielzahl von Sicherheitsbedrohungen anfällig sein. Darunter Viren, Malware, Spyware und weitere schädliche Anwendungen. Die Leistung und Sicherheit eines Browsers werden verbessert, wenn man das neueste Update verwendet. Dasselbe gilt für die Betriebssysteme von Mobilgeräten, Laptops und Desktops. Dies dauert in der Regel weniger als eine Stunde und kann zum Beispiel über Nacht geschehen.

2. Online-Banking-Benachrichtigungen

Entgegen der weitverbreiteten Meinung werden nicht alle Identitätsdiebe Kontodaten für ausschweifende Einkaufstouren nutzen. In der Regel werden sie kleinere Einkäufe über Kreditkarten tätigen oder mehrere kleine Beträge Bargeld abheben, um die Bank nicht auf ungewöhnliche Aktivitäten aufmerksam zu machen. Mobile Online-Banking Apps bieten daher in der Regel Benachrichtigungen an, die sie über Abbuchungen informieren. Vorsicht ist jedoch bei E-Mail- Warnungen zu verdächtigen Aktivitäten der Bank geboten, denn auch hier sind Phishing-Mails weit verbreitet. Auf Link Clicks in E-Mails, die nicht erwartet werden, ist daher zu verzichten, da hier eine URL hinterlegt sein kann, die auf eine Webseite führt, die der der Bank gleicht, jedoch zum Beispiel Zugangsdaten speichert. Daher sollte jede URL eigenständig im Browser eingegeben werden oder direkt die mobile App genutzt werden. Denn jede Nachricht

der Bank ist auch in den Online- Anwendungen der Bank einzusehen, so kann überprüft werden, ob es sich tatsächlich um eine Nachricht der Bank handelt oder einen Phishing-Versuch.

3. Bonitätsprüfungen
Die Überprüfung der eigenen Bonität steht häufig nicht an der ersten Stelle von To-Do-Listen zur Verbesserung der Sicherheit im Internet. Zusammen mit der Einrichtung von Online-Banking- Benachrichtigungen, kann die regelmäßige Überprüfung der Bonität jedoch auf verdächtige Aktivitäten aufmerksam machen. Zusätzliche Kreditkarten können zum Beispiel die Bonität verschlechtern. So können Unregelmäßigkeiten schnell auffallen. Denn wird überprüft, ob Konten auf den eigenen Namen eröffnet wurden, von denen man nichts weiß, kann man sich sicher sein Opfer von Identitätsdiebstahl geworden zu sein und entsprechend handeln.

4. Aktivieren der Zwei-Faktor-Authentifizierung auf einem Konto
Onlinekonten kann eine zusätzliche Sicherheitsebene hinzugefügt werden durch die Aktivierung einer Zwei-Faktor-Authentifizierung (2FA). Die Zwei-Faktor-Authentifizierung fügt einen zusätzlichen Faktor zum normalen Login-Verfahren hinzu, um die Identität zu überprüfen. Dies geschieht durch die zusätzliche Abfrage von zwei von drei möglichen Identifikatoren: etwas, das man kennt (Passwort, PIN-Nummer, Postleitzahl, etc.), etwas das man besitzt (Smartphone, Smartcard, etc.) oder etwas das man ist (Fingerabdruck, Iris-Erkennung oder Stimmerkennung). Durch die Aktivierung der Zwei-Faktor- Authentifizierung macht man es Cyberkriminellen besonders schwer, da nicht mehr nur das Abfangen von Zugangsdaten notwendig ist, um Zugang zu Online-Konten zu erlangen.

5. Durchatmen
Ein gesundes Maß an Vorsicht um die digitale Sicherheit ist vorrausschauend – und ein wenig anstrengend. Bei Vorsichtsmaßnahmen, um das digitale Leben zu schützen, geht es nicht darum eine große Anzahl an Produkten zu besitzen, sondern darum sich über bewährte Verfahren und hilfreiche

Tools zu informieren. Nutzt man jetzt die Zeit, um sich auch digital abzusichern, spart man in Zukunft viel Zeit und Nerven.

Es gibt aktuell viel Unsicherheit in der Welt und genau darauf haben Hacker gewartet. Zum Glück kann man sich durch die hier genannten Tipps und weitere Ressourcen vor ihnen schützen und ihnen ihr kriminelles Tun so besonders schwer machen.

Emmanuel Schalit

Was uns 2,5 Millimeter über Identity Management lehren können

Die Themen Datenschutz und -Sicherheit sind für Unternehmen weiterhin eine bedeutende Herausforderung, schließlich sind Cyberangriffe allgegenwärtig und der potenzielle Schaden immens. So zeigte das diesjährige Allianz Risk Barometer, dass Cybervorfälle erstmals als wichtigstes Geschäftsrisiko für Unternehmen weltweit angesehen werden. Für die neunte Auflage der Umfrage von Allianz Global Corporate & Specialty wurden mehr als 2.700 Risikoexperten aus über 100 Ländern zu den wichtigsten Unternehmensrisiken befragt. Weiterhin fanden jüngst Forscher des Kriminologischen Forschungsinstituts Niedersachsen und der Leibniz Universität Hannover heraus, dass 41 Prozent der Firmen in Deutschland in den vergangenen zwölf Monaten Opfer einer schweren Cyberattacke wurden. Der durchschnittliche Schaden pro Angriff lag bei 16.900 Euro. Doch so ernst die Lage auch scheint, die gute Nachricht ist, Betriebe können ihr Sicherheitsniveau durch organisatorische, vor allem aber technische Maßnahmen deutlich erhöhen und sind Angriffen nicht schutzlos ausgeliefert. Doch bevor es darum geht, wie man den Risiken effektiv begegnen kann, und welche Rolle das Thema Identitätsmanagement dabei spielt, hier ein Exkurs in die Luftfahrt.

Rückblick: Der British Airways-Flug 5390
Folgendes Szenario: Der britische Flugkapitän Tim Lancaster hängt in einer Höhe von 5.300 Metern aus dem Cockpitfenster seiner Maschine. Es waren 2,5 Millimeter, die ihn fast das Leben kosteten.

Zum Hintergrund: Der British Airways-Flug BA 5390 war am 9. Juni 1990 mit 81 Passagieren an Bord nach Málaga in Spanien aufgebrochen. Dreizehn Minuten nach dem Start – die Maschine hatte inzwischen eine Flughöhe von 5.300 Metern erreicht – hörten die Passagiere einen lauten Knall, und binnen zwei Sekunden ging der Kabinendruck verloren. Einer der Flugbegleiter rannte ins Cockpit und sah dort, wie Co-Pilot Alastair Atchison verzweifelt versuchte, die Kontrolle über das Flugzeug zurückzugewinnen, während Kapitän Lancaster aus dem offenen Frontfenster gesogen worden war – nur seine Beine befanden sich noch im Flugzeug.

24 Stunden zuvor waren an der Maschine, einem BAC 1-11 Jet-Airliner, Wartungsarbeiten durchgeführt worden. Dabei bemerkte ein Schichtleiter, nennen wir ihn Bob, dass 90 Schrauben an einer Cockpitscheibe des Flugzeugs ersetzt werden mussten. Er entfernte die Schrauben, ging mit einer dieser ins Lager und verglich sie dort mit den zahlreichen anderen Schrauben. Er identifizierte die benötigten Schrauben rein vom Sehen, ohne in die Service-Anleitung zu schauen. Dann wollte er 89 weitere Schrauben mitnehmen, stellte aber fest, dass sechs zu wenig da waren. Weil die Zeit drängte, fuhr Bob zu einem anderen Warenlager, zu dem er Zutritt hatte, und nahm dort sechs Schrauben mit, die den anderen ähnlich sahen. Ob er überhaupt Befugnis haben sollte, diesen Teil des Lagers zu betreten, war nie überprüft worden. Und Bob hatte nicht auf dem Lagerplan nachgesehen, wo sich die benötigten Schrauben befanden, sondern „wusste“ einfach, dass es die richtigen waren.

Zurück am Flugzeug, machte sich Bob an die Arbeit und ersetzte die Schrauben an der Cockpitscheibe. Allerdings hatte er nicht den richtigen Schraubendreher zur Hand. Er beschloss, einen Drehmomentschlüssel zu Hilfe zu nehmen und die Schrauben mit 9 Kilogramm Drehkraft anzuziehen – „das wird sicher reichen“, dachte er.

Leider passten der Schraubendreher und der Drehmomentbegrenzer nicht genau und sie waren auch etwas zu kurz, um damit an die Oberseite der Cockpitscheibe zu kommen. Als er sich über das Geländer seiner Arbeitsplattform beugte, konnte er die Schrauben an der Oberseite gerade noch erreichen, aber dies erforderte Geduld, einen guten Gleichgewichtssinn und viel Ausprobieren. Da einige Schrauben nicht für die Scheibe gedacht waren, rutschte der Schraubendreher beim Erreichen des Drehmoments leicht ab. Der Gedanke dahinter war, dass das schon in Ordnung ginge.

Was hat all das aber nun mit Identitätsmanagement zu tun?
Wie viele Mitarbeiter, die in Unternehmen tätig sind oder waren, haben immer noch die Möglichkeit, auf die Anwendungen und Daten zuzugreifen, zu denen sie in ihrer früheren Funktion Zugang hatten? Wie viele Mitarbeiter, so wie Bob, haben Betriebe schon innerhalb des Unternehmens versetzt, ohne zu prüfen, ob sie weiter Zugang zu Informationen haben, die für ihre neue Funktion unangemessen sind?

Bob hatte einen klar abgesteckten Aufgabenbereich; hier übernahm er allerdings die Rolle eines Technikers und niemand kontrollierte an diesem Abend seine Arbeit an dem Flugzeug. Man ging einfach davon aus, dass er wusste, was er tat. Wie viele Mitarbeiter von Unternehmen erhalten nur deswegen Zugang zu Plattformen und Anwendungen, weil es schon immer so war? Die Frage, die sich hier stellt ist, benötigt es einer Plattform, die alle Zugriffe laufend überprüft, Empfehlungen erteilt und gegebenenfalls auch die Zugriffsrechte entzieht?

Jede Firma hat solche Mitarbeiter, die eigentlich nur helfen und sich für ihr Unternehmen engagieren wollen. In diesem Fall jedoch hatte Bob dank seiner Führungsposition Zugang zu einem unkontrollierten Lagerraum und zu Ausrüstung, die er überprüfen und hinterfragen hätte sollen. Zudem setzte er sich über das System hinweg, indem er die falschen Werkzeuge verwendete. Auf die Welt der IT-Zugriffe übertragen, hieße das: Er nutzte seine erweiterten Zugriffsrechte, um das System zu umgehen, damit die Arbeit getan werden kann.

In der anschließenden Untersuchung nach dem Vorfall wurde festgehalten, dass es die falschen Schrauben waren, die das Cockpit-Fenster sichern sollten, dass Bob die üblichen, korrekten Verfahrensweisen nicht eingehalten hatte und dass niemand seine Arbeit überprüft hatte. Die Schrauben, die Verwendung fanden hatte, waren 2,5 Millimeter kürzer als die richtigen Schrauben und hielten sie der Belastung, die beim Unterdruck auf 5.300 Metern herrscht, nicht stand. Als alle sechs Schrauben herausgesprungen waren, wurde das Fenster herausgerissen.

Alastair Atchison konnte schließlich die Kontrolle über das Flugzeug zurückgewinnen und sicher landen, und glücklicherweise überlebten alle Insassen. Dem Flugbegleiter war es gelungen, den Kapitän an den Beinen festzuhalten. Und obwohl der Kapitän 22 Minuten aus dem Cockpit hing, erholte er sich vollständig und konnte später seinen Beruf wieder aufnehmen.

Wie Betriebe sich schützen können
Um konkret zurück zum Thema IT-Security zu kommen: Um ihr Sicherheitslevel drastisch anzuheben und ein Maximum an Schutz für ihre Daten zu ermöglichen, sollten Unternehmen dringend technisch vorsorgen. Hier ist vor allem eine geeignete Identity-Plattform wichtig, die dafür sorgen kann, dass Mitarbeiter über alle Versetzungen und Veränderungen hinweg verwaltet und kontrolliert werden. Im Falle, dass jemand versucht, das System oder seine Zugriffsrechte zu umgehen, sollte eine solche Plattform automatisch die zuständige Stelle benachrichtigen, Empfehlungen erteilen und gegebenenfalls Sicherheitsmaßnahmen ergreifen, indem sie den Zugriff automatisch sperrt, wenn nötig.

Um verheerende „2,5-Millimeter-Fehler“ zu vermeiden, sollten Unternehmen daran denken, eine Lösung aus dem Bereich Identity Management zu implementieren.

Ben Bulpett

Ben Bulpett, EMEA Marketing Director, SailPoint

Just-in-Time-Access: Ein Garant für Sicherheit und Agilität

Wie Untersuchungen von Gartner zeigen, setzen heute nur rund 10 Prozent der Unternehmen bei der Regulierung von privilegierten Zugriffen auf Just-in-Time (JIT)-Strategien. Dies bedeutet, dass der Großteil von ihnen Mitarbeitern dauerhaften Always-on-Access, d.h. zeitlich unbegrenzte Zugänge, zu kritischen Konten und

Stefan Schweizer, Regional Vice President Sales DACH, Thycotic

Ressourcen gewährt. Dieses Vorgehen mag bequem sein, da wichtige Arbeitsprozesse ohne Unterbrechungen aufrechterhalten werden können, verstößt jedoch gegen das Least Privilege-Prinzip und bedeutet für Unternehmen erhebliche Sicherheitsrisiken.

Können Mitarbeiter auf kritische Anwendungen oder Systeme zugreifen, obwohl sie diese zur Erledigung ihrer Arbeit nicht (oder nicht mehr) benötigen, erhöht sich das Risiko für bewussten oder unbewussten Missbrauch. So besteht etwa die Gefahr, dass Mitarbeiter unkontrolliert unautorisierte Handlungen durchführen, sensible Daten exfiltrieren oder privilegierte Passwörter mit unbefugten Kollegen teilen, die dann auf eine kritische Ressource zugreifen, ohne in einem entsprechenden Audit-Trail aufzutauchen. Gleichzeitig bergen unbegrenzte Zugriffe das Risiko, dass ehemalige Mitarbeiter oder Partner auch nach ihrem Ausscheiden aus dem Unternehmen weiterhin Zugang zu Unternehmensprivilegien haben und diese dann für ihre Zwecke missbrauchen.

Um die Cyberangriffsfläche ihres Unternehmens nachhaltig zu minimieren, müssen IT-Verantwortliche privilegierte Zugriffe systematisch einschränken. Dabei spielt neben der Standort-Restriktion, d.h. von wo aus User Zugang zu Privilegien haben, und der Handlungseinschränkung, d.h. was Benutzer mit privilegierten Konten machen können, die zeitliche Begrenzung der Zugriffe eine sehr wichtige Rolle. Je enger diese Begrenzung gefasst ist, desto kürzer ist das Zeitfenster, das Angreifern – seien es externe Hacker oder böswillige Insider – zur Verfügung steht, um in die Systeme einzudringen, sich dort lateral zu bewegen und Privilegien unentdeckt zu erhöhen.

Just-in-Time (JIT)-Zugriffe für mehr Sicherheit und mehr Agilität

Die Umsetzung eines funktionierenden Just-in-Time-Ansatzes ist für viele IT-Abteilungen eine Herausforderung. Denn nicht immer fällt es leicht, Zeitfenster so festzulegen, dass es zu keinen Behinderungen der Arbeitsprozesse kommt. Immerhin lässt sich nicht immer von vornherein klar bestimmen, wie lange Aktivitäten, die privilegierten Zugang erfordern, voraussichtlich dauern werden. Außerdem ist es nicht unüblich, dass vielbeschäftigte IT-Administratoren hin und wieder vergessen, privilegierte Konten auslaufen zu lassen oder nach Abschluss von Projekten oder dem Ausscheiden eines Mitarbeiters zu deaktivieren.

Dabei umfasst der JIT-Ansatz zwei verschiedene Möglichkeiten, um den Benutzern privilegierten Zugang nur dann zu gewähren, wenn sie ihn tatsächlich benötigen. Eine Möglichkeit ist dabei die Einrichtung von Einweg-Konten, die unmittelbar nach der einmaligen Nutzung gesperrt bzw. komplett gelöscht werden. Deutlich effektiver und langfristig gesehen weniger aufwendig ist jedoch das Erstellen von JIT-Zugängen. Hier werden keine kurzlebigen Konten erstellt, sondern reine Zugriffe, die Privilegien auf Anfrage vorübergehend – das kann 30 Minuten lang sein, aber auch mehrere Wochen oder Monate – erweitern und nach dieser Zeit dann automatisch ablaufen.

Weniger Reibungsverluste dank Automatisierung

Um zu vermeiden, dass die Benutzer jedes Mal auf die neue Freigabe durch einen befugten IT-Mitarbeiter warten müssen, ist es ratsam, den Genehmigungsprozess für zeitbeschränkte Zugriffe zu automatisieren. Fortschrittliche Privileged Access Management-Tools ermöglichen es Sicherheitsverantwortlichen, vorab granulare Richtlinien zu erstellen, welche eine Rechtfertigung für den Zugang zu kritischen Systemen, Datenbanken oder Anwendungen verlangen und Freigaben dann ohne das manuelle Eingreifen eines Mitarbeiters automatisch erteilen. Ist dies geschehen, können die Benutzer dann auf die von ihnen benötigten Ressourcen zugreifen, ohne selbst das Passwort zu kennen, da dieses in einem zentralen Passworttresor erstellt und verwaltet wird.

Hat der Nutzer seine Tätigkeit beendet und benötigt keinen Zugang mehr, meldet er sich ab, woraufhin der Zugriff unverzüglich widerrufen wird. Einige PAM-Lösungen verfügen über spezielle Checkout-Funktionen, die Anmeldedaten automatisch rotieren lassen, sobald der Abmeldevorgang beendet ist, so dass selbst dann, wenn die Anmeldedaten dem Benutzer nicht verborgen geblieben sind, er nicht mit den gleichen Anmeldedaten zurückkehren kann. Diese Automatisierung des JIT-Workflows entlastet sowohl die Endnutzer als auch die IT-Teams und sorgt für weniger Reibungsverluste und mehr Produktivität.

Klassische Just-in-Time-Szenarios

Drittanbieter: Externe Partner und Drittanbieter, die Zugriff auf Unternehmensressourcen benötigen, stellen IT-Administratoren oft vor Herausforderungen. Sie bedeuten ein höheres Sicherheitsrisiko, weshalb ihre privilegierten Zugriffe anders verwaltet und vor allem stärker überwacht werden müssen, als dies bei internen Mitarbeitern der Fall ist. PAM-Lösungen mit JIT-Ansatz ermöglichen es den verantwortlichen Administratoren, spezielle Policies für Auftragnehmer und Partner zu definieren. Diese stellen sicher, dass notwendige Aufgaben wie Fehlerbehebungen, Wartungen oder Penetrationstests problemlos von Drittanbietern durchgeführt werden können, reduzieren gleichzeitig aber das Zeitfenster für den Zugriff auf das notwendige Minimum. Das Risiko für Missbrauch oder Kompromittierungen, etwa nach einem selbst nicht zu kontrollierenden Sicherheitsvorfall bei einem Partner, wird auf diese Weise minimiert.

Remote-Mitarbeiter: Mitarbeiter, die remote arbeiten – sei es von zuhause oder unterwegs –, bedeuten für die IT-Sicherheit eines Unternehmens eine Herausforderung, weshalb sie klassische Kandidaten für JIT-Zugriffe darstellen. Indem privilegierte Zugriffe automatisch enden, selbst wenn der User einmal vergessen sollte, sich aktiv von einem Account abzumelden oder eine Anwendung zu beenden, wird einem Privilegien-Missbrauch in unkontrollierten Umgebungen vorgebeugt.

Bei Software zur Berechtigungserweiterung, die auf den Endgeräten installiert ist, können zuvor definierte Richtlinien zudem genau bestimmen, welche Aktionen durchgeführt werden können und welche Prozesse mit administrativen Rechten ausgestattet werden. Dies bedeutet, dass kein Benutzer nach der Beantragung des Zugriffs jemals die vollständige Kontrolle über eine Ressource erhalten wird.

Service-Konten: Anders als Named-Accounts, die einem Benutzer zugeordnet sind, werden Service-Konten – genauso wie andere Non-Human-Accounts – aufgrund der begrenzten menschlichen Interaktion selten inventarisiert und kontrolliert. Dies macht sie zu einem großen Sicherheitsrisiko, weshalb eine zeitliche Gültigkeit unabdingbar ist. PAM-Richtlinien können festlegen, dass Service-Konten automatisch stillgelegt werden, sobald sie nicht mehr benötigt werden, bzw. bis Administratoren mittels einer Überprüfung eine weitere Gültigkeit aktiv bestätigen.

Entwickler & DevOps-Teams: Entwickler und DevOps-Teams benötigen sicheren, aber gleichzeitig schnellen Zugriff auf privilegierte Ressourcen. Da statische IP-basierte Tresor-Lösungen den Anforderungen von DevOps-Umgebungen nicht gerecht werden, veröffentlichen viele DevOps-Manager Anmeldedaten für geschäftskritische Datenbanken, Konten oder Apps in ihren internen oder öffentlichen Speichersystemen wie z.B. GitHub. Dies birgt jedoch schwerwiegende Sicherheitsrisiken. Unternehmen sollten in diesen Fällen auf PAM-Tools setzen, die spezielle Hochgeschwindigkeitstresore bieten und temporäre Zugangsdaten für mehrere Cloud-Account-Typen oder Container generieren. Dies garantiert Sicherheit, ohne die Arbeit der Entwickler zu behindern.

Schrittweise Umsetzung

Die Einrichtung und Umsetzung von Just-in-Time-Zugriffen sollten systematisch und nach einer zuvor festgelegten Priorisierung erfolgen. Es empfiehlt sich, zunächst risikoreiche Anwendungsfälle zu adressieren und solche Situationen, von denen bekannt ist, dass sie nur selten genutzt werden. In einem zweiten Schritt kann dann eine Migrationspfad entworfen werden mit dem Ziel, die JIT-Strategie über sämtliche privilegierte Zugänge auszuweiten.

Wie bei allen privilegierten Aktivitäten sollte auch der privilegierte JIT-Zugriff in einem zentralen Tool aufgezeichnet und protokolliert werden, um eine einheitliche Berichterstattung und Auditierung zu gewährleisten. Jede privilegierte Aktivität, die sich außerhalb eines zentralen PAM-Tools abspielt, sollte einen Alarm erzeugen und eine entsprechende Überprüfung nach sich ziehen.

Basis dieses ganzen Prozesses ist eine gut durchdachte Least-Privilege-Strategie, die sicherstellt, dass der Zugriff auf Privilegien so eng wie möglich gefasst ist – sowohl was die Art der Konten, Systeme und Anwendungen angeht, als auch die zeitliche Verfügbarkeit.

Stefan Schweizer

1.2 ANGRIFFS-OBERFLÄCHEN

Mit Nutzerverhaltensanalyse Insider-Threats bekämpfen

Der Datendiebstahl durch Insider stellt die traditionelle IT-Sicherheit vor große Herausforderungen. Dies liegt vor allem daran, dass die Innentäter Mitarbeiter sind, die im Gegensatz zu externen Angreifern das Recht haben, im Netzwerk zu sein und auf Systeme und Daten zuzugreifen. Entsprechend greifen Standard-Sicherheitsmaßnahmen am Perimeter hier nicht. Vielmehr muss das Augenmerk auf verdächtiges Verhalten innerhalb der Systeme gerichtet werden. Die intelligente Analyse des Nutzerverhaltens (UBA) wird so zum Schlüssel, um Insider-Bedrohungen zu verhindern oder weitgehend abzuschwächen. Hierzu lernt die Software anhand von Protokoll- und Ereignishistorien (z.B. genutzte Programme, Dateizugriffe, Log-Ins), welches Verhalten für einen Mitarbeiter normal ist, um dann zu erkennen, wann es auffällig oder bedrohlich wird.

Trotz dieser hochentwickelten Lösungen ist die Aufdeckung einer Insider-Bedrohung schwieriger als die eines klassischen externen Angriffs. Mitarbeiter benötigen im Rahmen ihrer Tätigkeit den Zugriff auf wichtige und sensible Daten. UBA kann zwar abnormales Verhalten wie unübliche Zugriffsversuche erkennen, allerdings sollten Unternehmen diese ernste Bedrohung auf mehrschichtige Weise angehen. Dies kann beispielsweise die Erstellung und Kommunikation von Datenschutzrichtlinien für Mitarbeiter einbeziehen, aber auch Maßnahmen, um unzufriedene und verärgerte Mitarbeiter zu erkennen und entsprechende Schritte einzuleiten, um auf diese Weise zu verhindern, dass diese zu einer Bedrohung werden.

Gibt es eine „Täter-Persönlichkeit“?

Es gibt einige wissenschaftliche Studien darüber, warum Mitarbeiter zu Innentätern werden. Demnach gibt es drei Hauptkategorien: Datendiebstahl für finanziellen Gewinn, Datendiebstahl, um Geschäftsvorteile zu erlangen (IP-Diebstahl) und IT-Sabotage.

Diebstahl (und -manipulation) für Geld ist das

Klaus Nemelka, Technical Evangelist, Varonis Systems

offensichtlichste Motiv. Diese Art von Betrug wird eher von untergeordneten, nicht technik-affinen Mitarbeitern begangen, in der Regel in Zusammenarbeit mit Außenstehenden. Dabei handelt es sich um Mitarbeiter mit typischerweise finanziellen Problemen, die ihre Berechtigungen im Rahmen von Datenerfassungen oder als Kundenbetreuer nutzen, um Kredithistorien zu ändern, Leistungen anzupassen oder falsche Zugangsdaten zu erstellen – alles gegen eine „Gebühr". Der Diebstahl von Geld durch Mitarbeiter schafft es vielleicht nicht in die Nachrichten, aber die Forscher gehen davon aus, dass 5% der Unternehmen jedes Jahr durch Betrug mittels unberechtigtem Zugriff auf Computersysteme Geld verlieren.

Wenn wir von diesem Motiv absehen und ein wenig tiefer graben, entdecken wir eine andere Art von Innentätern. Diejenigen, die es auf IT-Sabotage oder den Diebstahl geistigen Eigentums abgesehen haben, sind meist technisch orientierte Mitarbeiter, die sich die Zugangsdaten anderer Mitarbeiter beschaffen können oder bereits über die entsprechenden Rechte verfügen – und damit Zugriff auf wertvolle Inhalte wie Code, sensible Dokumente, Verträge, Pläne u.ä. haben. Diese Mitarbeiter sind in der Lage, die Systeme von innen heraus zu korrumpieren, etwa indem sie Verzeichnisse löschen oder bösartigen Code in kritische Infrastrukturen einschleusen, und/oder große Mengen an vertraulichen Daten zu entwenden. Dies sind dann auch die Fälle, die enorme finanzielle Auswirkungen haben Schlagzeilen machen, etwa bei Googles Klage gegen Uber wegen des Diebstahls geistigen Eigentums.

Frühe Warnsignale

Warum begehen Mitarbeiter Cyberverbrechen? Gibt es neben den finanziellen Gründen auch andere? Die Wissenschaftler haben bei ihren Untersuchungen festgestellt, dass es in der Regel ein Auslöser-Ereignis gibt: eine Entlassung oder Streitigkeiten mit dem Arbeitgeber, Nichtberücksichtigung bei Beförderungen oder Unzufriedenheit mit einer Gehaltserhöhung. Mit anderen Worten, es gibt oft starke psychologische Elemente. Natürlich reagiert nicht jeder auf diese Trigger. Aber es gibt eine kleine Gruppe mit einer entsprechenden Neigung, die oftmals mit Suchtverhalten, Mobbing oder anderen persönlichen Problemen verbunden ist. Und für diese Menschen reichen dann solche Auslöser aus, eine Cyberstraftat zu begehen.

Als Mitarbeiter benötigen Insider keine besondere Software oder Tools, um Zugang zu erhalten, was ihre Entdeckung natürlich erschwert. Jedoch gibt es eine Eigenart von Insidern, die man gegen sie einsetzen kann: Sie zeigen in aller Regel Vorläuferaktivitäten, die normalerweise auch eine Art Probelauf ihrer geplanten Aktion umfassen: So durchsuchen sie Verzeichnisse, überprüfen Berechtigungen oder kopieren selektiv Code und andere sensible Inhalte. Bei Entwicklern und Administratoren, die auf Zerstörung aus sind, kann man beobachten, dass harmlose Code-Ausschnitte in bestehende Software eingefügt oder Konfigurationsdateien subtil geändert werden.

Diese Aktionen sind offenbar für die Mitarbeiter ein Test, durch den sie feststellen wollen, ob ihre Aktivitäten vom Unternehmen bemerkt werden und (interessanterweise) ob sich das Unternehmen für ihre Aktionen (also für sie) interessiert. Auf einer psychologischen Ebene mag dies für die Mitarbeiter dann das Okay sein, ihre Aktion auch tatsächlich durchzuführen.

Viele Unternehmen würden natürlich lieber ihren Mitarbeitern vertrauen, als sie zu überwachen, aber das macht sie angreifbar für genau diese Art von Taten. Es ist wichtig, potenzielle Insider wissen zu lassen, dass sie beobachtet werden, denn es kann sie vom Angriff abhalten. Und vorausschauende Unternehmen werden alle Mitarbeiter über ihre internen Datenschutzrichtlinien informieren.

Auffälliges Verhalten früh identifizieren

Fassen wir also nochmal zusammen: Ein Mitarbeiter mit einer besonderen Disposition erlebt ein auslösendes Ereignis bei der Arbeit: die Beförderung wurde abgelehnt, der Bonus ist niedriger als erwartet oder der Vorgesetzte drangsaliert ihn. Daraufhin beginnt er, die IT-Umgebung des Unternehmens unter die Lupe zu nehmen und führt erste Probeläufe seines Datendiebstahls oder seiner Sabotageaktion durch, um zu sehen, ob jemand etwas bemerkt. Schließlich begeht er seine Tat.

Software zur Analyse des Nutzerverhaltens spielt bei der Entdeckung dieser Probeläufe eine wichtige Rolle. Die UBA-Technologie sucht nach Nutzungsmustern, die auf ungewöhnliche oder abnormale Verhaltensweisen hinweisen. Da sich der Insider während der Vorbereitung auf den Angriff im Dateisystem umsieht, noch dazu oft in Bereichen, auf die er normalerweise nicht zugreift, wird das UBA dieses neue Muster bemerken und das IT-Sicherheitspersonal alarmieren. Hierbei ist zu bemerken, dass nicht jede UBA-Lösung in der Lage ist, auch Dateiaktivitäten zu erfassen und zu überwachen. Diejenigen, die dies können, haben entsprechend deutliche Vorteile bei der Erkennung der ersten verdächtigen Aktionen.

Um zu verlässlichen Ergebnissen zu kommen, muss UBA zunächst wissen, was als normales Verhalten dieses Nutzers gilt. Hierzu greift es auf die Historie der Aktivitäten zurück, also auf System- und Ereignisprotokolle, Dateizugriffe und Netzwerkaktivitäten. Dabei lernen die UBA-Algorithmen stets dazu und „verstehen" immer besser, welche Aktivitäten normal sind. Wenn sich ein Mitarbeiter nun von diesen Pfaden verabschiedet und sich mit seinen ersten Testläufen auf den Weg macht, ein Innentäter zu werden, registriert UBA diese verräterischen Aktionen und kann entsprechende Warnungen ausgeben.

UBA und andere Faktoren

Wie wir gesehen haben, macht es durchaus Sinn, die Informationen der UBA mit anderen Informationsquellen zu korrelieren, seien es Personalakten, Bewertungen oder ähnliches. Ein anormales Dateizugriffsmuster – jemand kopiert Dateien über das Wochenende – in Verbindung mit Informationen, dass sich der Mitarbeiter darüber beschwert hat, keine Beförderung erhalten zu haben, hat wesentlich mehr Aussagekraft als die bloße Identifizierung des abnormalen Verhaltens (vielleicht ist der Mitarbeiter nur mit einem Bericht spät dran?). Daher ist eine proaktive Datei- und Netzwerküberwachung und eine Alarmierung, wenn erste Anzeichen von Verhaltensproblemen auftreten, eine gute Möglichkeit, Insider-Bedrohungen auf die Schliche zu kommen.

Die Geschäftsführung sollte deutlich machen, dass sie Insiderbedrohungen ernst nimmt. Unternehmen sollten auch im Hinblick auf die Vermeidung von Insider-Vorfällen Weiterbildungsprogramme und Schulungen zum Thema Sicherheitsbewusstsein durchführen. Es gibt deutliche Hinweise darauf, dass potenzielle Insider ihre Pläne aufgeben, wenn sie wissen, dass ihre Aktivitäten im Rahmen spezieller Insider-Richtlinien überwacht werden. Wenn es also Anzeichen für ungewöhnliche Vorläuferaktivitäten eines Mitarbeiters zu geben scheint und eine zusätzliche Überwachung erforderlich ist, ist es vielleicht kein schlechter Zeitpunkt, eine E-Mail zu versenden, die die Mitarbeiter an die IP- und Sicherheitsrichtlinien des Unternehmens erinnert, einschließlich der Dateiüberwachung.

Anders ausgedrückt: Unternehmen sollten einen „Vertrauen, aber überprüfen"-Ansatz verfolgen. UBA kann so als Instrument zur Verhaltensänderung genutzt werden, um potenzielle Insider wieder zurück auf den „rechten Weg" zu bringen.

Worin liegt nun der Unterschied zwischen UBA und traditionellen ereignis-basierten Regeln (etwa aus SIEM- oder DLP-Systemen)? Können diese Insider-Datendiebstähle ebenso gut verhindern? Eher nicht, denn ein auffälliges protokolliertes Ereignis allein bietet eben nicht genügend Informationen und Kontext für eine entsprechende Regel, wodurch es zu zahlreichen „False Positives" kommen würde. UBA unterscheidet sich von anderen Methoden gerade dadurch, dass es aus (vergangenen) Mustern lernt und auf diese Weise in der Lage ist, schon die ersten Phasen etwa eines IP-Diebstahls zu identifizieren. Und das nahezu in Echtzeit, wodurch in aller Regel verhindert werden kann, dass Daten das Unternehmen jemals verlassen. Und sollte es dennoch zu einer erfolgreichen Datenexfiltration kommen, können die Auditprotokolle und andere Überwachungsergebnisse des UBA zur forensischen Aufklärung wesentlich beitragen und beweisen, dass Dateien tatsächlich gestolen wurden.

Klaus Nemelka

LinkedIn Betreffzeilen sind der neueste Trend bei Phishing-Angriffen

LinkedIn gilt als eines der größten webbasierten sozialen Netzwerke zur Pflege bestehender Geschäftskontakte. Das Business-Netz ermöglicht es seinen Nutzern, neue Geschäftsverbindungen aufzubauen unter Verwendung persönlicher Informationen, wie einem Lebenslauf mit Angaben zu beruflichen Stationen, der Ausbildung, besonderen Interessen und einem persönlichen Foto. Dadurch aber stellen Nutzer unabsichtlich eine Auswahl persönlicher und sensibler Informationen zur Verfügung, die Kriminelle zu ihrem Vorteil nutzen können. Um so schlimmer, da LinkedIn mit über 500 Millionen registrierten Nutzern in mehr als 200 Ländern zu den 50 meistaufgerufenen Websites gehört.

Kriminelle profitieren vom hohen Maß an Vertrauen, das mit der Online-Plattform verbunden ist, um böswillige Angriffe auf die Nutzer durchzuführen. Die Methode ist immer ähnlich: sie versenden gefälschte Nachrichten, die für die ahnungslosen Nutzer den echten LinkedIn Benachrichtigungen täuschend ähnlich ausschauen, da sie den offiziellen Namen und das Firmenlogo tragen. So gelangen neben den echten Nachrichten auch gefälschte mit der Betreffzeile ‚LinkedIn' in den Posteingang. Diese Angriffe sind auch deshalb so erfolgreich, da sie personalisiert auf das Ziel zugeschnitten sind und gestalterisch ebenfalls überzeugen. Sie enthalten in der Regel bösartige Links, die nach dem Anklicken auf gefälschte Webseiten führen, über die weitere private Daten des Opfers gestohlen werden können. Diese Phishing-Angriffe sind im Augenblick die beliebteste Angriffsmethode. Ein typischer Angriff sieht so aus.

Folgende Zeilen erreichen den LinkedIn User:

- Sie müssen Ihre LinkedIn-Profildatensätze aktualisieren, um Ihre Sicherheit bei der Nutzung des online-Dienstes zu gewährleisten. Klicken Sie Hier
- Die Nichteinhaltung kann sich auf Ihre Zukunft auswirken
- LinkedIn Online-Zugriff.
- Wir empfehlen Ihnen, die folgenden Maßnahmen zu ergreifen, um Ihr Konto zu schützen. LinkedIn Service
- Wenn dieser Prozess nicht innerhalb von 24-48 Stunden durchgeführt wird. Wir werden gezwungen, Ihren Konto Online-Zugang zu sperren, da es für betrügerische Zwecke verwendet werden kann
- @LinkedIn Datenschutzerklärung Für LinkedIn ™ 2019"

Im aktuellen Q2 Phishing Report von KnowBe4, dem Anbieter der größten Security Awareness Schulungs- und Phishing-Simulations-Plattform, wurde herausge-

funden, dass 56 Prozent der Betreffzeilen den Begriff ‚LinkedIn' enthielten – mehr als alle anderen Social Media Phishing-E-Mails zusammen. Dies lässt sich im Jahr 2019 mit einer bemerkenswerten Wachstumsrate von 75 Prozent bei Social Media-Phishing erklären. Dieser Anstieg, in Kombination mit Problemen der Schatten-IT, hindern die IT-Sicherheitsabteilungen daran, von Anwendern genutzte Social Media Apps auf Smartphones zu überwachen. „Menschen lieben es, sich auf diesen Plattformen mit Kollegen oder Geschäftspartnern zu verbinden, um Ideen und Informationen auszutauschen. Dadurch lassen sich neue Jobs oder ehemalige Kollegen finden und Karriereperspektiven verbessern. Dies verdeutlicht, warum Social Media Phishing-Angriffe im Zusammenhang mit vertrauenswürdigen und geschäftsorientierten Diensten wie LinkedIn so erfolgreich sind", erklärt Jelle Wieringa, Security Awareness Advocate bei KnowBe4. „Nutzer neigen dazu, ihren ‚verifizierten' Kontakten zu vertrauen, ohne darüber nachzudenken, wodurch die Chancen hoch sind, dass sie auf einen Link klicken, der angeblich von einem dieser vertrauenswürdigen Kontakte gesendet wurde."

Außer der Untersuchung von Phishing-E-Mails mit Social Media-Betreffzeilen, sind auch Phishing-Tests, die sich auf Passwortverwaltung konzentrierten, sehr erfolgreich. Immerhin 35 Prozent der Benutzer klickten die Links in den Test-E-Mails an. Darüber hinaus hatten ‚In-the-Wild-Angriffe' – also echte Phishing-E-Mails statt simulierten – den größten Erfolg, wenn sie den Empfänger um konkrete Maßnahmen baten, wie die Freigabe eines Outlook-Kalenders oder die Zuweisung einer Aufgabe auf einer Microsoft-Plattform.

Die von KnowBe4 identifizierten Social Media Phishing-Tests mit den höchsten Öffnungsraten sind:

- LinkedIn: 56%
- Anmeldealarm für Chrome auf Motorola Moto X: 9%
- 55. Jahrestag und Pizza-Party: 8%
- Dein Freund hat ein Foto von dir markiert: 8%
- Facebook Passwort-Rückstellungs-Verifizierung: 8%
- Dein Passwort wurde erfolgreich zurückgesetzt: 6%
- Neue Sprachnachricht um 1:23 Uhr: 5%

Die Angriffe auf Social-Media-Accounts sind im vergangenen Jahr um 43 Prozent gestiegen, wobei Social-Media-Phishing-Angriffe sogar um 75 Prozent zugenommen haben. Es ist offensichtlich, dass Unternehmen dies ernst nehmen und einen Abwehrmechanismus gegen diese Angriffe installieren müssen. Neben der Standard-Firewall, sind Mitarbeiter die letzte Verteidigungslinie eines Unternehmens und sie sind dann am erfolgreichsten, wenn sie kontinuierlich geschult und auf die neuesten Phishing-Bedrohungen vorbereitet werden. Sie bilden eine sogenannte ‚Human Firewall', die das Sicherheitssystem des Unternehmens weiter unterstützt.

Beispielsweise sollten die Angestellten wissen, wie sie Social Engineering und Phishing erkennen können, was sie tun müssen, falls sie darauf stoßen, und welche Gegenmaßnahmen einzuleiten sind. Unternehmen sollten überlegen, wie sie Mitarbeiter bezüglich dieser Bedrohungen und Risiken kontinuierlich sensibilisieren können. Es gibt spezielle Antiphishing-Programme, die Unternehmen zur Beseitigung dieser Sicherheitsrisiken und Bedrohungen nutzen können, wie simulierte Phishing-Emails, PhishER, PhishML usw. Bei PhishML handelt es sich um ein Modul innerhalb der PhishER-Plattform von KnowBe4. Es setzt maschinelle Lernverfahren und Algorithmen ein, vereinfacht, beschleunigt und erhöht zugleich die Präzision bei der Priorisierung verdächtiger Nachrichten. Darüber hinaus ist der neue Social Media Phishing Test (SPT) ein kostenloses IT-Sicherheits-Tool, mit dem Unternehmen feststellen können, welche Benutzer in ihrer Umgebung anfällig für diese Art von Phishing-Angriffen sind. SPT gibt Firmen einen schnellen Überblick, wie viele Benutzer zum Opfer werden könnten, damit sie Maßnahmen ergreifen können, um die Mitarbeiter zu schulen und das Unternehmen besser vor Social Media Phishing-Angriffen zu schützen.

Fazit

Viele Nutzer sind auf Social Media-Plattformen (Facebook, LinkedIn und Twitter) aktiv. Kriminelle nutzen diese wiederrum, um Profilinformationen der Benutzer und der Unternehmen zu sammeln, damit jene gezielte Speer-Phishing-Kampagnen erstellen können, um Konten zu übernehmen, den Ruf des Unternehmens zu schädigen oder Zugang zu dessen Netzwerk zu erhalten. Deshalb ist bei E-Mails von LinkedIn besonders große Vorsicht angebracht.

Jelle Wieringa

20 Jahre „I love you"-Virus: Wo stehen wir in Sachen Cybersicherheit heute?

„Ich habe verstanden, dass viele Leute einen Freund wollen, sie wollen einander, sie wollen Liebe", sagte Onel de Guzman dem investigativen Journalisten Geoff White vor kurzem. Bei IT-Sicherheitsexperten schrillen noch heute die inneren Alarmglocken, wenn sie den Namen des ehemaligen Informatikstudenten aus Manila hören. Nicht etwa, weil er mit seiner Aussage danebenliegt. Im Gegenteil.

Vor etwas mehr als 20 Jahren, am 4. Mai 2000, löste er eine wahre Virus-Pandemie aus. Digital. Mit dem „I love you"-Virus verursachte der damals 23-Jährige weltweit einen Schaden von geschätzt rund 10 Milliarden Dollar. Und zwar so: Seine Opfer öffneten einen vermeintlichen Liebesbrief, der einer E-Mail anhing. Beim Öffnen lud sich eine Schadsoftware auf den Computer und versendete sich selbst an weitere Kontakte des Opfers weiter. Was hat sich seitdem in 20 Jahren IT-Sicherheit getan und wie schützen vor allem Unternehmen heute effektiv ihre Netze? Und: Wäre de Guzmans Vorgehen heute, 20 Jahre später, noch möglich?

Viele Angriffe kommen über E-Mails

Die unzufriedene Antwort ist: Jein. Noch immer wird bei Cyberattacken auf den „menschlichen Faktor" gesetzt, wie Hacker ihn gerne selbst nennen. Viele Angriffe kommen weiterhin per E-Mail rein. Das sogenannte Phishing kennen wir alle. Es wird versucht, eine seriöse Seite, das kann etwa Google Mail, Paypal oder das eigene Bankinstitut sein, so gut wie möglich zu imitieren und Login-Daten des Users abzugreifen. Dank modernen Spamfiltern hat diese Methode zwar nur eine geringe Chance; wenn sie jedoch funktioniert, bedeutet sie für den Einzelnen oder das betroffene Unternehmen einen immensen Schaden. Ähnlich funktioniert es bei Schadsoftware. Ein berühmtes Beispiel für sogenannte Ramsomware ist der Verschlüsselungstrojaner Locky. Auch heute gibt es ähnliche Angriffsversuche, wobei die reine Erpressung durch Verschlüsselung mehr in Richtung Erpressung mit Veröffentlichung erbeuteter Daten geht.

Mit Machine Learning gegen neue Angriffsmuster

Ganz so einfach wie vor 20 Jahren ist ein Angriff auf die IT-Sicherheit dann aber doch nicht mehr. Denn die Gesellschaft ist digitaler geworden. Und das ist kein Widerspruch. Denn die Digitalisierung bietet nicht nur mehr Angriffsfläche für Hacker, wie man im ersten Moment glauben mag. Die digitale Gesellschaft ist auch aufgeschlossener. Sie weiß, dass sie nicht auf jeden Button in einer Mail drücken soll und Passwörter regelmäßig ändern muss. Auch der technische Schutz gegen Cyberangriffe hat enorme Fortschritte gemacht. Vor allem Unternehmen haben ihre IT massiv aufgerüstet – die weltweiten Ausgaben für Sicherheits-Hardware, -Software und -Services hat sich innerhalb von 20 Jahren auf mehr als 100 Milliarden US-Dollar fast verhundertfacht! Antivirus, Antispam, leistungsfähige Firewalls: Sie gehören heute selbst bei Kleinunternehmen zur IT-Grundausstattung.

Das zeigt sich auch im Anbietermarkt deutlich: Gab es früher die traditionellen Netzwerkanbieter, die sich auf Router, Switches und WLAN Access Points spezialisiert haben, gehören heute auch zunehmend Lösungen für mehr Cybersecurity – konkret Next-Generation Firewalls und ihr „Unified Threat Management" – zu deren Digitalisierungsangebot. Sie nutzen modernste Cybersecurity-Technologien wie Sandboxing und Machine Learning, um immer neue Angriffe abzuwehren. Ihr bewusst sehr grafisches User Interface wiederum trägt dazu bei, dass die richtige Konfiguration leichtfällt und weniger Fehler passieren. So haben es Spam, Viren und Malware sowie komplexen Cyberangriffen enorm schwer, ähnlichen Schaden wie der „I love you"-Virus vor 20 Jahren anzurichten.

Ein endloses Katz-und-Maus-Spiel

Dahinter steckt ein kontinuierlicher Entwicklungsprozess, in dem Tempo eine entscheidende Rolle spielt. Vereinfacht lässt sich das Verhältnis zwischen IT-Sicherheitsanbietern und Hackern als ewiges Katz-und-Maus-Spiel bezeichnen. Sobald eine Attacke erfolgreich abgewehrt und eine eventuelle Sicherheitslücke geschlossen wurde, wird schon der nächste digitale Angriff konzipiert.

Gegen die überall lauernde, sich ständig ändernde Gefahr hat sich ein Trend entwickelt: das „Zero-Trust-Modell". Hier gilt der Grundsatz, keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks zu vertrauen. Praktisch bedeutet das: Netzwerke werden stark segmentiert, etwa durch VLANs, um den Datenverkehr einfacher zu kontrollieren. Werden Unstimmigkeiten erkannt, können die Netzwerk-Parts schneller vom restlichen Betrieb abgekoppelt werden. Die Virus-Verbreitung wird gestoppt.

Der Faktor Mensch ist (mit)entscheidend

Ganz egal, welchen Weg die Technik beschreitet, eines bleibt im Vergleich zu vor 20 Jahren gleich: Technische Sicherheit ist nur so gut, wie der Mensch, der mit ihr arbeitet – ob analog oder digital. Deswegen reicht es als Unternehmen nicht aus, nur auf die neueste, modernste IT-Sicherheitstechnik zu setzen.

Sicher, die richtige Technik hilft, viele Dinge früh zu erkennen und die Flut an Phishing-Attacken, kompromittierenden E-Mails und Schadsoftware einzudämmen. Aber auch die Mitarbeiter müssen geschult und vor den Gefahren im Internet gewarnt werden. „Awareness" heißt das Zauberwort.

Das gilt umso mehr für gezielte, maßgeschneiderte Angriffe auf ganz bestimmte Unternehmen, die immer häufiger an die Stelle undifferenzierter Massenangriffe treten: die sogenannten Advanced Persistent Threats. Eine in diesem Kontext sehr beliebte Hacker-Methode – für die in der Szene sogar Wettbewerbe abgehalten werden – ist das Social Engineering. Es ist die Kunst, Menschen so zu manipulieren, dass sie schützenswerte Informationen preisgeben und so unwissentlich den Weg in die Unternehmensnetze öffnen.

Spätestens da sollten bei allen die Alarmglocken schrillen. So wie die der IT-Sicherheitsexperten beim Namen eines ehemaligen Studenten aus Manila.

Ralf Koenzen

Ralf Koenzen, Gründer und Geschäftsführer, LANCOM Systems

Warten bis zur nächsten Sicherheitslücke? Besser Fehler in der Richtlinien-Konfiguration beheben

Die Optimierung der Richtlinien-Konfiguration für Firewalls und andere Sicherheitseinrichtungen ist vielleicht nicht die spannendste Aufgabe, aber eine sehr wichtige, um Unternehmen zu schützen. Im Folgenden dreht sich alles um vier häufig auftretende Fehler im Zusammenhang mit Sicherheitsrichtlinien und wie Unternehmen diese vermeiden können.

Da Schadprogramme immer fortschrittlicher werden, ist die korrekte Verwaltung des Netzwerkschutzes wichtiger als je zuvor. Die Wirksamkeit von Firewalls und anderen Sicherheitseinrichtungen hängt von den Sicherheitsrichtlinien ab, die ihre Funktionen steuern. Diese Richtlinien, die zehntausend, oder sogar hunderttausend Firewall-Regeln kompromittieren können, geben vor: welcher Datenverkehr blockiert, welcher zugelassen wird und wohin er fließen darf. Dies dient der Sicherheit und Einhaltung von Vorschriften, um die Produktivität der Firma zu steigern.

Jedoch wird es schwieriger, diese Richtlinien einzuhalten, um die Anforderungen des Geschäftsbereiches optimal mit der Notwendigkeit der Risikobegrenzung und der Gewährleistung von größtmöglichem EDV-Schutz in Einklang zu bringen. In den meisten Unternehmen werden Geschäftsanwendungen rasch eingeführt oder geändert, um mehr Benutzer oder neue Funktionen einzubinden.

Organisationen verlagern ihre Daten außerdem in virtuelle und Cloud-Infrastrukturen. Dies bringt neue Sicherheitskontrollen und Verbindungslinien mit sich, die verwaltet werden müssen, damit Geschäftsanwendungen jederzeit unterbrechungsfrei funktionieren. Es ist daher nicht verwunderlich, dass die Analysten von Gartner schätzen, 99 Prozent der Firewall-Verstöße seien auf einfache Fehlkonfigurationen der Richtlinien zurückzuführen.

Robert Blank, Regional Sales Manager DACH, AlgoSec

Welche sind also die gängigsten und schädlichsten Fehlkonfigurationen, die sich in Firewall-Regelsätze und Sicherheitsrichtlinien einschleichen können? Im Folgenden wird dargestellt, welche die häufigsten Probleme sind und wie sie vermieden werden können.

Undefinierte Richtlinien-Konfigurationen erfassen

Allzu häufig werden Firewalls über undefinierte Richtlinien konfiguriert, um Datenverkehr von jeder Quelle zu jedem Ziel zuzulassen. Dies geschieht, weil IT-Teams zum Zeitpunkt der Anwendungsbereitstellung ihre genauen Anforderungen nicht kannten und sich deshalb entschlossen, mit weit gefassten Regeln zu beginnen, die später nach Bedarf angepasst werden können.

Theoretisch ist dies in Ordnung, aber in der Praxis finden diese Aktualisierungen kaum statt, denn die Anwendung arbeitet schließlich so, wie sie sollte. Unternehmen sind also leicht versucht, alles beim Alten zu lassen und sich auf die dringenderen Probleme zu konzentrieren. Mit undefinierten Firewall-Richtlinien ist das Netzwerk jedoch ständig gefährdet.

Um diese Gefahr zu beseitigen, sollten Unternehmen ihr Vorgehen umdrehen. Als Standard für Firewall-Richtlinien muss das Prinzip der geringsten Privilegien gelten, um diese dann nach Bedarf anzupassen. Idealerweise sollten Unternehmen die Abläufe abbilden, die für ihre Anwendungen tatsächlich erforderlich sind, bevor sie irgendeinen Zugriff gewähren.

Durch Bereitstellung der minimalen Privilegien, die ein Nutzer oder ein Dienst für ein normales Funktionieren benötigt, wird der potentielle Schaden begrenzt, der durch einen Verstoß verursacht werden kann. Auch nach der Implementierung sollten die Firewall-Richtlinien regelmäßig überprüft und aktualisiert werden, um den Trends der Anwendungsnutzung und der erforderlichen Konnektivität gerecht zu werden.

Fehler in der Übersetzung

Die meisten Unternehmen verfügen mittlerweile über gemischte Sicherheitsinfrastrukturen, die sowohl herkömmliche als auch Firewalls der nächsten Generation von unterschiedlichsten Herstellern beinhalten. Die Verwaltung einer solchen Mischung ist eine Herausforderung, da die einzelnen Firewall-Generationen und die Produkte der einzelnen Anbieter unterschiedliche Syntax und Semantik für die Erstellung von Sicherheitsrichtlinien verwenden.

Aus diesem Grund treten häufig Fehler auf, wenn Sicherheitsabteilungen versuchen, ihre vorhandenen Richtlinien auf neue Geräte zu verschieben. Dies kann sogar zu Anwendungsausfällen führen. Jeder Irrtum oder ‚Übersetzungsfehler' beim Schreiben dieser Richtlinien, wie auch beim Vornehmen von Netzwerkänderungen, kann dazu führen, dass wichtiger Datenverkehr blockiert oder unerwünschter Datenverkehr zugelassen wird. Keiner dieser Zustände ist akzeptabel.

Um diese Fehler zu beheben und gleichzeitig die Sicherheit auf allen Geräten effektiv zu optimieren sowie zu verwalten, sollten Unternehmen eine Lösung mit einer einzigen Verwaltungskonsole und einem einzigen Befehlssatz bereitstellen. Die Konsole sollte, unabhängig vom Hersteller, zentrale Sichtbarkeit und Kontrolle jeder Sicherheitseinrichtung bieten. Auf diese Weise können IT-Gruppen verschiedene Syntaxen in Ausdrücke übersetzen, die von den einzelnen Sicherheitskontrolltypen – On Premises oder in der Cloud – genutzt werden, um Regeln und Richtlinien zu erstellen. Damit sprechen die Sicherheitseinrichtung und das Unternehmen eine gemeinsame Sprache.

Schwache Optimierung verbessern

Die meisten Firewalls wenden Regeln in der Reihenfolge an, in der sie in der Firewall-Konfigurations-Software oder im Regelwerk aufgeführt sind. Die Firewall beginnt am Listenanfang und durchläuft Zeile für Zeile, bis sie die Regel erreicht, nach der betreffender Datenverkehr blockiert werden muss. Wenn keine Regeln zutreffen, darf der Verkehr passieren.

Dieser Ansatz ist zwar unkompliziert, optimiert jedoch nicht die Leistung des Geräts oder der Anwendung, die sich auf die Regelbasis der Firewall stützt. Dieselben Regeln in einer effizienteren Reihenfolge können die Leistung der Firewall und der darauf basierenden Anwendungen drastisch verbessern. Die Gesamtleistung wird beschleunigt, wenn Regeln, die häufiger aufgerufen werden, an einer höheren Stelle der Reihenfolge platziert werden als Regeln, die seltener gebraucht werden.

Deshalb ist es wichtig, dass Unternehmen für die optimale Gestaltung und Implementierung neuer Regeln sorgen, während vorhandene Regeln konsolidiert und neu geordnet werden, damit eine bestmögliche Leistung erzielt werden kann. Unternehmen sollten auch versuchen, die Netzwerksicherheit direkt mit kritischen Geschäftsanwendungen und -prozessen in Verbindung zu bringen, um risikobasierte und inhaltsbezogene Informationen zu liefern. Auf diese Weise können Unternehmen die Gegenmaßnahmen strategisch ordnen und auf kritische Prozesse konzentrieren, die das tägliche Geschäft fördern.

Unnötige Dienste beenden

Ein weiterer, häufiger Fehler der Firewall-Konfiguration besteht in der Ausführung veralteter Dienste. Zwei Beispiele sind das dynamische Routing, das auf Sicherheitseinrichtungen nicht aktiviert werden sollte, und DHCP-Server, die IPs verteilen und dadurch IP-Konflikte erzeugen, was zu Störungen der Verfügbarkeit führt.

Um diese Probleme zu vermeiden, sollten Unternehmen alle Geräte schützen und sicherstellen, dass die Konfigurationen vor der Bereitstellung der Geräte sorgsam geplant wurden, sowie danach kontinuierlich kompatibel sind. Diese Maßnahmen tragen dazu bei, dass Geräte reibungslos die Funktionen erfüllen, die sie erfüllen sollen. Die Sicherheit der gesamten Unternehmensstruktur wird ebenfalls erhöht, jedoch die Wahrscheinlichkeit verringert, dass auf der Firewall versehentlich ein riskanter Dienst ausgeführt wird.

Vor dem Hintergrund einer sich schnell entwickelnden Bedrohungslandschaft können es sich Unternehmen nicht mehr leisten, nachlässig zu sein. Sie machen sich selbst zu ihren schlimmsten Feinden, weil sie fehlerhafte Konfigurationen und Richtlinienfehler dulden oder sogar sehenden Auges einführen, die wiederrum zu Sicherheitslücken werden können. Eine Lösung, die zur effektiven Verwaltung der Sicherheitsrichtlinien, die Firewall-Regeln auf intelligente Weise automatisiert, verbessert schnell die gesamte Sicherheitslage eines Unternehmens – und verringert zugleich die Wahrscheinlichkeit einer gefährlichen Sicherheitslücke enorm.

Robert Blank

Wer den Schaden hat, braucht für den Spott nicht zu sorgen – Warum sich Unternehmen mit dem Schutz mobiler Geräte schwertun und was sie dringend ändern müssen

Sie gehören längst zur Tagesordnung - die erschreckenden Nachrichten über gehackte Behörden, ausspionierte Unternehmen und lahmgelegte Organisationen. Der mit einem Cyberangriff einhergehende Imageschaden ist beträchtlich. Dennoch reißt die Liste derer, die von einer solchen Attacke betroffen sind nicht ab. Das liegt nicht zuletzt daran, dass die Verantwortlichen in den Unternehmen das Thema Mobile Security weitestgehend ignorieren.

Bedenkt man, dass laut Gartner 80 % aller Arbeitsaufgaben bis Ende 2020 über Mobilgeräte erledigt werden[1], ist zu befürchten, dass diese Fehleinschätzung der Wichtigkeit fatale Folgen haben wird. Nach wie vor sind die mobilen Geräte ein immer größer werdendes Einfalltor für Cyberkriminelle. Langfristig kann Missachtung von Cyber-Security-Anforderungen deshalb nicht nur zum Verlust von Vertrauen, Umsatz und Know-How führen, sondern ganz leicht auch zu einem Schwund des Technologie-Vorsprungs.

Selbst wissenschaftliche Institute oder fortschrittliche Universitäten sind vor keinem Angriff gefeit. Erst im Mai erwischte es die Ruhr-Universität Bochum[2]. Während des Corona-Lockdowns wurde das IT-System der Hochschule durch einen Angriff von außen lahmgelegt. Sofort wurde das System ausgeschaltet und erst nach Tagen und entsprechenden Vorsichtsmaßnahmen sukzessiv wieder hochgefahren.

Es muss aber nicht immer so glimpflich ablaufen. Datenschützer warnen, dass Hacker die Verunsicherung durch die Corona-Pandemie gnadenlos ausnutzen[3]. Gezielte Angriffe oder böswillige Apps nutzen gerade in Krisenzeiten das Bedürfnis nach Information und durch die inzwischen kommerzielle Verfügbarkeit von Spyware-Kits, wird es Cyberkriminellen immer einfacher gemacht, zuzuschlagen.

Michael Krause, Geschäftsführer, TAP.DE Solutions GmbH

Es muss dringend was getan werden

Aber unabhängig von diesen Beispielen unterliegen Unternehmen oft dem Trugschluss, dass ihr Mobile Device Management automatisch auch für einen ausreichenden Schutz sorgt. Dass dem nicht so ist, wissen zwar die verantwortlichen IT-Spezialisten, aber ihre Vorgesetzten sehen hier keinen dringenden Handlungsbedarf. Obwohl man in Fachkreisen Angriffsmethoden wie Phishing, Tailgating, Whaling etc. kennt, schützen Unternehmen ihre Anwender nur unzureichend vor diesen perfiden Tricks. Nun stellt sich die Frage, wieso das so ist, wenn doch regelmäßig von Hackerangriffen berichtet wird?

Vielfach liegt es daran, dass sich die übergeordneten Instanzen nicht ausreichend mit dem Thema auseinan-

dersetzen und gutgläubig Meinungen übernehmen, ohne diese kritisch zu hinterfragen, geschweige denn, Quellen zu vergleichen. Häufig wird der Mythos verbreitet, dass Smartphones vor bösartigen Apps geschützt sind, solange der Benutzer die Software ausschließlich aus dem App oder Google Store bezogen hat. Des Weiteren wird im Hinblick auf Apple-Geräte davon gesprochen, dass diese nie bis kaum Bedrohungen ausgesetzt sind. Doch auch hier gibt es Schwachstellen, die gerne ausgenutzt werden, wie das Apple-Problem im April gezeigt hat, als es Angreifern möglich war, mithilfe einer versendeten E-Mail das Gerät zu manipulieren (bei iOS 13 sogar ohne, dass die E-Mail dafür geöffnet werden musste).[4]

Ein Geschäftsführer oder Sicherheitsexperte kann nicht jede Bedrohung auf dem Markt kennen. Jedoch müssen sie dafür Sorge tragen, dass Sicherheitslösungen diese Aufgabe für sie übernehmen und das Unternehmen vor Bedrohungen schützt.

Helfen kann hier sehr einfach der Einsatz einer Mobile Threat Prevention Lösung (MTP). Eine solche Lösung ist schnell und unkompliziert als Cloud- Dienst aktivierbar und sorgt dafür, dass einerseits die Daten und andererseits das Gerät sofort abgesichert sind. Das Ganze geschieht ohne, dass personenbezogene Daten in die Cloud übertragen werden. Es sind somit keine datenschutzrelevanten Probleme zu erwarten. Lediglich Metadaten werden von der Lösung verarbeitet.

Voraussetzung ist, dass die IT-Verantwortlichen die fatalen Folgen mangelnder Schutzmechanismen[5] aufzeigen. Die DSGVO und auch die hohen IT-Sicherheits-Anforderungen für die Betreiber kritischer Infrastrukturen (KRITIS) schaffen die Grundlage, diese dringend notwendigen Security Maßnahmen beim Management zu platzieren und „durchzusetzen".

Das abschreckende Beispiel eines Hardwareherstellers zeigt, welche Folgen mangelnde Datensicherheit haben kann. Gelingt es Kriminellen die IT eines Hardwareherstellers, der von 1-2 Prozent Marge lebt, zu kapern, kann dies für dessen Business tödlich sein. Denn sollten bei diesem Angriff personenbezogene Daten betroffen sein, darf laut DSGVO eine Strafe von bis zu 4 Prozent[6] des Jahresumsatzes veranschlagt werden – eine Summe, die das Unternehmen möglicherweise in die Insolvenz treibt. Vom Imageverlust ganz zu schweigen!

So hilft Mobile Threat Prevention (MTP)

Präventionsmaßnahmen sind unerlässlich. Moderne MTP-Lösungen können Unternehmen zuverlässig vor Sicherheitsbedrohungen schützen. Es muss jedoch festgelegt werden, welche Bereiche besonders schützenswert sind. Um mobile Geräte vollumfänglich zu sichern, sollten deshalb drei folgenden Angriffspunkte unbedingt in einer Mobile Device Security Strategie berücksichtigt werden.

Device

Der erste Gedanke, der einem Mobile Security in den Sinn kommt, ist natürlich die Absicherung des Gerätes selbst. Hierbei wird zum einen die Einhaltung vordefinierter Geräte-Konfigurationen betrachtet, wie beispielsweise die Verteilung einer einheitlichen Version des mobilen Betriebssystems. Zum anderen aber auch der Schutz oder die Warnung vor Jailbreak oder Root Attacken sowie OS Exploits und Schwachstellen.

Apps

Nicht nur das Gerät kann Einfallstor für Hacker sein, sondern auch Apps, die aus dem Google- oder App-Store bezogen wurden. Eine gute MTP Lösung schützt vor bösartigen Apps und blockt diese automatisch bei einem Downloadversuch. Auch bereits installierte Apps können von der Software auf bösartige Inhalte gescannt und blockiert werden. Das Unternehmen erhält einen ausführlichen Bericht über „gefährdete" Devices und kann unverzüglich Maßnahmen treffen.

Netzwerk

Häufig wird dem Bereich Netzwerk eine zu geringe Aufmerksamkeit in Bezug auf Sicherheit geschenkt, obwohl genau hier ein enormes Potenzial für Cyberkriminelle steckt. Nicht nur Phishing Mails oder SMS werden in der heutigen Zeit verbreitet, sondern auch kompromittierte WiFi Verbindungen. Hierunter verbergen sich scheinbar harmlose WiFi Hotspots in bekannten Umgebungen wie beispielsweise im eigenen Lieblingscafé. Auch bösartige URLs werden immer ausgeklügelter und lassen sogar Sicherheitsexperten in die Falle tappen.

Das Prinzip Hoffnung funktioniert nicht mehr

Um derartige Horrorszenarien zu vermeiden, ist eine Bewusstseinsänderung überfällig. Unternehmen müssen die im Einsatz befindlichen Technologien bzw. Strategien und ihre Wirkungskraft unter Berücksichtigung der aktuellen Bedrohungslage analysieren und schnellstmöglich erweitern. Mitarbeiter müssen mit Hilfe von Schulungen und Security Awareness Trainings über Bedrohungen aufgeklärt und entsprechend sensibilisiert werden. Sicherheitsexperten gehen sogar so weit und empfehlen Social Hacking Angriffe zu simulieren, um herauszufinden, wie Mitarbeiter in solchen Fällen reagieren.

Oft versteckt sich hinter einer SMS mit einer Gewinnbenachrichtigung oder einem kostenlosen WLAN-Hotspot ein ausgeklügelter Cyberangriff. Auf solche und ähnliche Gefahren müssen Benutzer aufmerksam gemacht werden, um diese als Gefahr zu erkennen und entsprechend zu reagieren.

Das Prinzip Hoffnung sollte längst ausgedient haben. Anwender müssen endlich vor Cyberkriminellen mit längst vorhandenen und bewährten Technologien geschützt werden!

Michael Krause

Referenzen: **[1]** Gartner, „Prepare for Unified Endpoint Management to Displace MDM and CMT", Juni 2018 **[2]** WDR-Nachrichten **[3]** Datensicherheit.de: Hacker nutzen Covid19-Krise **[4]** https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Warnung_iOS-Mail_230420.html **[5]** Check Point Video „Better safe than sorry" **[6]** DSGVO

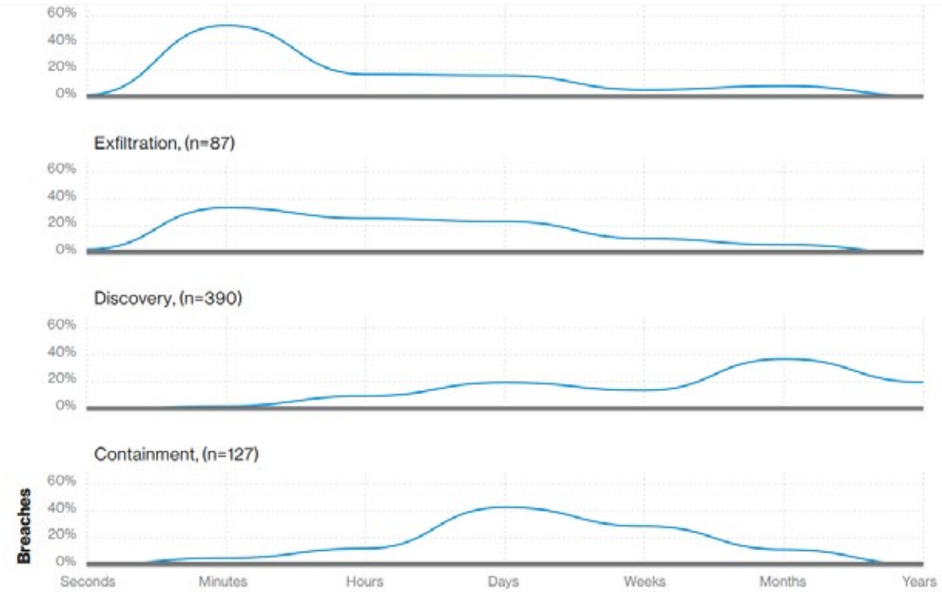


Abbildung 1: Zeitverläufe bei Datensicherheitsverletzungen, Verizon Data Breach Investigations Report 2019

Die wichtigsten Ursachen von Sicherheitsrisiken

Jedes Jahr um diese Zeit informiert Verizon in seinem Data Breach Investigations Report (DBIR) über die neuesten Trends in der globalen Bedrohungslandschaft. Die Ergebnisse des diesjährigen Berichts basieren auf Daten, die mehr als 70 Quellen (darunter Qualys) zu über 41.000 Sicherheitsvorfällen bereitgestellt haben, einschließlich mehr als 2.000 bestätigter Datensicherheitsverletzungen. Die Vorfälle verteilen sich auf eine Vielzahl von Regionen (mehr als 80 Länder) und Branchen.

Der 78-seitige Bericht spricht ein breites Spektrum von Themen an. Im Folgenden fokussiert sich dieser Beitrag auf drei wichtige Fragestellungen:

- Wer sind die bevorzugten Ziele von Hackern und weshalb?
- Warum ist es so wichtig, schneller zu werden – sowohl bei der Erkennung von Sicherheitsproblemen wie Schwachstellen oder Kompromittierungen als auch bei der Behebung der Probleme?
- Wie erhöhen mangelnde Übersicht, menschliche Fehler und durch Nachlässigkeit verursachte Fehlkonfigurationen die Sicherheitsrisiken von Unternehmen?

Wer sind die Opfer?

Fast die Hälfte der Datensicherheitsverletzungen betraf kleine Unternehmen. Dafür kann es mehrere Erklärungen geben. Kleine Unternehmen haben in der Regel eine schwächere Sicherheitsabwehr, weil sie über weniger Ressourcen und technisches Know-how verfügen. Sie sind aber auch deshalb ein attraktives Ziel, weil sie als Teil von Lieferketten Hackern den Weg in die Netzwerke größerer Unternehmen erleichtern können.

Was die verschiedenen Branchen betrifft, wurden Sektoren wie staatliche Einrichtungen, das Gesundheitswesen und der Finanzsektor hart getroffen. Das zeigt deutlich, dass sensible, vertrauliche Daten, die die Akteure in diesen Branchen besitzen, einen hohen Wert für die Angreifer haben, die diese dann wiederum verkaufen oder für umfangreichere Angriffe nutzen.

Zeit bis zur Erkennung, Zeit bis zum Patch

Besorgniserregend ist die Feststellung, dass mehr als die Hälfte der Sicherheitsverletzungen erst nach Monaten aufgedeckt wurden. Dies lässt darauf schließen, dass es den IT- und Sicherheitsteams nach wie vor schwerfällt, einen vollständigen Überblick über IT-Umgebungen zu gewinnen, die digitalisiert werden und somit hybride und immer stärker verteilt sind. Was nicht gesehen wird, kann nicht überwacht, bewertet, verteidigt oder geschützt werden.

Dieses Diagramm(Abbildung 1) verdeutlicht noch einmal die Zeitverläufe bei Datensicherheits-verletzungen.

Es wird deutlich, dass Kompromittierungen und Datendiebstähle eine Sache von Minuten sein können, während bis zur Entdeckung manchmal Tage vergehen, oft aber auch Wochen, Monate oder gar Jahre. Und wenn die Sicherheitsverletzungen dann bemerkt wurden, kostet es Zeit, Mühe und Ressourcen, sie nach so langer Zeit einzudämmen.

Marco Rottigni, CTSO, Qualys

Was die Schwachstellen betrifft, werden 50 Prozent innerhalb von 90 Tagen nach ihrer Entdeckung beseitigt und 25 Prozent innerhalb von 30 Tagen. Das mag vielen effizient erscheinen, doch hier ist noch eine Menge Luft nach oben. Besonders, wenn die Schwachstellenbeseitigung eng mit den Maßnahmen zur Erkennung integriert wird.

Die Zeiten sind vorbei, in denen isolierte, punktuelle Lösungen eingesetzt werden, um einzelne IT-, Sicherheits- und Compliance-Probleme zu beheben. Heterogene Produkte, die nicht interoperabel sind, führen zu Verzögerungen und Lücken. Das gilt insbesondere für die Verhinderung von Sicherheitsverletzungen, für die ein integriertes Programm benötigt wird, das Asset-Inventarisierung, Schwachstellenmanagement, Priorisierung von Bedrohungen und Patchmanagement umfasst.

Bevorzugte Taktiken

Bei 52 Prozent der Sicherheitsverletzungen wurde eine beliebige Form von Angriffen eingesetzt, während Malware-Infektionen 28 Prozent und Missbräuche durch autorisierte Benutzer 15 Prozent ausgemacht haben. Abgesehen vom Mangel an Sichtbarkeit unterstreichen diese Zahlen auch die Notwendigkeit, die Compliance zu stärken und Fehlkonfigurationen in digitalisierten, hybriden IT-Umgebungen zu reduzieren, die Elemente wie etwa Cloud-Instanzen, Container, herkömmliche Rechenzentren, Remote-Mitarbeiter und mobile Geräte umfassen.

Laut Verizon ist die häufigste interne Bedrohung nicht vorsätzliche Sabotage, sondern ein Mitarbeiterfehler, der ohne böse Absicht geschieht. Laut dem Bericht werden dabei „entweder Server falsch konfiguriert, was unerwünschten Zugriff ermöglicht, oder Daten auf einem Server öffentlich gemacht, zu denen nicht alle Benutzer hätten Zugang haben dürfen."

Die Dominanz externer Bedrohungen, die 69 Prozent der Sicherheitsverletzungen ausmachen ist ein weiterer besorgniserregender Trend – wobei Ransomware zu den am weitest verbreiteten Bedrohungen dieser Art zählt (bei 24 Prozent der Vorfälle eingesetzt). Dies unterstreicht die Wichtigkeit eines leistungsstarken Programms für Schwachstellen- und Fehlerbehebungsmanagement, damit die Angriffsfläche verringert wird. Um Sicherheit und Reaktionsgeschwindigkeit zu erhöhen, ist es sinnvoll einen Schwerpunkt auf folgende Aspekte zu legen:

- Priorisierung der Abhilfemaßnahmen, damit die kritischsten Bedrohungen für das eigene Unternehmen sofort erkannt und behoben werden können
- abteilungsübergreifend verteilte, dynamische Dashboards, um das Situationsbewusstsein zu stärken
- und transparente Automatisierung über alle Plattformen des IT- und Sicherheitsbetriebs hinweg.

Ein weiteres Ergebnis, das die Bedeutung eines starken Schwachstellenmanagement-Programms deutlich macht, ist, dass die Ausnutzung von Schwachstellen an dritter Stelle der beliebtesten Hacking-Techniken rangiert und dass der primäre Vektor für Hacker-Aktionen Webanwendungen sind.

Ein Schlüssel zur effektiven Priorisierung liegt in der Fähigkeit, Erkenntnisse zu Cyberbedrohungen zu verarbeiten und Kriterien wie die Ausnutzbarkeit einer Schwachstelle, Verfügbarkeit eines Patches und andere Echtzeitindikatoren für Bedrohungen heranzuziehen und mit vorhandenen Schwachstellendaten zu korrelieren.

Außerdem hebt der DBIR auch hervor, wie wichtig die Einhaltung von Richtlinien ist. Beispielsweise nennt er als die drei häufigsten Ursachen für die große Mehrzahl der Sicherheitsverletzungen den Missbrauch von Berechtigungen, eine falsche Handhabung von Daten und nicht genehmigte Workarounds: drei Synonyme für mangelnde Compliance.

Compliance wird oft als das Letzte angesehen, was bei implementierten Projekten noch zu tun ist. Der richtige Ansatz wäre dagegen, die Erfassung und Verarbeitung von IT-, Sicherheits- und Compliance-Daten von Anfang an in Einklang zu bringen. Auf diese Weise kann eine einheitliche Datenbasis („Single Source of Truth") geschaffen, bei der Daten aus mehreren Perspektiven visualisiert werden – je nachdem, wer von ihnen Gebrauch macht. Dies erleichtert es auch, Konfigurationsfehler zu reduzieren.

Fazit

Es ist Zeit, dass Unternehmen zu soliden Grundlagen für Sicherheit und Compliance zurückkehren. Beginnend mit einem ständig aktualisierten IT-Asset-Inventar und der umfassenden Erkennung von Schwachstellen und Fehlkonfigurationen. Weiterführend mit der Priorisierung von Abhilfemaßnahmen, indem die Indikatoren für Cyberbedrohungen mit vorhandenen Assets und deren Schwachstellen korreliert werden. Sehr wichtig ist außerdem ein integriertes Patchmanagement-Programm, damit anfällige Assets schnell abgesichert werden können.

Sämtliche Assets – also nicht nur On-Premises-Systeme – müssen abgedeckt werden: mobile Geräte, Cloud-Workloads, containerisierte Anwendungen, DevOps-Pipelines, IoT-Systeme und Betriebstechnik (OT). Nur so kann eine umfassende IT-Security gewährleistet werden.

Marco Rottigni

Threat Hunting: Die Jagd nach Cyberbedrohungen

Die Bedrohungssuche ist eine komplexe Aufgabe, aber mit den richtigen Tools und Technologien kann sie einen großen Unterschied für die Sicherheit in Unternehmen bedeuten.

Threat Hunting oder Bedrohungssuche bedeutet, aktiv nach Malware oder Angreifern zu suchen, die im Netzwerk lauern – und das möglicherweise schon seit geraumer Zeit. Cyberkriminelle lernen immer neue Tricks, um traditionelle Abwehrmaßnahmen zu umgehen. So können sie heimlich still und leise Daten abschöpfen, geduldig nach vertraulichen Daten suchen oder sich durch das Netzwerk arbeiten, um Anmeldeinformationen aufzuspüren. Die Bedrohungssuche unterscheidet sich von traditionellen Maßnahmen des Bedrohungsmanagements wie Firewalls, Intrusion Detection Systems (IDS), Sandboxing und Security Information and Event Management (SIEM). Alle diese Maßnahmen führen eine Untersuchung erst durch, nachdem ein Angriff oder ein Sicherheitsvorfall einen Alarm ausgelöst hat. Es handelt sich also um rein reaktive Maßnahmen.

Anhaltende Bedrohung

Grundlegende Sicherheitsmaßnahmen und ordnungsgemäß implementierte Antivirenprogramme, Firewalls und andere automatisierte Sicherheitstools sollten die Mehrheit der Bedrohungen daran hindern, einzudringen. Sicherheitsexperten gehen davon aus, dass 80 Prozent der Angriffe sehr simpel sind und durch Standard-Sicherheitsmaßnahmen eingedämmt werden können. Die übrigen 20 Prozent stellen hoch entwickelte Bedrohungen dar: Sie lassen sich nicht allein mit programmgesteuerten Lösungen erkennen. Sobald sich ein Angreifer unbemerkt in das Netzwerk eingeschlichen hat, gibt es kaum Möglichkeiten, ihn davon abzuhalten, dort zu verweilen. Studien besagen, dass Cyberkriminelle im Durchschnitt 190 Tage in einem Netzwerk verbringen, bevor sie entdeckt werden – mehr als genug Zeit, Schaden anzurichten. Fortgeschrittene persistente Bedrohungen (Advanced Persistent Threats, APTs) können viel Unheil stiften. Im Vergleich zu einem einfachen Hacking-Versuch erfordert ein APT deutlich mehr Aufwand und Aufmerksamkeit. Hier kommt Threat Hunting ins Spiel. Anders als Threat Detection, dessen Erkennung passiv ist und auf Alarme wartet, ist Threat Hunting aktiv und sucht nach nicht identifizierten schädlichen Aktivitäten.

Die Jagd nach Bedrohungen geht von der Prämisse aus, dass sich die Angreifer bereits im Netzwerk eines Unternehmens befinden und dieses heimlich überwachen und durchforsten. Threat Hunting stoppt diese Angriffe bevor sie ihre Ziele erreichen, indem es verdeckte Indikatoren für Kompromittierungen (IOCs) ausfindig macht. Threat Hunting bietet diverse Vorteile, einige direkt und andere indirekt. Zu den direkten Vorteilen zählen eine geringere Verweildauer für Angreifer, die schnelle Erkennung und Reaktion auf neue schädliche Aktionen sowie neue Erkennungsmethoden. Zu den indirekten Vorteilen zählen das Aufdecken von Regelverletzungen, nicht gepatchten Systemen, riskantem Benutzerverhalten und möglicherweise unbekannten Angriffsflächen in der Umgebung.

Threat Hunting basiert auf Metadaten von Netzwerk- und Endgeräten. Netzwerk-Metadaten sind die Basis für Big-Data-Analysen, während Endpunkt-Metadaten die Jagd auf Angreifer-Aktivitätsmuster ermöglichen. Metadaten lassen sich viel effektiver und günstiger speichern als echte Daten und schnell abfragen. Sie stellen Inhalt und Kontext bereit, der in Firewall-Protokollen oder SIEM-Dashboards nicht auftaucht.

Tarnen und täuschen

Es gibt noch weitere Methoden der Jagd: Zur Elevate-Plattform von Fidelis Cybersecurity etwa zählt neben Komponenten für den Schutz von Endpoints und den Schutz von Netzwerken auch eine Deception-Lösung, mit der sich das Verhalten von Cyberkriminellen beobachten lässt und die gleichzeitig der Ablenkung dient. Deception legt Köder und Attrappen aus, um Hacker und automatisierte Malware anzulocken. Statt vergeblich nach dem bösen Akteur im Ozean guter Daten zu fischen, liefert Deception aussagekräftige Alarme und Verkehrsanalysen. Moderne Deception bietet zudem gefälschte Zugangsdaten mit Active-Directory-Einträgen und simulierten Zugriffen auf Unternehmensressourcen. Dies bildet ein überzeugendes Scheinnetzwerk, das Geräte, Daten und Verhaltensweisen enthält, die alle dazu dienen, dass Angreifer die Köder verfolgen. So können die Verteidiger sie erkennen, daraus lernen und sich erfolgreich verteidigen. Deception stellt auch eine Abwehrmaßnahme für nicht standardmäßige Geräte dar, die keinen Sicherheitsagenten haben – beispielsweise IoT-Geräte für Unternehmen wie Drucker, intelligente Beleuchtungssysteme, Kameras und Switches – sowie nicht mehr supportete Systeme.

Security-Systeme sind wichtig, um gesammelte Metadaten für die Analyse über Ende-zu Ende-Beziehungen hinweg zur Verfügung zu stellen, Alarme auf Endgeräten zu überprüfen, Alarme zu Schlussfolgerungen zusammenzufassen, komplette Abläufe zwischen Deception, Endpunkt und Netzwerk für die Erkennung und Untersuchung bereitzustellen sowie automatisierte Antworten zu ermöglichen. Bei Stand-Alone-Lösungen werden Metadaten häufig nicht erfasst und genutzt. Zudem bleibt es den Unternehmen überlassen, über Schnittstellen (APIs) für eine benutzerdefinierte Integration zu sorgen. Laut Fidelis Cybersecurity können Kunden eine Anzahl von 40 bis 50-Sicherheitslösungen durch Konsolidierung und Integration auf 10-15 Systeme reduzieren. Der zu schützende Bereich wird dabei mit Asset-Profiling und -Klassifizierung als integriertes Feature abgebildet. Ein weiteres Beispiel ist die Bereitstellung von Informationen zu den Endpunkten zur Inventarisierung und um Schwachstellen zu erkennen. Beides verringert die Anzahl der erforderlichen Sicherheitslösungen.

Andreas Dumont, Freier Journalist, Redaktionsbüro Andreas Dumont

Roland Messmer, Sales Director Central Europe, Fidelis Cybersecurity

Fazit
Zusammenfassend lässt sich sagen, dass Unternehmen aktive Taktiken wie Threat Hunting zur Bedrohungserkennung in Betracht ziehen sollten. Mangelnde Ressourcen und Fähigkeiten sind hohe Barrieren, die sich aber überwinden lassen – etwa indem Teile an einen Provider für Managed Detection and Response (MDR) ausgelagert werden.

Andreas Dumont, Roland Messmer

1.3 SICHERHEITSKULTUR

Auf dem Weg in die neue Realität: Wie die Konvergenz von IT und Betriebstechnik den digitalen Wandel vorantreibt

Galina Antova, Mit-Gründerin und Chief Business Development Officer, Claroty

In den letzten Monaten hat sich die Konvergenz von IT- und Betriebstechnik (Operational Technology/OT)-Netzwerken dramatisch beschleunigt und unsere Definition von kritischer Infrastruktur erweitert. Da immer mehr Mitarbeiter von zu Hause aus arbeiteten, wurde die Infrastruktur ihrer Wohnungen zu einer kritischen Infrastruktur für das Unternehmen. Für Unternehmen, die zuvor versucht haben, ihre OT-Netzwerke so isoliert wie möglich zu halten und über keine Fernverbindung verfügten, war dies ein mühsamer und langfristiger Weg. Diejenigen hingegen, die bereits begonnen hatten, sich auf die digitale Transformation einzulassen, konnten den Übergang reibungsloser gestalten, da sie bereits angefangen hatten, sich über die Sicherheit in einer expandierenden und offenen Umgebung Gedanken zu machen.

Für alle Unternehmen mit OT-Netzwerken (und dies sind gemeinhin mehr als man annimmt) beschleunigte die Krise auch die Notwendigkeit der Zusammenarbeit von IT- und OT-Teams. Die extreme Umgestaltung des Arbeitsplatzes brachte eine Menge Stress und Fragen mit sich, insbesondere für Unternehmen in Branchen, die von physischen Prozessen abhängig sind wie die Fertigung, die pharmazeutische Industrie, Energie- und Versorgungsunternehmen oder die Lebensmittel- und Getränkeindustrie: Wie können wir die Produktion sicherstellen? Wie können wir dies tun, ohne dabei die Gesundheit und Sicherheit unserer Mitarbeiter zu gefährden? Was kann aus der Ferne gemacht werden und wo ist Präsenz vor Ort notwendig? Und wie können wir dies ermöglichen, ohne das Risiko von Cyberattacken zu erhöhen?

Bei der Beschäftigung mit diesen Fragestellungen wurde vielen Unternehmen klar, dass bestimmte Prozesse, wie der sichere Fernzugriff auf den Fertigungsbereich, nicht gut funktionierten oder gar nicht existierten. Als Unternehmen zumindest einen Teil ihres OT-Personals ins Homeoffice verlagerten, mussten Mitarbeiter, die zuvor in der Produktionsstätte arbeiteten, plötzlich Änderungen an Produktionslinien und Herstellungsverfahren von Zuhause aus vornehmen. In Fällen, in denen Unternehmen nicht über sichere Fernzugriffsmöglichkeiten verfügten, verwendeten einige OT-Mitarbeiter Tools, die nicht von der IT unterstützt wurden. In anderen Fällen konnten die Lösungen, die sie nutzten, nicht skalieren oder komplexere Konnektivitätsprobleme bewältigen.

Schritte zur Verbesserung der Zusammenarbeit
Die Pandemie hat Sicherheitslücken aufgedeckt und IT- und OT-Teams dazu gezwungen, zusammenzuarbeiten, um praktikable Lösungen voranzutreiben. Ein wesentliches Hindernis für die Zusammenarbeit beider Teams ist, dass die Sicherheitsteams oftmals über keine Transparenz in den OT-Netzwerken und keine Telemetrie verfügen. Es gibt jedoch spezielle Lösungen, die für OT-Transparenz und kontinuierliche Bedrohungsüberwachung entwickelt wurden, und die man schnell implementieren kann. Diese ermöglichen es IT- und OT-Teams, OT-Umgebungen gemeinsam zu betrachten, mit demselben Informationssatz zu arbeiten und spezifische Schritte zu unternehmen, um die Ausfallsicherheit zu erhöhen und neue Produktivitätsebenen zu erreichen. Auf diese Weise wird die Zusammenarbeit konkret und erstreckt sich nicht nur auf die Theorie.

Der unmittelbare Wert lässt sich erkennen, wenn man auf das Beispiel des sicheren Fernzugriffs auf den Fertigungsbereich zurückkommt. Jetzt, da die anfangs häufig recht hektisch in Betrieb genommenen Fernarbeitsplätze errichtet sind, müssen IT- und OT-Teams gemeinsam daran arbeiten, diese Verbindung resilienter zu machen: Durch umfassende und beide Teams umspannende Transparenz können Sicherheitsverantwortliche Remote-Sitzungen in Echtzeit beobachten und diejenigen beenden, die ein Risiko darstellen. Sie sind in der Lage, granulare Zugriffsberechtigungen zu definieren und durchzusetzen, so dass einzelne Benutzer nur für bestimmte Aufgaben in einem festgelegten Zeitfenster spezifischen Zugriff auf die notwendigen Ressourcen erhalten. Zudem können sie auch eine Multi-Faktor-Authentifizierung durchsetzen und Passwort-Tresore aktivieren, um die mit der Verwendung, gemeinsamen Nutzung und Verwaltung von Passwörtern verbundenen Risiken zu eliminieren.

Schneller digitaler Wandel
Trotz aller Herausforderungen der letzten Monate und der noch zu leistenden Arbeit zur Verbesserung der Resilienz erkennen zahlreiche Sicherheitsverantwortliche (CISOs), dass die (oft aus der Not geborene) zunehmenden Akzeptanz digitaler Transformationsprojekte eine enorme Chance darstellt. Unternehmen, die bisher nicht auf verteilte Modelle gesetzt hatten, weil sie nicht empfohlen oder auch für unmöglich gehalten wurden, wissen jetzt, dass sie nicht nur möglich, sondern für den Aufbau von Widerstandsfähigkeit, die Aufrechterhaltung der Produktivität und die Förderung von Wettbewerbsvorteilen von wesentlicher Bedeutung sind. Es ist jedoch eine große Herausforderung für OT-Fachleute, den Rückstand aufzuholen und die seit über 25 Jahren bestehende IT-OT-Sicherheitslücke zu schließen, insbesondere da die Anzahl der Konnektivitätspunkte exponentiell wächst. Die Kombination aus Altgeräten, vielen weiteren Angriffsvektoren und versierten, oftmals staatlich unterstützten Angreifern erzeugt eine schwierige Großwetterlage.

Dabei ist es hilfreich, IT- und OT-Netzwerke nicht mehr als getrennt zu betrachten, sondern als eine einheitliche Infrastruktur, da sie als solche auch von den Angreifern gesehen und verstanden wird. Mit dieser Perspektive kann man damit beginnen, Governance und Prozesse ganzheitlich anzugehen, was die Resilienz nachhaltig verbessert. Was die Technologie anbelangt, so muss man in aller Regel von Grund auf starten, da OT-Netzwerke zumeist über keine modernen Sicherheitskontrollen verfügen. Was sich wie ein Nachteil anhört, ist jedoch eher ein Vorteil: Es besteht keine Notwendigkeit, die gewachsene Komplexität der IT-Security mit häufig mehr als 15 verschiedenen Tools zu replizieren. Vielmehr gibt es spezielle OT-Technologien, bewährte Verfahren und spezielle Playbooks, die mehrere Sicherheitsfunktionen adressieren, wodurch sich das Risiko in sehr kurzer Zeit wesentlich reduzieren lässt.

Während wir auf eine Zukunft hinarbeiten, die mehr und mehr verteilt sein wird, konvergieren IT- und OT-Umgebungen weiter und IT- und OT-Teams müssen noch stärker zusammenarbeiten, um ihre Initiativen zur digitalen Transformation umzusetzen. Allen gemeinsam ist das gleiche Ziel: die Risikominimierung. Diese muss in OT-Umgebungen jedoch auf eine andere Art und Weise umgesetzt werden als wir es von der IT kennen. So spielt für IT-Sicherheitsteams beispielsweise das Patchen und der Einsatz von Sicherheitslösungen eine wichtige Rolle, während OT-Teams eher die Ausfallzeiten im Blick haben, die mit Updates und der Implementierung von Kontrollen einhergehen können. Diese Unterschiede müssen wir erkennen und respektieren, da wir nur so das gemeinsame Ziel erreichen können.

Galina Antova

Unternehmen brauchen eine Sicherheitskultur

Eine gesunde und effektive Sicherheitskultur trägt wesentlich zur Sicherheit eines Unternehmens bei. Doch bei der Umsetzung tun sich viele deutsche Betriebe schwer.

Sicherheit muss mehr sein als ein lästiges Anhängsel, das es eben auch zu erledigen gilt. Sicherheit muss vielmehr eine Grundhaltung sein, die Basis eines Unternehmens, und von der Führungsebene bis zum Praktikanten muss jeder mitziehen. Eine angemessene Sicherheitskultur schafft die entsprechenden Voraussetzungen.

Andreas Dumont, Freier Journalist, Redaktionsbüro Andreas Dumont

Der Faktor Mensch
In Sachen Hardware und Software ist Sicherheit inzwischen im Bewusstsein der meisten Unternehmen verankert: Firewalls, Endpoint-Security, Detection & Response, Access Control und viele weitere Techniken gehören heute zum gängigen Abwehr-Arsenal gegen Cybercrime. Doch es gibt noch einen weiteren Bereich, den viele Firmen nicht auf dem Radar haben – die eigenen Mitarbeiter. Auch die ausgefeilteste Technik schützt nicht vor dem Einfallstor Mensch. Manche Studien gehen davon aus, dass mehr als drei Viertel der erfolgreichen Cyberangriffe aus menschlichem Fehlverhalten resultieren. Zu den hauptsächlich verwendeten Angriffsvektoren zählen Social Engineering und insbesondere Phishing. Wenn es einem Cyberkriminellen gelingt, auch nur einen einzigen Mitarbeiter zu einem Fehlverhalten zu verleiten, dann ist die Sicherheit des gesamten Unternehmens gefährdet. Deshalb ist eine gelebte Sicherheitskultur von großer Bedeutung. Mit den passenden Schulungen wandeln sich die Mitarbeiter von einem unkalkulierbaren Sicherheitsrisiko zu einem wertvollen Sicherheitsfaktor.

Sein und Schein
In der Studie „Rise of Security Culture" von Forrester Consulting gaben 94 Prozent der Teilnehmer an, dass eine Sicherheitskultur wichtig für den Geschäftserfolg sei. Doch die Realität sieht anders aus: Das Sicherheitsbewusstsein der Mitarbeiter liegt bei vielen Unternehmen im tiefen Dornröschenschlaf. Viele Entscheider und Geschäftsführer reden von einer Sicherheitskultur, wollen aber kein Geld in die Hand nehmen, um eine solche nachhaltig umzusetzen und aufrechtzuerhalten. Vor allem KMUs haben hier einen großen Nachholbedarf.

Die Schwierigkeiten beginnen schon bei der Definition der Sicherheitskultur, unter jeder etwas anderes versteht. Jelle Wieringa, Security Awareness Evangelist beim Schulungs-Spezialisten KnowBe4, definiert es so: „Es ist das Wissen, die Überzeugungen und das Verhalten der Personen in einem Unternehmen. Es sind diese drei Elemente, die Sie grundsätzlich angehen müssen."

Dazu kommt, was für das eine Unternehmen gut ist, funktioniert in einem anderen vielleicht gar nicht. Und wie lässt sich der Erfolg einer Sicherheitskultur messen, die wenig greifbar erscheint? Das norwegische Unternehmen CLTRe hat sich genau darauf spezialisiert. Es hat eine Methode entwickelt, mit der sich der aktuelle Zustand der Sicherheitskultur und deren Veränderungen im Laufe der Zeit bewerten lässt. Damit lässt sich feststellen, ob ein Unternehmen eine ernsthafte Sicherheitskultur lebt, oder ob es nur so tut.

Phishing und Social Engineering

Phishing bleibt der große Türöffner für das Einschleusen von Malware. Die Methoden von Social Engineering werden immer ausgeklügelter und sind oftmals nur schwer zu erkennen. Unternehmen können Unsummen für ihr IT-Budget ausgeben, aber wenn die Mitarbeiter immer noch auf jeden Link in ihren E-Mails klicken, dann ist das alles für die Katz.

Mehr als die Hälfte der Unternehmen tun nichts, um Mitarbeiter vor Phishing zu schützen. Sie können eine Firewall kaufen, aber gegen Social Engineering gibt es keine technische Lösung. Unternehmen jeder Größe sollten Security-Awareness-Trainings einführen und ihre Mitarbeiter regelmäßig zur Erkennung von Phishing schulen, und die Sicherheit als Teil der Arbeitsaufgaben in die Unternehmenskultur integrieren. Gut geschulte Mitarbeiter können als erste Verteidigungslinie im Unternehmen fungieren.

Zuckerbrot ohne Peitsche

Eingeschliffene Verhaltensweisen von Menschen zu ändern, ist ein schwieriges Unterfangen. Cyberkriminelle lieben das. „Wenn man ihnen das Wissen vermitteln, ihnen helfen, zu verstehen, was Phishing ist, welche Formen Phishing haben kann, und sie verstehen, warum es wichtig ist, nur dann kann man ihr tatsächliches Verhalten verändern“, ist Wieringa überzeugt.

Der Schlüssel zum Erfolgt liegt auch darin, richtiges Verhalten zu belohnen, satt Fehler zu bestrafen. Mitarbeiter ändern ihr Verhalten dann, wenn sie Lob für sichere Arbeitsweisen bekommen, wenn sie sich an Vorbildern orientieren können, oder auch, wenn sie eine Tätigkeit unzählige Male durchführen bis sie zu einem Automatismus geworden ist. Hier sind Geschäftsführer, Entscheider und Vorgesetzte in der Pflicht: Sie müssen die Sicherheitskultur vorleben. Wer A predigt aber B durchführt, wird nur Wenige für A begeistern können. Sie müssen handeln, statt nur zu reden, und mit gutem Beispiel vorangehen.

Wege zur Sicherheitskultur

Das Konzept der Sicherheitskultur ist nicht neu. Sie ist eine Art Unterabteilung der Unternehmenskultur. Wenn man die Unternehmenskultur als ein großes Buch betrachtet, dann ist die Sicherheitskultur ein Kapitel in diesem Buch. Es ist ein Kapitel, das nicht so oft gelesen wird.

Viele stehen nicht der Wert einer Sicherheitskultur. Es geht nicht um Technologie. Kultur ist schwer zu erklären, es gibt weder eine Standardformel noch einen Trick, der bewirkt, dass Unternehmen eine gute Sicherheitskultur erhalten. Sicherheitskultur ist eine C-Level-Angelegenheit, die Top-Down erlogen muss. Sie basiert auf dem Dreiklang Wissen, Verstehen, Verhalten. Eine Sicherheitskultur zu entwickeln, umzusetzen und zu betreuen kostet viel Zeit – und Geld. Doch es lohnt sich. Zum einen sind die Unternehmen vor Cyberangriffen und anderen Sicherheitsvorfällen besser geschützt – die übrigens ein Vielfaches der Summe kosten können, die für eine anständige Sicherheitskultur notwendig ist. Zum anderen profitieren sie auch indirekt: Unternehmen mit einer guten Sicherheitskultur steigen auch im Ansehen ihrer Kunden. Es ist das beste Marketing, das man bekommen kann.

Die Sicherheitskultur im Unternehmen ist ein Unterfangen, das niemals endet. Nach einer erfolgreichen Entwicklung und Einführung einer Sicherheitskultur muss das Unternehmen am Ball bleiben. Das Wichtigste ist eine kontinuierliche Kommunikation. Es geht darum, Abläufe bei sicherheitsrelevanten Meldungen zu stärken und regelmäßig die Fortschritte zu kommunizieren. Mitarbeiter wie Management sollten immer mal wieder diskutieren, was gut läuft und was verbessert werden könnte. Ein teamorientierter Ansatz verstärkt das Gefühl, dass alle an einem Strang ziehen. Teilen Sie Ihre Verbesserungen allen mit, um zu zeigen, dass die Sicherheitskultur weiter aufgebaut wird. Fortschritte schaffen zudem neue Budgets, denn Sicherheitskultur kostet leider Geld.

Andreas Dumont

Deep Fakes – Falsche Tatsachen bedrohen die Unternehmenssicherheit

Im Internet sind Fakes weit verbreitet: Manipulierte Bilder, erfundene Nachrichten oder falsche Behauptungen. Es wird immer schwieriger, zwischen Fake und Wirklichkeit zu unterscheiden. Inzwischen gibt es eine neue Fälschungsvariante: Deepfakes.

Zum ersten Mal aufgetaucht ist diese Art der verdrehten Realität im Dezember 2017 auf der Plattform Reddit. Ein Benutzer hatte ein Video veröffentlicht, in dem die Gesichter von Prominenten glaubhaft in schlüpfrige Szenen eingebaut wurden. Dafür hat der anonyme Absender einen Algorithmus erstellt, der auf frei verfügbaren Applikationen beruht wie Keras und Googles TensorFlow.

Inzwischen sind solche gefälschten Videos auf vielen Plattformen wie Twitter oder Discord verboten. Doch Deepfakes haben ihren Siegeszug bereits begonnen und lassen sich nicht mehr aufhalten.

Fälschung ohne Fachwissen

Früher waren Videofakes, bei denen Gesichter ausgetauscht wurden, nur mit viel Arbeit und fachlichem Wissen zu bewerkstelligen. Für Deepfakes ist das nicht notwendig, denn die Manipulationen erstellt der PC weitgehend automatisch.

Deepfakes verdanken ihren Namen der Tatsache, dass sie auf Deep Learning basieren. Das ist eine besondere Art des Machine Learnings, das bei künstlicher Intelligenz zum Einsatz kommt. Die den Deepfakes zu Grunde liegenden Algorithmen werden mit großen Mengen Bild- und Videomaterial gefüttert. Je mehr Daten von einer Person vorliegen, desto besser und genauer fällt das Resultat aus. Videos sind das perfekte Ausgangsmaterial, da sie sich in Hunderte Einzelbilder aufsplitten lassen und die Person aus den unterschiedlichsten Perspektiven zeigen. Schon wenige Hundert Bilder der Zielperson reichen aus, um einen plausiblen Deepfake zu erzeugen. Ein Beispiel, wie das Ganze funktioniert, ist hier zu sehen: https://www.youtube.com/watch?v=5rPKeUXjEvE&feature=youtu.be

Die eigentliche Arbeit erledigt ein neuronales Netz. Wenn man es mit Bildern von Kätzchen versorgt, lernt es mit der Zeit, Tier und Hintergrund zu unterscheiden, so dass es letztlich selbst Kätzchen erzeugen kann. Mit Köpfen und Gesichtern funktioniert es analog. Das neuronale Netz weiß am Ende genau, welche Merkmale das Gesicht der Zielperson aufweist, und kann es selbstständig neu erzeugen und in bestehende Videos einpflanzen. Ein Algorithmus erstellt dabei den Fake, ein zweiter sucht nach Fehlern und meldet diese zurück. Mit der Anzahl der Wiederholungen steigt die Qualität des Fakes. Auch Stimmen lassen sich auf diese Weise nachbauen, das nennt sich dann Deepvoice.

Der grundlegende Unterschied zu den herkömmlichen Fakes, bei denen etwa der Kopf aus einem Bild in ein anderes Bild eingefügt und dann mit Photoshop noch ein wenig retuschiert wird, ist folgender: Deepfakes hantieren nicht mit bestehenden Daten, sondern erzeugen neues Material.

Der Code für Deepfakes ist Open Source und steht somit jedermann zur Verfügung. Auf GitHub lassen sich mehrere Projekte finden, in denen Entwickler an solchen Algorithmen arbeiten, ein Beispiel ist FakeApp.

Deepfakes erkennen

Deepfakes wirken auf den ersten Blick authentisch, sind aber nicht perfekt. Wenn aus bestimmten Blickwinkeln nicht genügend Daten zur Verfügung stehen, dann muss der Algorithmus auf Details verzichten. Das führt zu leicht schwammigen Bildbereichen. Auch der Haaransatz und die Ohren wirken manchmal bei genauem Hinsehen etwas unscharf oder unecht. Kleine Details sind oft verräterisch: zwei ungleiche Ohrringe, zu viele Schneidezähne, eine unsymmetrische Brille. Das neuronale Netz kennt die echte Welt nicht mal ansatzweise und auch weiß nicht, wie Schärfentiefe oder Schatten physikalisch korrekt aussehen. Menschen fallen „schräge“ Dinge meistens schnell auf.

Mit Hilfe von speziellen Programmen lassen sich zudem Blinzelmuster, die Hautfarbe oder das Pulsieren des Blutes analysieren. Ein Siver Bullet gegen Deepfakes existiert allerdings noch nicht.

Gefahren durch Deepfakes

Um Deepfakes mit einem Programm wie FakeApp zu erzeugen, ist lediglich eine möglichst leistungsstarke Nvidia-Grafikkarte notwendig. Sie stellt die nötige Rechenleistung bereit. Mit einer PC-CPU funktioniert es grundsätzlich auch, dauert aber wesentlich länger. Deepfakes stehen folglich nicht nur Youtube-Trollen zur Verfügung, sondern auch Cyberkriminellen.

„Deepfakes könnten dazu missbraucht werden, um Unternehmen oder Einzelpersonen zu erpressen, indem die Zielperson in eine strafbare Szenerie platziert wird. Gefälschte Manager-Anweisungen, einen bestimmten Betrag zu überweisen, führen womöglich zu finanziellen Verlusten. Auch das im Privatbereich verbreitete Ident-Verfahren per Video ist nicht mehr fälschungssicher,“ erklärt Jelle Wieringa, Security Awareness Advocate bei KnowBe4.

Gesellschaftliche Veränderungen sind zu befürchten, wenn es immer schwieriger wird, die Echtheit eines Videos zu bestimmen. Auch Videobeweise – vor Gericht, nicht im Fußball – verlieren vielleicht ihre Beweiskraft. Letztlich lassen sich Deepfakes und Deepvoice auch für Meinungsmache und Propaganda einsetzen und um die Politik zu beeinflussen. Im Zeitalter von Social Media verbreiten sich Videos schnell, auch wenn es sich dabei offensichtlich um Deepfakes handelt. Man sieht, was man sehen will. Dazu kommt: Deepfakes werden in Zukunft immer glaubwürdiger wirken.

Gesetzliche Maßnahmen – Fehlanzeige in Deutschland

China hat eine neue Regierungspolitik veröffentlicht, welche durch KI gefälschte Nachrichten und irreführende Videos verhindern soll. Die neue Regelung sieht vor, dass bei deren Veröffentlichung im Internet, gekennzeichnet werden soll, dass der betreffende Beitrag mit KI- oder VR-Technologie erstellt wurde. Geschieht dies nicht wird ein Strafverfahren eröffnet. Die Regelung tritt zum Neujahr 2020 in Kraft. Ihre Durchsetzung wird von der Cyberspace Administration of China übernommen.

Die chinesische Regierung zieht mit ähnlichen Gesetzen nach, die bereits in den USA zur Bekämpfung von Cyber-Kriminalität existieren. Im vergangenen Monat war Kalifornien der erste US-Bundesstaat, der

die Verwendung von Deepfakes in der Werbung für politische Kampagnen unter Strafe stellte. Das Gesetz, AB 730 genannt und von Gouverneur Gavin Newsom unterzeichnet, macht es zum Verbrechen, Audio-, Bild- oder Videodaten zu veröffentlichen, die einen falschen beziehungsweise schädlichen Eindruck von den Worten oder Handlungen eines Politikers vermitteln. Die Norm gilt für Kandidaten innerhalb von 60 Tagen nach einer Wahl und soll bis 2023 auslaufen, sofern sie nicht ausdrücklich verlängert wird.

In Deutschland existiert kein grundlegendes Gesetz, welches Deepfakes reguliert. Tatsächlich sind aber zwei Gesetzestexte zum Thema heranzuziehen. Zum einen verletzt die Verwendung von Gesichtern das Recht am eigenen Bild, welches im Kunsturheberrechtsgesetz geregelt ist. Demnach sind Bilder von Personen nicht ohne deren Einwilligung zu verwenden. Ergänzend regelt das Grundgesetz das Persönlichkeitsrecht, da die öffentliche Diffamierung dem Ruf der Betroffenen schaden könnte.

Schulung und Sensibilisierung

„Mitarbeiter sind das größte Risiko, und dem sicherheitsbewussten Verhalten jedes Einzelnen kommt eine entscheidende Bedeutung zu. Unternehmen sollten ein Bewusstsein dafür schaffen, dass Deepfake-Attacken jederzeit möglich sind. Wer weiß, dass eine Stimme am Telefon nicht zwangsläufig zu der erwarteten Person gehört, kann möglichen Angriffen besser aus dem Weg gehen. Die alleinige Implementierung von Sicherheitstechnologien wie Firewall, IDS oder Endpoint Protection reicht nicht mehr aus. Zusätzlich sind „menschliche Firewalls“ gefragt“ führt Wieringa aus.

Ein Weg zur Sensibilisierung sind firmenspezifische Schulungen, in denen auf mögliche Social-Engineering- und Deepfake-Angriffe auf das jeweilige Unternehmen eingegangen wird. Generische Awareness-Trainings hingegen werden von den Mitarbeitern oft als lästige Pflichtübung betrachtet und erzielen folglich bestenfalls mäßigen Erfolg. Viele Unternehmen setzen nach wie vor auf den Angstfaktor. Um Verhaltensänderungen zu erzielen, ist es aber erfolgversprechender, die positiven Auswirkungen eines korrekten Verhaltens hervorzuheben. Wieringa erläutert: „Bei Security-Awareness-Training sollte es nicht einfach darum gehen, Wissen zu vermitteln, sondern darum, das Verhalten zu verändern. Das gelingt am besten mit Emotionen. Es muss den Mitarbeitern Spaß machen, sicherheitsbewusstes Verhalten zu erlernen.“

Die Trainings der Schulungsplattform KnowBe4 etwa arbeiten auch mit Comics und Netflix-ähnlichen Videoserien. Cliffhanger sorgen dafür, dass die Kunden von sich aus mehr davon haben wollen. Auch Gamification-Elemente wie zu gewinnende Badges oder Wettkämpfe zwischen mehreren Teams eines Unternehmens sorgen spielerisch für eine Sensibilisierung. Training sollte Spaß machen, interaktiv und auf die aktuellen Bedrohungen zugeschnitten sein.

Fazit

Die Technologie für Deepfakes wird bald so gut sein, dass die Stimme in Echtzeit generiert werden kann. Ein Angreifer kann so direkt mit seinem Opfer interagieren und etwa wie ein Vorgesetzter oder wie der CEO des Unternehmens klingen. Es ist also höchste Zeit, Mitarbeiter wie auch Privatpersonen zu sensibilisieren. Auf der anderen Seite könnte sich Deepvoice auch dazu nutzen lassen, Trainings mit der Stimme des Chefs oder eines beliebten Schauspielers durchzuführen.

Andreas Dumont

Business Continuity vs. Security

Gerade jetzt hat die Aufrechterhaltung des Geschäftsbetriebs für viele Unternehmen höchste Priorität. Um diese zu garantieren, mussten IT- und Sicherheitsteams bei dem enormen Zuwachs an Homeoffice-Arbeitsplätzen einige Risiken eingehen, die von Angreifern ausgenutzt werden können. So ist die Zahl der Mitarbeiter, die über das Internet mit Unternehmensressourcen verbunden sind, weltweit um über 30 Prozent angestiegen, die Nutzung von Microsoft Teams hat sich gar verfünffacht. Durch diesen Wettlauf um Remote-Arbeitsplätze entstehen jedoch Einstiegspunkte für Angreifer: Jedes neue System mit Internetanschluss und jeder Mitarbeiter, der von Zuhause aus arbeitet, vergrößert die Angriffsfläche. Und durch den Zeitdruck wird das Risiko zusätzlich erhöht.

Zahlreiche Bedrohungen für Homeoffice-Arbeitsplätze

Wie versuchen nun Angreifer Profit aus dieser außergewöhnlichen Situation zu schlagen? Die Spezialisten des Varonis Incident-Response-Teams konnten einen deutlichen Anstieg von Brute-Force-Angriffen auf VPNs, Remote Desktops und Microsoft 365-Konten erkennen. Bei einer solchen Attacke versuchen Angreifer durch ein automatisiertes Ausprobieren von vorab gesammelten Listen von Anmeldeinformationen die richtigen Benutzername/Passwort-Kombinationen herauszufinden. Brute-Force-Angriffe sind also recht einfach gestrickt, aber effektiv. Wenn es einem Angreifer gelingt, sich mit einer der anvisierten Ressourcen zu verbinden, erhält er Zugang zu Infrastruktur und Daten, die er zerstören, gegen Lösegeld verschlüsseln oder stehlen kann. Leider verfügen die die wenigsten Unternehmen über Einblicke in einen „normalen“ Fernzugriff und können infolgedessen nicht den Unterschied zwischen einem legitimen Homeoffice-Nutzer und einem Angreifer erkennen, der ein Nutzerkonto kompromittiert hat.

Einen gewissen Schutz bietet hier Multi-Faktor-Authentifizierung. Dabei benötigen die Nutzer neben dem Passwort einen weiteren Faktor, in aller Regel eine PIN, die sie per SMS auf ihrem registrierten Mobiltelefon erhalten. Dabei ist aber zu bedenken: Auch die Multi-Faktor-Authentifizierung kann mittels Phishing umgangen werden, indem sowohl Passwörter als auch die PINs abgefangen werden. Dies stellt für versierte Hacker nur eine minimale Hürde dar. Und die starke Verbreitung von Microsoft 365 bietet Angreifern weitere Möglichkeiten. So können sie etwa mittels bösartiger Azure Apps Benutzer so täuschen, dass sie Zugriff auf ihre in der Cloud gehosteten Daten gewähren. Wenn ein Angestellter auf eine scheinbar normale „Zugriff erlauben“-Seite klickt, kann der Angreifer Zugriff auf alle Daten erhalten, auf die der Angestellte in Microsoft 365 zugreifen kann, einschließlich Dateien und E-Mails.

Alle diese beschriebenen Bedrohungen funktionieren, ohne dass der (private) Computer oder das Heimnetzwerk im Homeoffice kompromittiert werden muss. Diese ungemanagten Geräte stellen eine zusätzliche Herausforderung dar. Die IT- und Sicherheitsverantwortlichen haben hierüber keinerlei Kontrolle und können den jeweiligen Sicherheitsstatus kaum beeinflussen. Es kann (und wird) sich dabei auch um ältere, nicht gepatchte Systeme handeln, die leicht mit Malware infiziert werden können. Dies wiederum erlaubt Angreifern zahlreiche Möglichkeiten, über VPN-, Cloud- oder Web-Anwendungen Zugriff auf sensible Unternehmensdaten und -ressourcen zu erhalten.

Gefahren auch von Innen

Neben diesen eher technischen Aspekten sollten wir aber auch die psychologischen Aspekte nicht aus den Augen verlieren. Mitarbeiter stehen in diesen Zeiten unter Stress und befürchten aufgrund der wirtschaftlichen Entwicklungen möglicherweise Entlassungen. Im Jahr 2008, auf dem Höhepunkt der Finanzkrise, haben unsere Sicherheitsexperten viele ungewöhnliche Aktivitäten identifiziert: Zahlreiche Mitarbeiter unserer Kunden haben beispielsweise auf Daten zugegriffen, auf die sie normalerweise nicht zugegriffen haben, haben Daten kopiert u.ä. Dieses abnormale Verhalten ist schon in normalen Büros mit von der IT-Abteilung gemanagten Computern schwer zu erkennen. Bei Homeoffice-Nutzern ist diese Herausforderung ungleich größer.

Die Geschäftskontinuität ist verständlicherweise im Moment für Unternehmen ein Hauptanliegen. Die Mitarbeiter sollen weiterhin in der Lage sein, ihre Aufgaben bestmöglich zu erledigen. Bei aller Eile, ihnen alle nötigen Ressourcen und Daten zur Verfügung zu stellen, sollte man aber auch die Sicherheit nicht aus den Augen verlieren. Denn ein einziges kompromittiertes Nutzerkonto reicht aus, enormen Schaden für das gesamte Unternehmen zu verursachen. Um dies zu verhindern, sollten ein paar Punkte beachtet werden:

- **Stellen Sie sicher, dass Sie Verbindungen zu und durch Ihre entfernte Infrastruktur sehen können.** Wenn Sie nicht nachvollziehen können, wer sich wann und von wo aus mit internetfähigen Geräten oder Cloud-Ressourcen verbindet, sind Sie blind für mögliche Gefahren und Risiken und haben keine Möglichkeit, eine legitime Verbindung von einer kompromittierten zu unterscheiden.
- **Verschaffen Sie sich Einblick in die Infrastruktur und Daten, auf die aus dem Homeoffice zugegriffen wird.** Nur wenn Sie wissen, auf welche Ressourcen und Daten von den entfernten Mitarbeitern zugegriffen wird, können Sie einschätzen, ob es sich um normale, legitime Aktivitäten handelt oder um einen Angreifer oder Innentäter.
- **Setzen Sie auf Automation.** Gerade bei einer hohen Anzahl von Homeoffice-Nutzern kommt es zu vielen Verbindungen und Zugriffen, die man unmöglich manuell überprüfen kann. Hier kann es auch schnell zu einer wahren Flut an Warnmeldungen kommen, auf die dann kaum mehr reagiert wird. Die sogenannte Alarmmüdigkeit ist gerade aktuell eine ernsthafte Gefahr. Effektiver ist es, mittels Automatisierung die Aktivitäten mit weiteren Informationen anzureichern und in einen Kontext zu bringen. Auf diese Weise lassen sich ungewöhnliche Aktivitäten wesentlich präziser identifizieren, untersuchen und gegebenenfalls stoppen. Die intelligente Analyse des Nutzerverhaltens ist hier die einzige Möglichkeit, abnormale Aktivitäten effektiv und schnell zu identifizieren.
- **Reduzieren Sie die Angriffsfläche.** Selbst wenn die Geschäftskontinuität eine Priorität ist, stellt ein breiter Zugang ein großes Risiko dar. Mitarbeiter haben in aller Regel Zugriff auf viel zu viele Daten. Gemäß dem Datenrisiko-Report 2019 können in jedem zweiten Unternehmen (53 %) alle Mitarbeiter auf mehr als 1.000 sensible Dateien zugreifen und bei fast ebenso vielen (51 %) unterliegen mehr als 100.000 Ordner keiner Zugriffsbeschränkung. Die Begrenzung der Zugriffsrechte nach dem need-to-know-Prinzip, bei dem jeder Mitarbeiter nur auf die Daten zugreifen kann, die er tatsächlich für seine Arbeit benötigt, ist ein wirksames Mittel, um den Schaden zu reduzieren, den ein Angreifer anrichten kann. Auch die Beschränkung des Zugriffs in großem Maßstab erfordert Automatisierung: es gibt viel zu viele Dateien und Ordner, die manuell bewertet und korrigiert werden müssen. Im Durchschnitt hat ein Mitarbeiter Zugriff auf 17 Millionen Dateien und über eine Million Ordner!

Für Cyberkriminelle bieten diese Zeiten enorme Chancen und oftmals leichte Beute. Noch nie war es einfacher, Schwachstellen zu monetarisieren. Und es ist auch nicht absehbar, wie lange diese Situation anhalten wird, aber wir können davon ausgehen, dass ein größerer Teil der Belegschaft für eine beträchtliche Zeit im Homeoffice arbeiten wird. Deshalb ist es jetzt höchste Zeit, die Business-Continuity-Pläne in Bezug auf die Sicherheit zu hinterfragen und hier gegebenenfalls nachzujustieren.

Michael Scheffler

Michael Scheffler, Country Manager DACH, Varonis Systems

1.4 CLOUD SECURITY

Cloud- und lokale Umgebungen: Ratschläge für Unternehmen, um ihre IT-Strukturen umfassend zu verwalten, und wie eine Security-Automatisierung dabei hilft

Vor kurzem habe ich mich zu einem Couch-Talk mit unserem Produktmarketing-Manager Yitzy Tannenbaum zusammengesetzt. Wir wollten meine Erfahrungen aus der Arbeit mit Hunderten von Unternehmen weltweit und in verschiedenen Branchen erörtern und darüber sprechen, wie deren Sicherheitsansätze miteinander verglichen werden können und zugleich kontrastieren. Gemeinsam diskutierten wir die Veränderungen, die ich in der Unternehmenssicherheit sehe, und sprachen darüber, wie verschiedene Organisationen die Sicherheit in ihren komplexen Netzwerkumgebungen unterschiedlich verwalten. Einige Auszüge unseres Gesprächs möchte ich hier wiedergeben.

Cloud Computing berührt alles...

Jeder einzelne Kunde, mit dem ich arbeite, hat sich entschieden, Teile seiner IT-Infrastruktur auf die eine oder andere Weise in die Cloud zu verschieben. Daher werden nun einige Geschäftsanwendungen vom traditionellen Rechenzentrum in die Cloud und in softwaredefinierte Netzwerke (SDN) geschoben. Das herkömmliche On-Premise-Netzwerk wird also allmählich auf Cloud- oder Hybrid-Implementierungen umgestellt. Diese hybriden Umgebungen aber erfordern komplexe Richtliniensätze für Firewalls, was den Bedarf an Sicherheitslösungen für die Verwaltung dieser Netzwerkregeln erhöht.

...das macht die Sicherheit komplexer

Die üblichen Cloud-Anbieter, wie Amazon Web Services (AWS) und Microsoft Azure, bieten integrierte Sicherheitskontrollen zu geringen oder gar keinen Kosten an. Diese sind sogar bis zu einem gewissen Grad sehr effektiv. Wir sehen jedoch, dass Unternehmen zusätzlich klassische Firewall-Drittanbieter einführen, in der Regel auf der Ebene der Virtual Private Cloud (VPC) oder des VNet, um eine höhere Filter- und Kontrollstufe zu erreichen. Das ist es ja, was diese Firewall-Anbieter gut können – sie ermöglichen den höheren Grad an Kontrolle, der für die Segmentierung größerer Netzwerke oder VPCs innerhalb der hybriden- oder Cloud-Umgebung erforderlich ist.

Das bedeutet, dass Unternehmen mit einer Kombination aus hybriden, Cloud- und On-Premise-Sicherheitskontrollen täglich arbeiten, die von sehr unterschiedlichen Personen mit sehr unterschiedlichen Prioritäten – und traditionell mit sehr unterschiedlichen Geschwindigkeiten – verwaltet werden. Wie wir wissen, ist die Cloud aber sehr dynamisch in ihrer Struktur – Stichwort: enorme Skalierung – und erlaubt hohe Geschwindigkeiten bei vielen Verbindungen – ein halsbrecherisches Tempo im Vergleich zu traditionellen Hub-and-Spoke-Modellen.

Die Kontrolle über die Sicherheit erhalten

Organisationen beginnen aus diesem Grund, ihre Konzepte zu ändern. Viele unserer Kunden haben nun spezielle Cloud-Sicherheits-Teams eingesetzt, während andere die Sicherheitskontrollsätze an das Personal von DevOps übergeben haben – letztere sind eigentlich für die Einführung von neuem Code in die Cloud verantwortlich. Dies kann jedoch das Risiko eines ‚Wildwest-Szenarios' mit sich bringen: Plötzlich müssen sich die Abteilungen, die ein großes Interesse an der Konnektivität zur Cloud haben – um die Verwendung ihrer Anwendungen zu ermöglichen – selbst um die Sicherheitskontrollen kümmern.

Dabei ist das Risiko offensichtlich: Das Personal der DevOps hat möglicherweise keinen Sicherheitshintergrund und ist daher weniger geneigt, die Sicherheit in der Cloud auf eine Weise zu verwalten, die der allgemeinen Unternehmensführung entspricht. Aus diesem Grund sind traditionelle Sicherheitsgruppen so sehr darauf bedacht, Einblick in die Cloud zu gewinnen, um die Kontrolle über den Netzwerkverkehr wiederzuerlangen.

Eine große Herausforderung für die Unternehmen liegt im Bereich Netzwerk und Sicherheit und besteht darin, diese isolierten Prozesse zusammenzubringen. Dann kann das Personal in der Cloud und bei DevOps sehr schnell Änderungen in der Cloud vornehmen, indem es sich direkt an die APIs und die Cloud-Anbieter wendet.

Die Konnektivität, die in der On-Premise-Umgebung gegeben sein muss, um sicherzustellen, dass alle Anwendungen funktionieren, erfolgt jedoch nach wie vor über umständliche, manuelle Firewall-Änderungen. Dies kann leicht zu Fehlern führen, die sich über lokale und Cloud-Umgebungen erstrecken – in unserer Umfrage vom Mai 2019 zu den Sicherheitsherausforderungen in der Cloud hatten 42,5 Prozent der Befragten einen Netzwerk- oder Anwendungsausfall erlebt. Die Hauptursache war ein betriebliches oder menschliches Versagen bei der Verwaltung von Sicherheitsgeräten. Aus diesem Grund suchen Unternehmen zunehmend automatisierte Sicherheitslösungen, die einen umfänglichen Überblick der Umgebungen und vollständige Kontrolle von einer einzigen Plattform aus ermöglichen.

Organisationen müssen die Möglichkeit haben, sowohl Cloud-Umgebungen als auch On-Premise und SDN an einem Ort zu betrachten und die Konnektivität für Schlüsselanwendungen in all diesen Umgebungen auf einen Blick zu sehen. Sie können nicht langwierig mit unterschiedlichen Prozessen und Technologien umständlich hantieren.

Überlastung der Sicherheitsregeln

Während unseres Gesprächs diskutierten Yitzy Tannenbaum und ich die Herausforderung für Organisationen, die mit einem geschäfts-kritischen Fehler umgehen müssen. Es ist klar, dass die Priorität darin besteht, die entsprechende Anwendung so schnell wie möglich zum Laufen zu bringen. Das aber bedeutet, dass die Versuchung besteht, den Datenverkehr umzuleiten oder eine Sicherheitsregel schnell zu ändern, ohne das bestehende Regelwerk an sich zu optimieren.

Wenn ich in ein großes Unternehmen gehe und mir, beispielsweise, das größte Rechenzentrum dort ansehe, gibt es sehr häufig Firewalls, die seit Jahren in Betrieb sind. Sie haben meist einen organischen Aufbau und mehrere Umzüge im Rechenzentrum oder von Firewall zu Firewall durchlaufen. Über die Jahre hat sich so ein massiver Block von Sicherheitsregeln aufgebaut.

Vor allem große Unternehmen haben daher einen riesigen Bestand an Sicherheitsregeln zu verwalten. Üblicherweise stellen wir bei der Analyse der Sicherheitsinfrastruktur eines neuen Kunden fest, dass 50 Prozent – oder sogar mehr – seiner Sicherheitsrichtlinien überarbeitet oder optimiert werden könnten. Aufgrund der höchst dynamischen Netzwerkumgebung eines Unternehmens muss diese Bereinigung früher als später erfolgen.

Übergang zur kontinuierlichen Einhaltung

Ein weiterer Effekt der zunehmend dynamischen, schnelllebigen Netzwerklandschaft ist die notwendige Erkenntnis, dass Unternehmen die Überprüfung der Compliance nicht mehr als Nebensache verstehen dürfen, die einmal im Jahr, wie eine Übung, durchgeführt wird. Wirtschaftsprüfer verstehen das zunehmend und suchen daher nach Möglichkeiten, um die Konformität aufrechtzuerhalten. Sie suchen Lösungen zur Auditierung, die zudem eine Warnung ausgeben, wenn eine Veränderung im Netzwerk stattfindet, welche sich auf die Compliance auswirkt.

Besonders hier setzen Security-Automatisierungen an, die sich um die Verwaltung und Änderung von Sicherheitsrichtlinien kümmern und diese Anforderungen erfüllen können. Die neue Netzwerklandschaft hat außerdem den Effekt, dass die Anwendungseigentümer eine sehr genaue Vorstellung davon bekommen, wie hoch das Risiko ist, das von ihren Anwendungen für die Unternehmensumgebung ausgeht. Sie werden somit in die Lage versetzt, mehr Verantwortung für die geschäftlichen Auswirkungen der von ihnen gewünschten Änderungen zu übernehmen und diese genauer prüfen zu können. Das heißt nicht, dass die Anwendungseigentümer plötzlich für die Sicherheit ihrer Anwendungen zuständig sind – sondern sie bekommen ein besseres Gefühl dafür, wie sich eine bestimmte Anwendungen auf die Bedrohungslage des Unternehmen auswirkt.

Beschleunigung von Änderungen

Unsere Diskussion brachte uns auf das Thema ‚Zero-Touch Security Automation'. Im Einklang mit einer Bereinigung der Sicherheitsregeln in einem typischen Netzwerk und dem Fokus auf kontinuierlicher Einhaltung der Compliance, ist die Zero-Touch-Sicherheit unerlässlich. Sie sorgt dafür, dass Unternehmen sicher und agil bleiben können, während ihre Netzwerke komplexer werden und sich schnell verändern.

All dies fällt zusammengefasst unter das seit langem bestehende Sicherheitsprinzip des ‚geringsten privilegierten Zugriffs'. Eigentlich ist die Idee nicht neu, denn sie besagt lediglich, dass nur Anwendungen, die wirklich miteinander reden müssen, über das Netzwerk verbunden werden sollten. Wenn Netzwerke jedoch wachsen und komplexer werden, und sich mit der Zeit organisch verändern, bleibt dieses Prinzip häufig auf der Strecke – und mit ihr die Kontrolle durch die IT-Abteilungen.

Um diese wiederzuerlangen, müssen Unternehmen in der Lage sein, sämtliche Verbindungen innerhalb ihrer IT-Umgebung zu kontrollieren. Dabei hilft eine Security-Automatisierung enorm, die den Mitarbeitern viele manuelle Prozesse, die nur umständlich zu bewältigen sind, abnimmt, damit jene sich auf die wirklich wichtigen Aufgaben der Absicherung des Unternehmens konzentrieren können.

Kyle Wickert

Kyle Wickert, Worldwide strategic architect, AlgoSec

IT-Security als Designkriterium für Software aus der Cloud

Cloud-Anwendungen sind aus deutschen Unternehmen mittlerweile nicht mehr wegzudenken. Laut aktuellem Cloud-Monitor von Bitkom und KPMG setzen derzeit bereits 73 Prozent aller Unternehmen in Deutschland auf Cloud-basierte Rechenleistung. Bei der Wahl des für sie passenden Anbieters ist ihnen das Thema Sicherheit besonders wichtig. Bestehen native Cloud-Anwendungen aber aus verteilten Mikroservices, sind klassische Security-Konzepte in diesem Zusammenhang nicht länger ausreichend. Einer der Gründe hierfür ist, dass im Vergleich zu vor Ort installierten Software-Lösungen klassische Firewalls keinen ausreichenden Schutz mehr bieten, da es in diesem Fall kein klar lokalisierbares Davor oder Dahinter gibt. In jeder segmentierten Cloud-Umgebung ist es daher notwendig, wirksame Security-Mechanismen bereits in jedem kleinsten Cloud-Bestandteil selbst zu verankern. Die Sicherheit eines IT-Systems lässt sich

Oliver Henrich, Vice President Product Engineering Central Europe, Sage

bei dieser Art von Architektur damit nicht länger im Nachhinein realisieren. Der Schutz der Software-Anwendung muss daher als integraler Bestandteil des Systemdesigns von Anfang an im Entwicklungsprozess miteingeplant werden und alle Ebenen und Bestandteile der Cloud-Anwendungsarchitektur umfassen.

Identity- und Access Management sowie stete Kontrolle als zentraler Grundpfeiler

Identitätsnachweise sowie Mechanismen zur Identitätsüberprüfung, auch bekannt als Authentisierung und Authentifizierung, erfordern in verteilten Cloud-Szenarien einen anwendungs- und plattformübergreifenden Ansatz. Für Software-Anbieter, die auch native Cloud-Systeme im Portfolio haben und diese etwa über eine eigene Plattform zur Verfügung stellen, empfiehlt es sich, ein eigenes Identitätsmanagement zu implementieren. Wenn diese Plattform beispielsweise in der Microsoft Azure Cloud betrieben wird, werden Rollen und Zugriffsrechte aus dem Azure Active Directory importiert. Als technologische Basis für ein plattformeigenes Identitätsmanagement bietet sich Auth0 aufgrund seiner Multiproviderfähigkeit an. Theoretisch könnten sich User künftig also auch mit einer Bank-ID in Buchhaltungs- oder Warenwirtschaftsmodule einloggen.

Neben robustem Zugriffsschutz durch ein plattformweites Identity- und Access-Management zählt das Thema Transparenz zu den tragenden Säulen eines jeden ganzheitlichen Cloud-Security-Konzepts. Denn die große Stärke einer Cloud, nämlich die Verarbeitung dynamisch wechselnder Work-Loads, bringt auf der anderen Seite die Notwendigkeit mit sich, diese oftmals weiträumig verteilten Work-Loads permanent zu überwachen. Folglich müssen Monitoring-Funktionen über alle Anwendungen, Services und Architekturebenen hinweg tief in der Cloud-Infrastruktur integriert sein – was sich zum Beispiel mit den erprobten Tools aus dem Azure Security Center realisieren lässt.

End-to-End-Verschlüsselung unterstützt Datensicherheit

Hinsichtlich der wichtigen Themen Datenschutz und Informationssicherheit ist es empfehlenswert, auf eine durchgängige End-to-End-Verschlüsselung zu setzen. Hierbei sind zwei verschiedene Szenarien für den aus- und eingehenden Datenverkehr in Cloud-Rechenzentren zu unterscheiden: Für die Clientkommunikation mit dem Server via Internet, etwa bei der Nutzung von OneDrive for Business, kommen ausschließlich SSL/TLS-Verbindungen mit 2048-Bit-Verschlüsselung zum Einsatz. Das zweite Szenario betrifft Datenbewegungen zwischen zwei oder mehreren Rechenzentren, um die Datensicherheit durch Georedundanz zu maximieren. Egal, ob klassische SQL-Server-Transaktion oder BLOB-Deltas für Multi-Target-Anwendungen – Datenströme dieser Art sollten gehärtet durch eine zusätzliche Verschlüsselung und ausschließlich über ein privates Netzwerk transportiert werden. Darüber hinaus garantieren SSL-Zertifikate die Echtheit von Quelle und Ziel des verschlüsselten Datentransfers.

Mosaikartig zusammengesetzte Cloud-Anwendungen, deren Servicebausteine auf ganz verschiedenen, geografisch mitunter weiträumig verteilten Servern laufen, sind in besonderer Weise anfällig für DDoS-Angriffe: Wenn es Cyberkriminellen gelänge, nur einen dieser Server zum Beispiel per IP-Stressing in die Knie zu zwingen, können fehlende Dienste eine komplette Cloud-Anwendung lahmlegen. Genauso wie das Monitoring sollten daher auch unterschiedliche DDoS-Schutzvorkehrungen schon auf der Ebene der Serviceinfrastruktur implementiert sein. Eine Möglichkeit sind beispielsweise selbstlernende DDoS-Protection-Services für die fortlaufende Überwachung und Untersuchung des gesamten Datenverkehrs. Die zugrundeliegenden Algorithmen decken verdächtige Verkehrsmuster und andere Indikatoren auf, die auf einen möglicherweise bevorstehenden DDoS-Angriff hindeuten.

Architekturansätze für den Einsatz von Mikroservices

Im Kontext der Bereitstellung Cloud-basierter Services spielt auch die Frage nach den Architekturansätzen für den Einsatz von Mikroservices eine Rolle. Entscheidend ist in diesem Zusammenhang auch, welchen Hosting-Provider der Anbieter für seine Cloud-basierten Services gewählt hat. Im Fall der Microsoft Azure Cloud kann er beispielsweise seine Anwendungen als Docker Container innerhalb der Azure Kubernetes Service-Umgebung (AKS) laufen lassen. Diese Plattform bringt zwei bewährte Architekturansätze für den Einsatz von Mikroservices zusammen, nämlich serverlose Dienste als Function-as-a-Service sowie Container mit zugehöriger Orchestrierung. AKS ermöglicht die effiziente Verwaltung von Anwendungen auf Containerbasis inklusive aller involvierten Speicher- und Netzwerkkomponenten. Und zwar aus der Perspektive der Work-Loads – also weitgehend unabhängig von der zugrundeliegenden Infrastruktur.

AKS-Dienste basieren generell auf unabhängigen Prozessen, die via APIs mit einem sogenannten ETCD-Cluster kommunizieren. Zur API-Authentifizierung können solche Cluster wahlweise LDAP-Server, digitale Zertifikate, statische Token oder das Auth0-Protokoll OpenID-Connect (OICD) verwenden. Darüber hinaus bietet Kubernetes ein integriertes Tool zur rollenbasierten Zugriffskontrolle (RBAC) von API-Servern, womit sich individuelle Schreib- und Leserechte von Pods und darin enthaltenen Containern präzise steuern lassen. An dieser Stelle wird deutlich, inwiefern das Security-by-Design-Prinzip gleichsam als DNA in AKS verankert ist.

Designprinzip Sicherheit

Die Verlagerung von On-Premise-Work-Loads in die Cloud verlangt ein grundlegend neues Entwicklungsparadigma, das bei der Entwicklung jedes einzelnen Servicebestandteils verteilter Anwendungen IT-Security als Designprinzip zugrunde legt. Außerdem aber muss selbstverständlich auch die physische Plattform gegen Cyberangriffe abgesichert sein. Bei der Beurteilung der Frage, inwieweit dies für eine konkrete Lösung zutrifft, können sich Unternehmen an Zertifikaten wie FISMA, ISO und SOC orientieren.

Oliver Henrich

SASE - Wie Sicherheit am Edge den Unterschied macht

Nathan Howe, Director Strategic Transformation EMEA, Zscaler

New Work und Cloud Computing gestalten die Arbeitswelt völlig um. Um diese Transformation erfolgreich zu bewältigen, muss auch die Internet-Sicherheit für die zunehmend mobilen Mitarbeiter neu gedacht werden. Folgt man dem SASE-Framework von Gartner, muss sich die Sicherheit aus dem Netzwerk ans Edge und damit zum Mitarbeiter verlagern.

Moderne digitale Geschäftsmodelle schaffen neue Möglichkeiten für die flexible Einbindung von Kunden und Mitarbeitern in den Arbeitsalltag. Längst sind es nicht mehr nur Road Warriors und digitale Nomaden, die die Agilität des mobilen Zugriffs auf die Büro-Anwendungen in der Cloud zu schätzen wissen. Pandemien, Wetterverhältnisse mit Stürmen und Überschwemmungen, Generalstreiks oder Buschfeuer verschaffen dem Home Office-Konzept ganz neue Argumente und tragen zur Popularität des grenzenlosen Arbeitsplatzes bei.

Damit Unternehmen diese neuen Arbeitsmodelle unterstützen können, müssen sie jedoch einen weltweit verfügbaren und abgesicherten Zugriff zu Anwendungen für ihre Mitarbeiter bereitstellen. Oberste Prämisse ist, dass der Anwendungszugriff für den Mitarbeitersicher und ohne Hürden oder Umwege gestaltet ist. Unabhängig von welchem Standort der mobile User auf Applikationen im Netzwerk oder in Multicloud-Umgebungen zugreifen möchte, muss Sicherheit und Geschwindigkeit an erster Stelle stehen. Hier geraten traditionelle Netzwerkarchitekturen an ihre Grenzen. Eine Genese von der Netzwerk-zentrierten zur Anwender-zentrierten IT-Infrastruktur ist erforderlich in dessen Zuge Netzwerkarchitektur- und Sicherheitsanforderungen neu ausgerichtet werden müssen.

Neue Anforderungen an Arbeitsumgebungen

Eine IT Abteilung muss sich dazu auf neue Anforderungen einlassen. Daten sind über Cloud-Anwendungen und verschiedene Cloud Provider sowie auf das Netzwerk verteilt und Anwender arbeiten von überall aus. Die Migration der geschäftskritischen Systeme in die Cloud erzwingt ein Umdenken, wie Mitarbeiter auf die Services zugreifen können. Angesichts der Allgegenwart günstiger Internetverbindung ändert sich die Erwartungshaltung der Mitarbeiter an die Zugriffsgeschwindigkeit und auch an den Komfort des grenzenlosen Zugangs zu Anwendungen. Wird das Internet zum neuen Unternehmensnetz steigt für Mitarbeiter allerdings auch das Gefahrenpotenzial durch die sich ständig verändernde Cyberkriminalität. Die größte Umstellung für die IT-Sicherheit ist die durch die Transformation einhergehende Umstellung von der Kontrollinstanz hin zur Risikominimierung.

Solange Anwendungen im Rechenzentrum vorgehalten wurden, war die IT mit der Bereitstellung der Anwendungen betraut und hatte die Kontrolle. Verlassen die Anwendungen das Rechenzentrum und die Anwender das Netzwerk, verlagert sich die Verantwortung. Es geht nicht mehr nur um die Absicherung des Netzwerks durch Sicherheitsinfrastruktur am Perimeter und die Verwaltung der Hardware. Heute ist der sichere Zugriff auf Applikationen in komplexen Cloud-Szenarien erforderlich. In der Cloud-basierten Welt muss anstelle der separat betrachteten Netzwerke und Sicherheit ein übergreifendes Gefüge aus Netzwerk, Sicherheit und Connectivity treten, das den reibungslosen und sicheren Zugriff auf Anwendungen ermöglicht, unabhängig davon, wo diese vorgehalten werden. Denn nichts wäre dem Anwender weniger vermittelbar, als wenn die Zugriffsgeschwindigkeit durch die Cloud, die Agilität und Flexibilität bieten soll, für den Einzelnen leidet.

Abgeleitet aus diesen Anforderungen wurde das Secure Access Service Edge (SASE) entwickelt, es kombiniert umfassende WAN-Fähigkeiten mit zahlreichen Netzwerksicherheitsfunktionen (wie SWG, CASB, FWaaS und ZTNA) um die dynamischen, sicheren Zugangsanforderungen von Unternehmen zu unterstützen.

Sicherheit wandert aus dem Netzwerk hin zum Anwender

Anstatt ein traditionelles Konzept zur Lösung eines modernen Problems zu verwenden, dreht SASE das Sicherheitsmodell einfach um. Während sich sogenannte Legacy-Ansätze darauf konzentrierten Anwendungen innerhalb des Netzwerks mit einem Perimeter zu umgrenzen, konzentriert sich SASE auf den User, und die Sicherheit auf dem Weg zu seinen Anwendungen, die in privaten und public Multicloud-Umgebungen sowie im Netzwerk vorgehalten werden. Das Rahmenwerk sieht vor, dass der Datenverkehr während des gesamten Weges von einem Anwender zu seiner Anwendung gesichert wird – unabhängig davon, wo sich der Benutzer gerade aufhält, oder wo die Anwendung vorgehalten wird. Der entscheidende Punkt dabei ist, dass der Begriff ‚Edge' beschreibt, worauf

der Anwender zugreifen möchte und nicht, wo er sich befindet. So wird jederzeit Sicherheit ermöglicht und nicht mehr nur im Netzwerk oder auf einem Endgerät des Anwenders.

Eine solche Sicherheitsfunktion kann durch eine Transit-Cloud zur Verfügung gestellt werden, die den Weg der Anfrage eines Anwenders zu seiner Anwendung überwacht. Eine Cloud Security Plattform ist also ein Bestandteil eines SASE-Konzepts, denn darüber werden die Sicherheits-Policies für den Datenverkehr zwischen Anwender und seiner Applikation ausgeführt. Die Sicherheitsfunktionalität befindet sich dann nicht mehr an einem physischen Standort, sondern in der Cloud, wo die Filter und Richtlinien in Echtzeit im ein- und ausgehenden Datenverkehr zwischen User und Anwender wirken können und ständig aktiviert sind. Der moderne Weg zur Risikominimierung ist demnach nicht mehr die Aufgabe netzwerkbasierter Konnektivität, sondern stattdessen Benutzer über einen Zero-Trust-Netzwerkzugang (Zero Trust Network Access, ZTNA) mit Anwendungen zu verbinden. ZTNA stellt sicher, dass nur Benutzer, die zum Zugriff auf eine Anwendung berechtigt sind, diesen erhalten. Die Berechtigung wird über Richtlinien festgelegt, die in der Security Cloud umgesetzt werden. So wird eine Microsegmentierung auf Ebene der einzelnen Anwendung möglich, und der Zugriff auf das gesamte Netzwerk gehört in einem solchen Rahmenwerk der Vergangenheit an.

Benutzererfahrung im Mittelpunkt

Bislang waren die Benutzer innerhalb des Firmennetzwerks tätig und die Anwendungen, auf die sie zugriffen, lagen im Rechenzentrum; Server und IT-Infrastruktur gehörten zur IT-Abteilung. In diesem Modell ist es einfach, die Benutzererfahrung zu kontrollieren. Heute liegen die Anwendungen und Daten jedoch in mehreren Cloud-Umgebungen verteilt und werden auf dem herkömmlichen Weg über VPN-Verbindungen aufgerufen. Dieser Pfad geht allerdings wieder mit dem Umweg über das Rechenzentrum einher und verlängert damit den Weg des Users zur Anwendung.

Das SASE-Rahmenwerk bezieht für die direkt Anbindung ans Internet von jeder Niederlassung deshalb weitere Komponenten für die Konnektivität, wie SD-WAN-Lösungen mit ein. Direktes Ausbrechen von jedem Unternehmensstandort spart Umwege und profitiert wiederum von einem Cloud-basierten Sicherheitskonzept. Um niedrige Latenzzeiten zu gewährleiten und den Anwender auf dem direkten Weg mit seiner Anwendung zu verbinden können außerdem Peering-Points zwischen Cloud-Anbietern und Cloud Service Providern beitragen.

Das SASE-Framework eignet sich hervorragend zur Bewältigung der Herausforderungen des sogenannten New-Work-Modells und der zunehmend vernetzten, sich wandelnden Arbeitswelt. Neben einer schnelleren Bereitstellung und besseren Nutzung von Cloud-Diensten profitieren Unternehmen auch von größerer IT-Sicherheit bei reduzierten Kosten, weniger Komplexität, geringerem Verwaltungsaufwand und zentraler Durchsetzung neuer Richtlinien auf allen Systemen. Die IT Abteilung kann damit nicht nur ein sicheres und schnelles Anwendererlebnis anbieten, sie erhält über eine Cloud-Plattform auch wieder den Einblick in alle Datenströme zurück und kann damit das Internet als neues Unternehmensnetz kontrollieren, auch wenn die Mitarbeiter mobil arbeiten.

Nathan Howe

360°-Cloud-Sicherheit mit dem Shared Responsibility Model

Unternehmen profitieren auf vielerlei Weisen von Cloud Computing: es macht nicht nur Mitarbeiter, sondern auch Geschäftsprozesse produktiver, effizienter und flexibler. Doch halten damit auch sicherheitsrelevante Herausforderungen Einzug in das Unternehmensnetzwerk, die es zu meistern gilt. Rolf Haas, Senior Enterprise Technology Specialist bei McAfee, stellt im folgenden Fachbeitrag das 360° Shared Responsibility Model vor und erklärt, warum es für Provider, Unternehmen und Anwender gleichermaßen wichtig ist, an einem Strang zu ziehen, wenn es um die Sicherheit in der Cloud geht.

Sicherheit ist keine Sache von Einzelgängern. Die Gewährleistung von sicheren Umgebungen sollte nicht nur in den Händen einer einzelnen Partei liegen. Vielmehr sollte die gesamte Verantwortung unter sämtlichen involvierten Akteuren aufgeteilt werden. Betrachtet man beispielsweise den Kontext einer Autovermietung – vom Werk bis hin zum Mieter – wird klar, wie wichtig es ist, dass jede Instanz ihren Beitrag zum Sicherheitsniveau kennt und leistet:

Der Autohersteller muss dafür sorgen, dass sein Wagen fahrtauglich und sicher ist – Bremsen und Airbags müssen demnach den vorgegebenen Sicherheitsstandards entsprechen. Das Unternehmen, das den Wagen vermietet, kann dies nicht beeinflussen, sondern trägt an anderer Stelle seine ganz eigene Verantwortung. Es muss sicherstellen, dass einzelne Komponenten des Wagens regelmäßig auf Verschleiß und Funktionsfähigkeit geprüft werden. Außerdem muss der Vermieter darauf achten, dass seine Kundschaft die rechtlichen Anforderungen erfüllt, um einen Wagen mieten und fahren zu dürfen. Zwar stellt der Hersteller ab Werk eingebaute Sicherheitsgurte zur Verfügung, doch liegt es beim Fahrer selbst, diese während der Fahrt anzulegen und sich gemäß den Vorgaben der StVO zu verhalten – auf diese beiden Aspekte haben nämlich weder Hersteller noch Vermieter irgendeinen Einfluss.

Wie in diesem Beispiel mit der Sicherheit im Rahmen einer Autovermietung, verhält es sich mit der Sicherheit in der Cloud. Auch hier entstehen Schwachstellen und Sicherheitslücken, sobald eine Partei ihrer Verantwortung nicht nachkommt. Datenlecks, Compliance-Verstöße, damit verbundene Bußgelder und Reputationsschäden sind nur einige gefährliche Folgen einer solchen Fahrlässigkeit. Mithilfe des 360° Shared Responsibility Models wird diesem Problem entgegengewirkt: Es sieht die gleichwertige Aufteilung aller Verantwortungsbereiche in der Cloud vor und bindet ebenso sämtliche Akteure mit ein – vom Provider über die beziehenden Unternehmen bis hin zu jedem einzelnen Cloud-Nutzer.

Stolpersteine, die die Cloud-Sicherheit gefährden

Im Rahmen einer Umfrage im Oktober 2019, die unter IT-Leitern und -Angestellten durchgeführt wurde, stellte McAfee fest, dass über 90 Prozent der befragten IT-Leiter ihr Unternehmen als „Cloud first" beschreibt – also als sehr stark auf Cloud Computing ausgerichtet. Die eingangs beschriebenen Vorteile stellen einige wichtige Gründe dar, warum sich immer mehr Unternehmen für den Einsatz von Cloud-Technologien entscheiden. Zudem machen die Offenheit gegenüber Markt-Expansion und kürzere Produkteinführungszeiten die Cloud zu einer gewinnbringenden Ergänzung zu traditionellen, lokalen Netzwerken. Ein Großteil der befragten IT-Leiter verbindet sie darüber hinaus mit einem erhöhten Sicherheitsniveau, da sie davon ausgehen, dass Provider bereits von Anfang an für den Schutz ihrer Kunden sorgen. Doch der Schein trügt, denn das Angebot der Provider deckt nicht alle Elemente und Dienste automatisch ab.

Eines der größten Sicherheitsrisiken, welches nur sehr begrenzt in den Wirkungsbereich der Provider fällt, ist die Menge an sensiblen und unternehmenskritischen Daten, die auf Cloud Servern gespeichert und – meist mittels ungeschützten Cloud-Verlinkungen – versendet wird. Rund 21 Prozent nehmen Daten dieser Art laut des Cloud Adoption and Risk Reports von McAfee auf Cloud Servern insgesamt ein. Und die Tendenz steigt: 61 Prozent der befragten IT-Leiter schätzt, dass über die Hälfte der Daten aus sensiblen Inhalten bestehen, die sich innerhalb ihrer Unternehmens-Cloud-Anwendungen bewegen. 96 Prozent planen sogar, zukünftig sogar noch mehr dieser Inhalte in der Cloud zu lagern.

Für Cyber-Kriminelle ist dies ein gefundenes Fressen: Sie kennen die Schlupflöcher, die durch Vernachlässigung der Sicherheit in Form der sogenannten Schatten-IT oder von unvorsichtigen Mitarbeitern entstehen, die beispielsweise infizierte E-Mail-Anhänge öffnen. Durch sie verschaffen sie sich Zugang zu den Unternehmensnetzwerken – sowohl lokal als auch zur Cloud. In solchen Fällen wird offensichtlich, dass sich Unternehmen nicht einzig und allein auf Cloud Provider verlassen können, sondern erkennen müssen, dass sie selbst einen Teil der Verantwortung über den Schutz ihrer IT-Landschaft und ihrer Daten mithilfe eines Shared-Responsibility-Ansatzes übernehmen müssen.

360° Shared Responsibility: Einmal das volle Programm, bitte

IT-Verantwortliche fungieren als Schnittstelle zwischen der IT-Landschaft und dem Rest des Unternehmens und sind für die Einhaltung der Compliance zuständig. Deshalb ist es umso wichtiger, dass sie nicht nur wissen, wo sich mögliche Lücken ergeben könnten, sondern auch, wem welche Art von Sicherheitsverantwortung zukommt.

Die Hauptverantwortung der Provider verteilt sich primär auf zwei Bereiche: zum einen der Schutz von Komponenten – wie Verkabelung, Datenspeicher und Server – vor physischen Schäden und schädlichen Eingriffen, zum anderen die Absicherung der Netzwerk- und Hosting-Infrastruktur. Zu letzterem zählen vor allem Rechenzentren, Server-Hardware und Netzwerk-Konnektivität. Eine Vernachlässigung dieses Aspekts führt nicht nur dazu, dass die Kommunikation zwischen einzelnen Cloud-Diensten leidet, sondern ebenso zu Schwachstellen, die Cyber-Kriminelle zum Beispiel mittels DDoS-Attacken (Distributen Denial-of-Service) gezielt ausnutzen können.

Die Kunden der Provider – sprich: Unternehmen, die Cloud-Technologie in ihre IT-Landschaft integrieren – sind verantwortlich für die Funktionalität einzelner Applikationen, deren Schutz vor Bedrohungen sowie für das Identity und Access Management (IAM). Über die Vergabe von Nutzungsprivilegien regeln sie, welche Mitarbeiter welche Bereiche der Cloud betreten und welche Daten sie herunter- oder hochladen dürfen. Hierfür müssen sie Tools zur Verfügung stellen, mit der die IT-Mitarbeiter Zugangsbefugnisse prüfen, vergeben, blockieren und überwachen können. Ebenso braucht die IT-Abteilung Lösungen, mithilfe derer sie sämtliche Geräte verwalten können, die dazu autorisiert sind, sich mit dem Netzwerk zu verbinden – egal, ob aus dem Büro oder dem Home Office.

Wie der Fahrer des Mietautos auf Regeln im Straßenverkehr und einen sicheren Fahrstil samt Sicherheitsgut achten muss, ist jeder einzelne Anwender im Unternehmen für eine „sichere Fahrweise" in der Cloud verantwortlich. Da die Daten in der Cloud ständig in Bewegung sind durch Download, Upload und Versand, gilt es sämtliche Geräte wie Laptops und Smartphones abzusichern, die Zugang zum Netzwerk haben. Außerdem spricht das Shared Responsibility Model die Problematik von unvorsichtigen Mitarbeitern direkt an. Diese werden dazu aufgerufen, Daten achtsamer zu nutzen. Über Schulungen, die das Unternehmen organisiert, sollen sie lernen, ein erhöhtes Sicherheitsbewusstsein zu entwickeln.

Fazit

Sobald im Rahmen der Autovermietung eine Sicher-

Rolf Haas, Senior Enterprise Technology Specialist, McAfee

heitslücke entsteht, weil sich niemand für seinen Bereich für verantwortlich hält, kann es tragisch enden. Im Falle der Cloud stehen IT-Landschaft, unternehmenskritische Dokumente und sensible, persönliche Daten sowie Geschäftsergebnisse und -reputation auf dem Spiel. Das 360° Shared Responsibility Model soll sicherstellen, dass sämtliche Akteure ihre Verantwortung im Rahmen der Cloud-Sicherheit kennen, diese wahrnehmen und folglich alle Akteure an einem Strang ziehen. Denn sicher lässt es sich am besten „fahren".

Rolf Haas

Bei der Zusammenarbeit die Sicherheit nicht vergessen: Wie man Collaboration-Tools sicher einsetzt

Mit dem Homeoffice kam die Collaboration: Um die Produktivität und Zusammenarbeit auch bei verstreuten Mitarbeitern zu gewährleisten, setzen Unternehmen verstärkt auf Kollaborationslösungen wie Slack oder Microsoft Teams. So hat sich nach Angaben von Microsoft die tägliche Nutzung von Microsoft Teams im Zeitraum von November 2019 bis März 2020 von 20 Millionen auf 44 Millionen Benutzer mehr als verdoppelt. Und auch bei der Slack-Nutzung sieht es ganz ähnlich aus. Doch mit dieser sprunghaften Verbreitung steigen auch die Risiken für die Cybersicherheit, die nun dringend adressiert werden müssen.

Im Hinblick auf den sicheren Einsatz der Collaboration-Tools sollten Unternehmen vor allem drei Aspekte ins Blickfeld nehmen:

Zugangskontrolle:

- Es muss sichergestellt werden, dass die Nutzer Zugriff auf zugelassene Anwendungen haben, während der Zugriff auf nicht zugelassene Applikationen und Instanzen kontrolliert wird.
- Die Anwendungen müssen so konfiguriert sein, dass sie die erforderlichen Funktionen zur Einhaltung der Unternehmensrichtlinien (etwa in Hinblick auf Compliance-Anforderungen oder Archivierung) nutzen.
- Richtlinien für die Verwendung privater Geräte (BYOD) müssen erstellt und durchgesetzt werden. So kann der Zugriff über solche Geräte grundsätzlich blockiert oder aber ein (eingeschränkter) Zugriff mit spezifischen Kontrollen zum Schutz der Daten zugelassen werden.
- Für den Zugriff durch Dritte, also beispielsweise autorisierte Partner, sollten strenge Regeln gelten, während ein Gastzugriff auf Collaboration-Nachrichten und -Dateien blockiert werden sollte.

Thomas Ehrlich, Country Manager DACH, Netskope Germany

Datensicherheit

- Es muss sichergestellt werden, dass Daten nicht versehentlich oder absichtlich mit anderen Nutzern, etwa globalen Nutzergruppen, ausgetauscht werden. Sämtliche Berechtigungen müssen auf bestimmte, genau definierte Nutzer und Gruppen beschränkt werden.
- Die Kollaborationslösung muss die Verschlüsselung ordnungsgemäß und in Übereinstimmung mit den Richtlinien des Unternehmens einsetzen.
- Besonders wichtig ist die Identifizierung sensibler Daten, die in den Collaboration-Anwendungen gespeichert sind, basierend auf für das Unternehmen und/oder die Branche relevanten Kriterien.
- Sämtliche Sicherheitsmaßnahmen müssen sich sowohl für innerhalb der Kollaborationsplattform oder des Cloud-Speichers abgelegte Daten (also Daten im Ruhezustand) als auch für Daten in Bewegung gelten.

Schutz vor Malware

- Inhalte müssen sowohl in den Kanälen der Anwendung als auch in direkten Person-zu-Person-Nachrichten auf Malware untersucht werden.
- Ebenso muss der Bedrohungsschutz sowohl inline (zum Echtzeitschutz von Inhalten) als auch durch Scannen nach in der Anwendung gespeicherter Malware sichergestellt werden.

Statische und dynamische Daten

Daten in der Cloud kann man grundsätzlich in zwei unterschiedliche Kategorien aufteilen: Zum einen die innerhalb der Kollaborationsplattform oder des Cloud-Speichers gespeicherten, abgelegten Daten (data at rest), zum anderen Daten, die in Bewegung sind (data in motion). Um die abgelegten Daten wirkungsvoll zu schützen, benötigen Sicherheitsverantwortliche eine tiefgreifende Transparenz und einen umfassenden Überblick über die Kollaborationsplattformen und eine präzise Bewertung des Sicherheitsstatus bei der gemeinsamen Nutzung von Daten. Diese muss sich über die Kollaborationslösung und die angeschlossenen Cloud-Speicher erstrecken. Um die Daten wirkungsvoll zu schützen sowie effektive Data Loss Prevention (DLP) umzusetzen und damit Datendiebstähle zu verhindern, müssen sämtliche Dateien sowohl in privaten und öffentlichen Teams oder Kanälen als auch in privaten Nachrichten auf sensible Inhalte gescannt werden. Dabei kommen folgende Kriterien in Betracht:

- PCI-Daten, also Zahlungs- und Bankinformationen wie Kreditkarten- oder Kontonummern
- Personenbezogene Daten wie Ausweisnummern, Adressen oder Geburtsdaten
- Vertrauliche Unternehmensdaten, die entweder mit einem Datenklassifizierungstool explizit klassifiziert oder mit einer leistungsstarken und flexiblen Datenidentifizierungsbibliothek dynamisch erkannt werden
- Sensible und vertrauliche Daten mit speziellem Wert für das Unternehmen, also etwa in Bezug auf geistiges Eigentum und proprietäre Daten

Nach einer Klassifizierung der Daten müssen entsprechende (abgestufte) Richtlinien zum Schutz vertraulicher Daten eingerichtet und vor allem auch durchgesetzt werden. So kann etwa bei sensiblen Daten eine gemeinsame Nutzung mit Mitgliedern einer bestimmten Gruppe erlaubt sein, ein Teilen mit anderen Gruppen oder externen Partnern jedoch nicht.

Die Cloud zeichnet sich durch eine enorme Dynamik auch und insbesondere bei der Nutzung von Daten aus. Insofern muss auch der Inline-Schutz zu jeder Zeit gewährleistet sein. Der Cloud & Threat Report 2020 hat gezeigt, dass ein Fünftel der Benutzer Daten lateral zwischen Cloud-Anwendungen bewegt und beispielsweise Dokumente von OneDrive auf Google Drive kopiert oder sie über Slack teilt. Die Daten überschreiten dabei mehrere Grenzen: Sie bewegen sich zwischen Cloud-App-Suites, zwischen verwalteten und nicht verwalteten Anwendungen, zwischen unterschiedlichen App-Kategorien und zwischen den unterschiedlichen Anwendungs-Risikostufen. Entsprechend muss ein wirkungsvoller Schutz den Zugriff auf Anwendungen identifizieren und Instanz-bezogene Richtlinien durchsetzen können, damit die Daten auch dort verbleiben, wo sie hingehören. Dabei können verschiedene Ansätze verfolgt werden: So lassen sich beispielsweise grundsätzlich Anmeldungen bei nicht autorisierten Instanzen von Cloud SaaS-Anwendungen verbieten. Dadurch wird sichergestellt, dass die Benutzer nur die genehmigte Anwendungsinstanz verwenden und nicht auf nicht autorisierte Instanzen (etwa das private Dropbox-Konto) zugreifen können. Ein alternativer Ansatz besteht darin, eine Richtlinie zu verwenden, die es den Benutzern erlaubt, sich bei jeder Instanz der Anwendung anzumelden, während gleichzeitig DLP-Profile zum Schutz der Daten durchgesetzt werden. Dieser Ansatz verhindert, dass sensiblen Unternehmensdateien in eine nicht zugelassene Instanz der Kollaborationsanwendung hochgeladen werden. Darüber hinaus schützt dieselbe Richtlinie Daten, wenn ein Benutzer versehentlich oder absichtlich versucht, sie von seinem Endpunkt in riskante File-Sharing-Anwendungen wie WeTransfer, persönliche Cloud-Speicheranwendungen wie Dropbox oder über einen E-Mail-Dienst (wie das persönliche Google Mail-Konto) zu exfiltrieren.

Gerade im Homeoffice werden oftmals private, also nicht von der IT-Abteilung gemanagte Rechner verwendet. Sicherheitsverantwortliche sollten dann in der Lage sein, die Verwendung dieser Geräte zu kontrollieren und zu steuern, wie sie auf die zugelassenen Cloud-Collaboration-Anwendungen wie Slack oder Microsoft Teams zugreifen. Dies kann durch die Integration einer Identitätsmanagement-Lösung (z. B. Okta) erreicht werden. Auf diese Weise kann man separate Zugriffs- und DLP-Richtlinien auf Benutzer mit nicht verwalteten Geräten anwenden und verhindern, dass sie sensible oder proprietäre Daten herunterladen.

Tools für die Zusammenarbeit sind gerade im Homeoffice unerlässlich und bieten zahlreiche Vorteile. Allerdings darf deren Einsatz nicht auf Kosten der Sicherheit gehen. Nur wenn man beides verbindet, lässt sich der volle Nutzen realisieren. Entsprechend müssen sich Unternehmen der Risiken (etwa im Hinblick auf Zugriffsrechte, Datenschutz und Malware) bewusst sein und diese gezielt adressieren. Nur so lässt sich der kooperativen Austausch mit anderen Mitarbeitern und Partnern aufrechterhalten und die Betriebskontinuität sicherstellen.

Thomas Ehrlich

1.5 DARK WEB

Digitales Risikomanagement: Was bringt der Blick ins Dark Web?

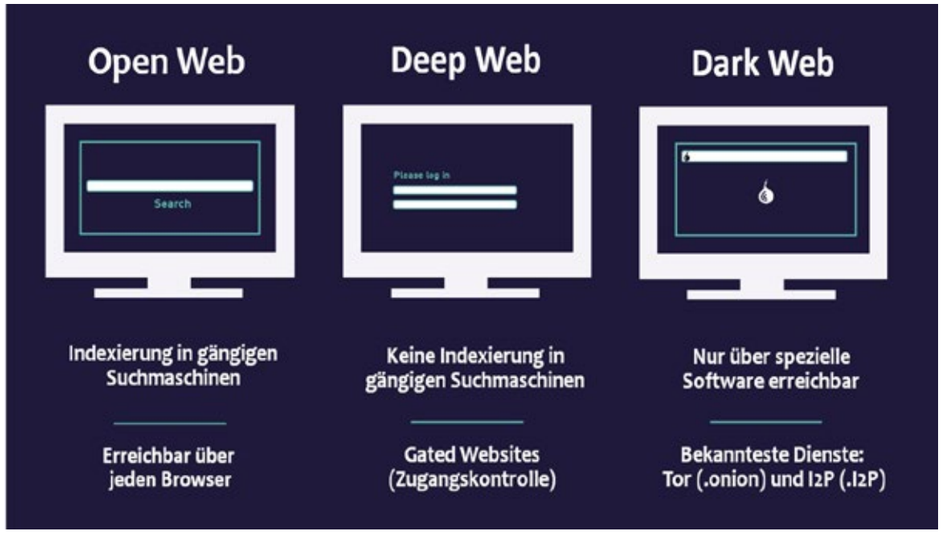
Bedrohlich, verborgen und kriminell. Das Dark Web ist für Kriminelle ein idealer Spielplatz, um mit illegaler Ware zu handeln und Cyberangriffe zu planen. In den dunklen Ecken des Internets hat sich ein komplexes Ökosystem entwickelt, das Ransomware-as-a-Service, Partnerschaften sowie Fortbildungskurse anbietet. Das macht das Dark Web auch für Unternehmen interessant, zum Beispiel wenn es darum geht geleakte Zugangsdaten oder Dokumente zu identifizieren.

Was ist das Dark Web? Zunächst einmal keine Panik. Niemand gelangt beim Surfen im Internet aus Versehen ins Dark Web. Der Zugriff ist nur mit speziellen Tools und Software möglich, d. h. es braucht Know-how und ein klares Ziel. Vielmehr werden Informationen verschlüsselt und der Zugang zu Marktplätzen und Foren unterliegt teilweise strengen Kontrollen. Naturgemäß zieht dieser Ort diejenigen an, deren oberste Priorität Geheimhaltung und Anonymität ist. Darunter fallen logischerweise auch Drogen- und Waffenhändler, Terroristen, Vertreiber von Kinderpornographie und Cyberkriminelle.

Drei Irrtümer über das Dark Web

Dennoch ist es wichtig zu wissen, dass das Dark Web nicht nur für illegale Zwecke genutzt wird. Auch Regimekritiker, Geheimdienste, Whistleblower, verdeckte Ermittler und investigative Journalisten nutzen den Deckmantel der Anonymität. Zudem bieten legitime Unternehmen, wie die New York Times oder Facebook, Tor-basierte Dienste an und veröffentlichen dort Content. Nicht alles, was sich im Dark Web findet, muss daher automatisch kriminell sein.

Ein zweiter häufiger Irrtum: Das Dark Web lässt sich nicht mit dem Deep Web in einen Topf werfen. Tatsächlich ist das Deep Web bis zu 10.000mal größer



als das Open Web und lässt sich mit gewöhnlichen Suchmaschinen wie Google, Yahoo oder Bing nicht abfragen. Auch hier sind gezielte Suchanfragen nötig sowie in der Regel eine zusätzliche Zugriffsberechtigung (z. B. Login). Genutzt wird das Deep Web von Bibliotheken, Museen, Regierungsbehörden, Institutionen und Organisationen, die dort ihre Datenbestände archivieren.

Bei Cyberkriminalität denken viele in erster Linie an einen opportunistischen Einzeltäter, der im Alleingang agiert und nur im Dark Web zu finden ist. In Wirklichkeit steckt jedoch hinter den illegalen Machenschaften von Cyberkriminellen ein komplexes Netzwerk an Dienstleistern und Abnehmern, in dem feste Regeln herrschen und langfristige Ziele verfolgt werden. Das kriminelle Ökosystem schützt sich und versucht mithilfe von Hosting, Counter-Anti-Virus-Diensten und Tools der Strafverfolgung zu entgehen. Dabei entwickeln die Kriminellen stets neue, innovative Wege und bewegen sich auch verstärkt auf Foren und Chat-Kanälen im Open Web.

Stefan Bange , Country Manager DACH , Digital Shadows

E-Learning für die Cyberkriminellen von Morgen

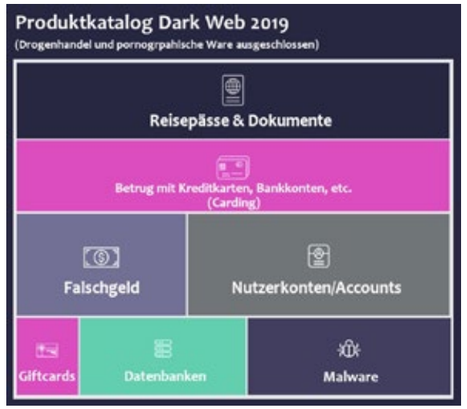
Parallelen zu den Geschäftsstrategien legaler Unternehmen und Start-ups sind dabei kein Zufall. Auch unter Cyberkriminellen ist der Innovationsdruck hoch. Erfahrene Betrüger und Händler von Login-Daten bieten mittlerweile sogar Cybercrime-Kurse an, in denen sie einem interessierten Publikum diverse Techniken beibringen. Diese reichen von Kreditkartenbetrug, der Manipulation von Geldautomaten und Geldwäsche bis zu Social Engineering, Botnets und dem Exploit von Sicherheitslücken.

In der Regel ist die Einführungsveranstaltung bei solchen Lernangeboten kostenlos. Einsteiger können die meist russischen Seminare für 75.000 Rubel (ca. 1.080 Euro) buchen und erhalten damit Zugang zu weiteren E-Learning Kursen, einschließlich Schulungs- und Informationsmaterial sowie den direkten Kontakt zu „Tutoren“. Gezahlt wird in Bitcoins. Für eine Kursgebühr von (umgerechnet) 650 Euro erhalten die Teilnehmer begleitend zum Webinar Schulungs- und Informationsmaterial. Die Anbieter versprechen ein umfassendes Know-how in Sachen Kreditkartenbetrug, mit dem selbst Anfänger zu professionellen Cyberkriminellen aufsteigen. Die Investition in eine solche Ausbildung kann sich durchaus lohnen. Nach erfolgreichem Abschluss des Kurses können die angehenden Hackern bei einer 40-Stunden-Woche mit einem Monatseinkommen von 10.500 Euro rechnen. Für Organisationen und Unternehmen ist das Fortbildungsangebot im Dark Web brandgefährlich, da nun auch Amateure das nötige Training sowie die Tools erhalten, um eine erfolgreiche kriminelle Karriere zu starten.

Schwarze Schafe in der Betrüger-Familie

Die Professionalisierung von Cyberkriminalität zeigt sich unter anderem auch in den teilweise strengen Regeln und Kontrollmechanismen, die sich im Laufe der Zeit auf Marktplätzen, Foren und Webseiten im Dark Web etabliert haben. Ähnlich wie in der legalen Wirtschaft braucht es ein Mindestmaß an Vertrauen, um mit Waren zu handeln und Geschäfte abzuschließen. Marktplätze bieten beispielsweise einen Treuhandservice an, der sowohl Käufern als auch Verkäufer in der undurchsichtigen Welt der Cyberkriminalität ein Stück weit Sicherheit verspricht. Parallel zu den neuen Marktplätzen im Dark Web werden auch verstärkt Messaging-Dienste wie Telegram und Jabber genutzt, um unter anderem die Glaubwürdigkeit von Angeboten zu prüfen.

Trotzdem müssen sich auch Cyberkriminelle vor Betrugsversuchen in Acht nehmen. Dazu gehören beispielsweise falsche Social-Media-Datenleaks, Handel mit ungültigen Kreditkarten oder bezahlte und nicht ausgeführte Hackerdienste. Betrüger in den eigenen Reihen, sogenannte Ripper, sind daher ein gewaltiges Problem für das florierende Geschäft. Ihre Aktivitäten beeinträchtigen den Markt und schmälern den Gewinn sowohl für Anbieter illegaler Dienste und gestohlener Daten als auch für deren Käufer. Die Mehrheit der kriminellen Plattformen beschäftigt sich daher intensiv mit dem Problem. Die Webseite Ripper.cc beispielsweise bietet eine übergreifende Bibliothek, in der Profile vermeintlicher Ripper angelegt werden – einschließlich Informationen zu Kontakt, Identifikation und eingesetzter Betrugsmasche. Über ein Plug-In für Jabber werden Akteure sogar gewarnt, wenn sie mit jemandem aus der Ripper-Datenbank in Kontakt kommen.



Dark Web Monitoring für Unternehmen

Der Blick in die digitale Unterwelt ist nicht nur spannend, sondern kann sich für Unternehmen tatsächlich lohnen und entscheidend zur Cybersicherheit beitragen. Um das Risiko von Angriffen einzuschätzen und entsprechende Maßnahmen zu ergreifen, sollten Unternehmen potentielle Angreifer im Auge behalten, Entwicklungen in der Hacker-Szene verfolgen und aktuelle Tools und Techniken kennen. Was und wer steckt hinter dem Forum, auf dem der Anbieter aktiv ist? Wie ist seine Reputation im Dark Web? Wie wickelt er Geschäfte ab und wo liegt sein Fokus? Und was ist seine bevorzugte Taktik? Für Unternehmen können diese Fragen auf den ersten Blick einschüchtern wirken. Vor allem wenn unternehmenseigene, sensible Daten auf kriminellen Seiten gefunden werden, stellt sich neben einem schnelleren Pulsschlag auch das Gefühl der Hilflosigkeit ein. Was tun? Hilfreich ist hier die Fokussierung auf klare Risikobereiche sowie die Unterstützung durch technische Tools und die Expertise von Threat Intelligence-Spezialisten.

Dark Web-Monitoring fokussiert sich daher auf drei Schwerpunkte: Bedrohungen aufspüren und zurückverfolgen, ungeschützte Login-Daten identifizieren und Betrug aufdecken. Die Überwachung wird kontinuierlich auf neue Quellen ausgedehnt und deckt neben dem mysteriösen Dark Web auch frei zugängliche Social Media-Profile, Webseiten und Chat-Kanäle, offene

File-Sharing-Dienste und Server ab. Monitoring-Tools und Datenerfassungstechniken wie Crawling und Spidering übernehmen mit dem Sammeln der Daten die Schwerstarbeit und konzentriert sich dabei auf vorab definierte Keywords und unternehmenskritische Assets. Mit Hilfe von Datenanalytik werden die gesammelten Informationen schließlich ausgewertet, gefiltert und priorisiert. Hier kommen erfahrene Sicherheitsexperten zum Einsatz, die sich als verdeckte Ermittler in kriminellen Foren bewegen, im regelmäßigen Austausch mit Anbietern und Hackern stehen und die relevanten Ergebnisse in einen Kontext rücken. Der kombinierte Ansatz aus Technologie und Experten-Know-how erlaubt einen tiefen Blick in die finstersten Ecken des Dark Webs. Auf dieser Wissensgrundlage lassen sich frühzeitig Gegenmaßnahmen treffen, Angriffe vorhersagen und Verteidigungsstrategien aufstellen. Unternehmen können auf diese Weise im Katz-und-Maus-Spiel mit der cyberkriminellen Welt nicht nur mitspielen, sondern auch gewinnen.

Stefan Bange

Gehackte Informationen im Dark Web – mehr Sicherheit durch gezieltes Monitoring

Barry McMahon, Senior Manager für Identitäts- und Zugriffsmanagement, LogMeIn

Was ist das Darkweb? Sind dadurch persönliche Informationen in Gefahr? Laut einer aktuellen Umfrage [1] unter 500 deutschen Internetusern machen sich die meisten Anwender kein Bild von den hier drohenden Risiken. Sie wissen nicht, wo sie mit dem Schutz dagegen beginnen sollen. Das hat auch Folgen für Unternehmen: Sie sind in der Pflicht, das Sicherheitsbewusstsein der Mitarbeiter zu erhöhen, um die Möglichkeit der Weitergabe vertraulicher Daten zu senken.

Durch die Covid-19-Pandemie und die dadurch zunehmende Fernarbeit stehen Cybergefahren für Unternehmen stärker denn je im Vordergrund. Privat verbringen Verbraucher mehr Zeit online, zumal Anbieter von Produkten und Dienstleistungen ihre traditionellen Wege für Verkauf und Kundeninteraktion um digitale Kanäle ergänzen oder diese ausbauen.

Diese zum Teil erzwungene Intensivierung der webbasierten Kommunikation verschafft den Cyberkriminellen eine größere Angriffsfläche. Nachrichten über Datenschutzverletzungen und die Entwendung von Informationen, um sie im Darkweb zum Verkauf anzubieten, gehören bereits zum Alltag. Doch den Verbrauchern scheint nicht bewusst zu sein, welche Auswirkungen eine Offenlegung ihrer persönlichen Daten im Darkweb hat – weder für sie persönlich noch für ihren Arbeitgeber.

Aber es ist entscheidend, dass die Benutzer wissen, womit sie es zu tun haben, wenn es um das Darkweb geht. Zudem müssen sie erfahren können, ob und welche Daten über sie dort in Umlauf geraten sind. Das ist umso entscheidender, da 31 Prozent der 500 befragten deutschen Internetuser gar nicht wissen, was das Darkweb überhaupt ist, geschweige denn, wie ihre Daten kompromittiert werden können.

Darkweb – die unbekannte Seite des Internets

Das Darkweb besteht aus den Bereichen des Internets, die nicht über Suchmaschinen wie Google zugänglich sind. Immer wieder rückt es durch spektakuläre Nachrichten über Datenschutzverletzungen enormen Ausmaßes ins Bewusstsein. Etwa wenn Tausende gestohlener Passwörter, Bankkontonummern und Krankenakten dort zum Verkauf angeboten werden. Um so bedenklicher ist, dass laut einem aktuellen Data Breach Investigation Report [2] 80 Prozent der Fälle von Informationsdiebstahl auf Nutzer selbst zurückzuführen sind, die bei ihren Logins schwache Passwörter nutzen. Dabei sind sich die Verbraucher durchaus der Risiken bewusst, die mit schwachen und mehrfach verwendeten Kennwörtern einhergehen. Doch die Angst, die eigenen Zugangsdaten zu vergessen, überwiegt offenbar und führt dazu, dass sie entgegen besseren Wissens einfache, einmal gemerkte Passwörter immer wieder verwenden [3].

Nur wenige Internetnutzer verstehen die wahre Dimension des Darkwebs. Selbst Experten sind sich uneins: Je nach Studie wird dessen Größe auf zwischen 0,005 Prozent [4] und 96 Prozent [5] des gesamten World Wide Web eingeschätzt. Die Gefahr ist aber nicht zu unterschätzen: Eine kürzlich von der University of Surrey durchgeführte Untersuchung ergab, dass fast zwei Drittel (60 Prozent) der Einträge im Darkweb das Potenzial haben, Unternehmen nachhaltig zu schädigen [6]. Sicher wird nicht alles für illegale Zwecke verwendet. Doch die zahlreichen kriminellen Netzwerke erfordern, dass Anwender ihre Daten mit höchster Sorgfalt schützen. Denn neben illegalen Waren aller Art werden hier vor allem Kreditkartennummern und gestohlene Passwörter zum Verkauf angeboten.

Darüber hinaus können Darkweb-User dort auch Dienste für Distributed-Denial-of-Service (DDoS)-Attacken oder Phishing-Attacken zum Sammeln von Betriebs- und Finanzdaten anmieten. Dieses Angebot macht es Cyberkriminellen sehr leicht, Firmen oder Privatpersonen anzugreifen. Das kann schwerwiegende finanzielle Folgen haben. Dazu kommen noch die Imageschäden für betroffene Unternehmen, deren unzureichende Sicherheitsvorkehrungen offengelegt werden.

Gehackte Informationen melden

Immerhin würde jeder vierte Betroffene Geld zahlen, um private Informationen aus dem Darkweb entfernen zu lassen [7]. Bei Anwendern, die einen solchen Angriff bereits erlebt haben, ist die Bereitschaft mit rund 50 Prozent sogar höher. Viele denken aber wohl, dass sie das nicht betrifft: Lediglich 13 Prozent bestätigten, dass ein Unternehmen, mit dem sie Kontakt hatten, Opfer eines Cyber Breach war. Die Dunkelziffer ist sicher um ein Vielfaches höher, berücksichtigt man, dass seit 2013 über 9,7 Milliarden Datensätze verloren gegangen sind oder gestohlen wurden – Tendenz steigend.

Zudem können die wenigsten Internetnutzer erfahren, ob Auskünfte zu ihrer Person online zum Verkauf stehen. Inzwischen gibt es jedoch Lösungen, die proaktiv nach E-Mail-Adressen, Benutzernamen und anderen exponierten Zugangsdaten in Datenbanken von Drittanbietern suchen und die Anwender vor deren Kompromittierung warnen. Passwortmanager beziehen daher verstärkt das Darkweb in ihr Angebot mit ein. Sie zeigen gehackte Webseiten an und präsentieren Links, über die Benutzer alle offengelegten Anmeldedaten ändern können. So zeigen diese Tools die Gefahren schlechter Passwortpraktiken auf und tragen dazu bei, Nutzer dafür zu sensibilisieren. Zudem schlagen sie für die betroffenen Logins neue komplexe Passwörter vor.

Sicherheit beginnt im Kopf

Das Aufdecken krimineller Aktivitäten im Internet ist sicher eine der grundlegenden Aufgabe beim Thema Darkweb Monitoring. Doch beginnt der wahre Kampf gegen Cyberkriminelle bereits mit der Sensibilisierung der Anwender zu Cyberrisiken von Seiten der Arbeitgeber.

Der Mensch ist meist das schwächste Glied in der Kette. Anwender versäumen es, höhere Standards an ihr Verhalten anzulegen – wie eben einzigartige und komplexe Passwörter zu nutzen. Doch auch viele Unternehmen messen einer übergeordneten Sicherheitskultur nur einen geringen Wert bei. Sie unterlassen es daher, das Risikobewusstsein ihrer Mitarbeiter gezielt zu fördern.

Gefahren zu vermeiden und abzuwehren ist ein Prozess, eine ständige Aufgabe. IT-Sicherheit und Mitarbeiter müssen zusammenarbeiten, um die Vorsichtsmaßnahmen in Unternehmen auf einen einheitlich hohen Standard zu bringen – gerade in Zeiten von Remote Work. Denn Fernarbeit wird für einen großen Teil der Unternehmen vorerst die Norm bleiben, trotz der schrittweisen Rückkehr zur Büropräsenz. Die daraus entstehenden Herausforderungen werden nicht einfach wieder verschwinden, sondern eher noch zunehmen. Denn nur jeder zweite befragte Mitarbeiter in Deutschland will wieder Vollzeit zurück ins Büro – wie eine aktuelle Umfrage zu Fernarbeit belegt [8].

Heimnetzwerke bieten Hackern eine noch leichtere Möglichkeit, Informationen zu stehlen und im Darkweb zum Verkauf anzubieten. Unternehmen sollten sich in Zeiten von steigender Remote-Arbeit wieder verstärkt auf Cyberbedrohungen konzentrieren und auf die erhöhten Risiken reagieren. Die Verwendung einzigartiger, zufällig generierter Passwörter für verschiedene Konten und die Investition in Lösungen mit integrierten Datenschutzfunktionen und einem proaktiven Darkweb-Monitoring sind ein guter Anfang für mehr Sicherheit.

Barry McMahon

Quellen: **[1]** https://www.lastpass.com/de/solutions/dark-web-monitoring/infographic/take-the-mystery-out-of-the-dark-web **[2]** https://enterprise.verizon.com/resources/reports/dbir/ **[3]** https://www.lastpass.com/de/resources/psychology-of-passwords-2020 **[4]** https://www.techradar.com/news/the-dark-web-represents-only-a-fraction-of-the-rest-of-the-internet **[5]** https://medium.com/tecoquest/the-deep-web-is-96-of-the-internet-google-know-only-4-of-it-819cd53fa7c6 **[6]** https://www.surrey.ac.uk/news/4-10-dark-net-cybercriminals-are-selling-targeted-ftse-100-or-fortune-500-hacking-services **[7]** https://blog.lastpass.com/2019/09/would-you-pay-to-buy-back-your-information-off-the-dark-web/ **[8]** https://www.goto.com/de/blog/posts/why-remote-work-is-good-for-the-planet-and-your-employees

1.6 DIGITALISIERUNG

Wie können wir die Digitalisierung der kritischen Infrastrukturen sicher gestalten?

Galina Antova, Mit-Gründerin und Chief Business Development Officer, Claroty

Bis vor kurzem war der Schutz kritischer Infrastrukturen eine rein physische Angelegenheit: Dicke Mauern, hohe Zäune und teilweise bewaffnetes Personal waren der Schlüssel zum Schutz unserer Energie-, Transport- und Wasserinfrastruktur vor potenziellen Gefahren. Dieser Status quo bestand überraschend lange Zeit, auch wenn fast jeder andere Aspekt unseres Lebens zunehmend digitalisiert wurde. Die meisten Branchen haben die digitale Transformation in den letzten Jahren voll und ganz angenommen und die Geschäftswelt ist von einem hochkomplexen Netz aus vernetzten Technologien abhängig geworden. Auch unser Privatleben ist von der digitalen Technologie geprägt, die sich zum de-facto-Standard für alles entwickelt hat – von der Bezahlung von Rechnungen bis zur Überwachung unserer Gesundheit. Doch im Laufe des digitalen Zeitalters blieben die industriellen Kontrollsysteme, die unserer kritischen Infrastruktur zugrunde liegen, weitgehend vom Internet isoliert, und der Sicherheitsperimeter war lange Zeit fast vollständig physisch.

Die digitale Transformation

Doch mittlerweile hat der digitale Wandel mit seiner Aussicht auf eine höhere Effizienz und größere Flexibilität auch die industrielle Welt erreicht. Vernetzte Informations- und Kommunikationstechnologien, die die Bereiche Wirtschaft und Handel antreiben, wachsen schnell mit den operativen Technologien (OT) zusammen, die unsere kritische Infrastruktur steuern. Die Kombination aus fortschrittlicher Computertechnik und industrieller Automatisierung trägt dazu bei, die Produktivität und den Output zu steigern. Dieser Ansatz eröffnet auch neue Möglichkeiten rund um die vorbeugende und Fernwartung und hilft, Situationen zu lösen, bevor sie zu kostspieligeren Problemen eskalieren, die wiederum zu schweren Ausfällen führen können. Aber auch dieser Fortschritt bringt neben all

den Vorteilen auch eine Reihe Risiken mit sich. Unsere (kritische) Infrastruktur muss sich nun zunehmend auf potenziell katastrophale Bedrohungen vorbereiten, die weit über den Rahmen von Sicherheitszäunen und bewaffneten Wachen zur Abwehr hinausgehen.

Wachsende Cyberbedrohungen

Der Umgang mit Cyberangriffen gehört mittlerweile zum Geschäftsalltag, bedenklich regelmäßig lesen wir über einen schweren Sicherheitsvorfall bei einem großen Unternehmen. So wurde etwa im Juli bekannt, dass einige deutsche Konzerne aus unterschiedlichen Branchen von der Hackergruppe Winnti angegriffen wurden. Sicherheitsexperten vermuten, dass die Angreifer aus China stammen und wahrscheinlich von staatlichen Stellen organisiert oder beauftragt werden. Mit der zunehmenden Vernetzung steigen natürlich die Risiken – und Betreiber von kritischen Infrastrukturen bilden da keine Ausnahme. Und dieses neue Feld wird von Bedrohungsakteuren genutzt, um Aufklärungsaktionen durchzuführen, Fernzugriff zu erhalten und sogar schwere Angriffe zu starten. Glücklicherweise sind diese Vorfälle bislang deutlich seltener als die ständigen Angriffe auf Unternehmen aus der Finanzbranche und dem Handel. So gab es in den letzten Jahren weltweit tatsächlich nur eine geringe Anzahl an Fällen. Die Auswirkungen eines Angriffs auf die Infrastruktur sind jedoch weitaus größer als in fast jedem anderen Sektor. Während ein Verstoß, den ein Einzelhandelsunternehmen erleidet, seinen Gewinn beeinträchtigt und seine Kunden einem erhöhten Betrugsrisiko aussetzt, kann ein erfolgreicher Angriff auf kritische Infrastrukturen auf nationaler Ebene viel konkretere und weitreichendere Auswirkungen haben – und möglicherweise sogar Leben gefährden.

Fortschrittliche Infrastruktur-Angriffe

Der Wendepunkt für die Cybersicherheit in kritischen Infrastrukturen erfolgte im Jahr 2015 mit dem ersten bekannten erfolgreichen Angriff auf ein Stromnetz. Im Dezember 2015 wurden die Informationssysteme von drei Energieversorgern in der Ukraine von einem Angriff getroffen, der später das Netz zum Erliegen brachte. Der Angriff war sehr organisiert, komplex und folgte einem mehrstufigen Ansatz, der mehrere verschiedene Angriffstechniken kombinierte. Als erster Schritt wurden die Unternehmensnetzwerke mit einer leistungsstarken Malware namens BlackEnergy kompromittiert, die über eine Spear-Phishing-E-Mail verbreitet wurde. In der Folge ergriffen die Angreifer die Kontrolle über die SCADA-Systeme (Supervisory Control And Data Acquisition), um Umspannwerke aus der Ferne abzuschalten und IT-Infrastrukturanlagen zu deaktivieren. Daneben wurde eine weitere Malware namens KillDisk eingesetzt, um große Mengen an Dateien zu löschen, die auf Workstations und Servern gespeichert waren, und schließlich wurde ein DDoS-Angriff (Distributed Denial of Service) eingesetzt, um ein Call Center zu deaktivieren und so zu verhindern, dass Verbraucher Informationen über den Blackout erhalten. Das Resultat: 225.000 Menschen hatten zwischen einer und sechs Stunden lang keinen Strom. Aufgrund des anhaltenden Konflikts zwischen der Ukraine und Russland zu diesem Zeitpunkt wurde der Angriff von den meisten Experten der russische APT-Gruppe zugeschrieben.

Die Ukraine war ein Jahr später, im Dezember 2016, Opfer eines weiteren schweren Angriffs auf ihr Stromnetz. Dieser zweite Angriff setzte fast ein Fünftel von Kiew rund eine Stunde außer Strom, wobei vielfach davon ausgegangen wird, dass diese Attacke vor allem eine Art Testlauf der Angreifer gewesen ist. Der zweite Angriff verfolgte einen anderen Ansatz als der erste und setzte auf die Malware Industroyer bzw. Crashoverride. Die Malware wurde speziell entwickelt, um industrielle Kontrollsysteme zu stören und enthält eine Reihe von Komponenten, die verschiedene Aktionen ausführen: So stellt ein Backdoor-Element eine Fernverbindung her, die es Angreifern ermöglicht, Befehle zu geben und Angriffe auszuführen. Für den Fall, dass diese Hintertür entdeckt wird, steht den Angreifern noch eine zweite zur Verfügung. Vier separate Payload-Komponenten richten sich dann gegen bestimmte Industrieprotokolle, während ein Wiper wichtige Registry-Keys löscht und Dateien überschreibt, was die spätere Wiederherstellung erheblich erschwert.

Zwar sind die Angriffe auf die Ukraine glücklicherweise bislang eher außergewöhnlich, doch die Gefahr eines neuen Vorfalls ist sowohl für die Energiewirtschaft als auch für andere kritische Einrichtungen auf der ganzen Welt groß. Jüngste Untersuchungen, die gemeinsam vom UK Infrastructure Transitions Research Consortium an der University of Oxford und dem Centre for Risk Studies an der Cambridge Judge Business School durchgeführt wurden, haben das potenzielle Risiko für das Vereinigte Königreich durch einen Cyberangriff quantifiziert. Ausgehend von den ukrainischen Vorfällen schätzten die Forscher, dass ähnliche Angriffe auf Großbritannien mehr als 111 Millionen Pfund pro Tag kosten könnten. Es wurde der Schluss gezogen, dass selbst ein relativ kleiner Vorfall die Stromversorgung von mehr als 1,5 Millionen britischen Bürgern beeinträchtigen könnte. Es ist davon auszugehen, dass diese Zahlen auf die meisten europäischen Länder übertragbar sind.

Ins Unbekannte

Eine der größten Herausforderungen in der Cybersicherheit ist die Einbeziehung des Unbekannten. Während sich Sicherheitsteams und Security-Lösungen schnell an neu entdeckte Schwachstellen, Malware und Techniken anpassen können, kann man sich eben nur schwerlich auf bisher unbekannte Bedrohungen vorbereiten. Wir müssen leider davon ausgehen, dass in vielen industrielle Systeme bereits unbekannte Malware buchstäblich schlummert und nur auf Anweisungen wartet, zu gegebener Zeit zuzuschlagen. Der damalige Direktor der US-amerikanischen nationalen Nachrichtendienste Dan Coates sagte Anfang 2019 vor dem Kongress, dass die Sicherheitskräfte davon ausgehen, dass Russland im Falle einer Krise Cyberangriffe auf die zivile und militärische Infrastruktur durchführt, um diese zu stören.

Wie bei traditionellen Waffen können auch Cyber-Angriffstools, wenn sie sich nur in den Händen einiger Nationalstaaten befinden, eine abschreckende Wirkung erzielen. Angriffe würden zu Gegenangriffen führen, so dass große Schlagabtäusche eher unwahrscheinlich sind. Gleichwohl kann es durchaus zu staatlich unterstützten Aktivitäten in kleinerem Rahmen kommen, insbesondere wenn die Zuordnung des Angriffs nicht ohne weiteres möglich ist.

Im Gegensatz zur konventionellen Kriegsführung können schwere Cyberangriffe jedoch auch von nicht-staatlichen Akteuren mit vergleichsweise geringen Ressourcen organisiert werden. Kritische Infrastrukturen stellen (bislang) ein unattraktives Ziel für den durchschnittlichen Kriminellen dar, der insbesondere durch finanziellen Gewinn motiviert ist. Andere Branchen versprechen höhere Gewinne bei weniger Aufwand und Risiko. Allerdings ist die Infrastruktur nach wie vor potenziell durch nichtstaatliche Akteure wie Terroristen gefährdet. Und möglicherweise entwickeln auch Cyberkriminelle im Bereich der kritischen Infrastrukturen noch lohnende Geschäftsmodelle.

Ist der Weg zurück ein Ausweg?

Die vielleicht größte Herausforderung bei der Sicherung der weltweiten Infrastruktur besteht darin, dass sie nie so konzipiert wurde, dass sie gegen diese Art von Bedrohungen geschützt ist. Die meisten Systeme waren für den Betrieb in hochsicherer Umgebung vorgesehen, geschützt vor Störungen durch Wände, Tore und Schutzeinrichtungen. Das bedeutet, dass den Geräten oft grundlegende Funktionen wie Authentifizierung und Verschlüsselung fehlen. Die Herausforderung wird durch die fragmentierte und intransparente Natur der Angriffsziele noch verschärft. Der größte Teil der kritischen Infrastruktur der Welt läuft auf einer Vielzahl alter und undurchsichtiger Protokolle, von denen viele proprietär sind, was es viel schwieriger macht, eine einheitliche Sicht auf die Systeme als Ganzes zu erhalten.

Ein verbreiteter Lösungsvorschlag für die Problematik besteht darin, die Digitalisierung zurückzudrehen. So kündigte im Juli 2019 die US-Regierung Pläne an, kritische Systeme auf analoge und manuelle Technologie umzustellen, um die wesentlichen Leitsysteme des Netzes zu isolieren. In einer Pressemitteilung zur Verabschiedung des Securing Energy Infrastructure Act (SEIA) heißt es, dass sichergestellt werden soll, dass Angreifer wieder physischen Zugriff benötigen würden, um sie zu stören oder zu beschädigen.

Aber ist dieser Weg zurück wirklich ein Fortschritt, zumindest in Sachen Sicherheit? Es ist eher davon auszugehen, dass dieser Schritt eher kontraproduktiv ist und der Innovation schaden könnte. Die kritische Infrastruktur, sei es die amerikanische oder die eines anderen Landes auf der Welt, ist nicht verwundbar, weil sie digital ist, sondern weil die Bedrohungsakteure die Landschaft besser verstehen als diejenigen, die sie verteidigen sollen.

Transparenz ist der Schlüssel

Wir stehen heute vor der ungewöhnlichen Situation, dass die Industrie und nicht die Regierung an vorderster Front bei potenziellen Konflikten stehen. Angesichts einer großen Anzahl kritischer Infrastrukturen, die von der Privatwirtschaft verwaltet werden, ist es weitgehend Sache der einzelnen Unternehmen, für die Transparenz ihrer eigenen Netzwerke und der Fähigkeit zur Identifizierung und Abwehr von Bedrohungen zu sorgen. Deshalb muss die oberste Priorität darin liegen, diese Transparenzlücke zu schließen, welche es Angreifern derzeit ermöglicht, komplexe Angriffspläne umzusetzen, ohne entdeckt zu werden. Industrie und staatlichen Stellen müssen hier zusammenarbeiten, um die heterogene, zerklüftete und undurchsichtige Angriffsfläche von heute in eine transparente Verteidigungsarchitektur zu verwandeln, die es den Verteidigern ermöglicht, Bedrohungen zuverlässig zu erkennen und abzuwehren.

Galina Antova

Sicherheitsherausforderungen für die neuen Technologien in Europa

Neue Technologien erweitern Unternehmensstrukturen in Sekundenschnelle, stellen Sicherheitsexperten jedoch vor neue Aufgaben. Eine aktuelle Studie nennt in diesem Zusammenhang vor allem die Datensicherheit als Hürde

Es ist schwer in Unternehmen den Anfang und das Ende der digitalen Transformation klar festzumachen. Organisationen müssen sich dem Tempo der Digitalisierung und der damit einhergehenden veränderten Bedrohungslage anpassen. Innovationen sollten kontinuierlich implementiert werden, um dem Zyklus zu folgen und neue Möglichkeiten auszuschöpfen.

Es handelt sich nicht lediglich um eine reine Investition. Dies zeigt der Data Threat Report-Europe Edition, welcher europäische Betriebe und deren Datensicherheit in Bezug auf sensible Informationen in digitalen Transformationsumgebungen analysiert. Über ein Drittel (36 Prozent) der Befragten gibt an,

Thorsten Krüger, Regional Sales Director DACH, Thales

dass sie die Märkte, an denen sie beteiligt sind, durch ein digitales Transformationsprojekt durchdringen möchten.

Der Bericht zeigt auf, dass die Datensicherheit die meisten Organisationen weiterhin vor eine Herausforderung stellt. In Transformations-Umgebungen sind Daten häufig anfällig und ungeschützt. Doch damit sind die Herausforderungen und das Aufgabenspektrum für CIOs und die IT-Funktion noch nicht ausgeschöpft. IT-Verantwortliche müssen sich nicht nur mit einer Bandbreite neuer Basistechnologien, welche die Grenzen von Konnektivität, Stabilität und Effizienz sprengen, sondern auch mit einer Reihe von Sicherheitsherausforderungen auseinandersetzen.

Die Untersuchung betrachtet unter anderem die digitale Transformation in Europa und zeigt, dass der Kontinent im weltweiten Vergleich leicht zurückfällt. Deutschland liegt jedoch über dem Durchschnitt. Oberflächlich betrachtet bietet Digitalisierung Unternehmen die Chance durch hybride, cloudbasierte Infrastrukturen, anderen Mitbewerbern mit älteren Perimeterstrukturen voraus zu sein. Dennoch stehen gerade diese Firmen vor der Herausforderung Sicherheitsarchitekturen in alte Infrastrukturen zu implementieren und gleichzeitig neue, digital transformative Technologien einzuführen. Es ist ein paradoxes Unterfangen, denn dies kann dazu führen, dass Sicherheitsfachleute ihr Ziel verfehlen, nehmen sie an, neue Technologien bieten automatisch mehr Schutz. Doch steigt die Anzahl der zu sichernden Infrastruktur, ist das Netzwerk nicht weiter lokal im Server verankert. Je mehr Daten auf eine stetig steigende Zahl an Umgebungen verteilt sind, desto schwieriger wird es für das Unternehmen, sich auf den Schutz von Daten in einer einzelnen Umgebung zu konzentrieren. Daher ist ein intelligenter Ansatz für die Datensicherheit und die Einführung moderner, hybrider Multi-Cloud-Technologien notwendig. Ein nicht zu unterschätzender Fakt ist, dass das Potential an Firmen, welche der Cloudifizierung folgen, in Europa noch nicht ausgeschöpft ist, denn sie nutzen im weltweiten Vergleich mit 67 Prozent bisher weniger Clouds wie SaaS, PaaS und IaaS für die Speicherung sensibler Daten. Insgesamt speichern jedoch 98 Prozent der europäischen Unternehmen diese Daten auf digital transformierbaren Umgebungen. Das zeigt das Potential, aber auch die Herausforderung auf.

Die überwiegende Mehrheit (84 Prozent) der Betriebe nutzt heutzutage digitale Transformationstechnologien wie Big Data, Container, Blockchain und das Internet der Dinge (IoT). Wie entwickeln sich diese Innovationen aus der Sicht der Cyber-Sicherheit?

IoT

Der Bericht stellte primäre Bedrohungen für das Internet der Dinge in Europa fest: Angriffe auf IoT-Geräte sowie deren Verlust oder Diebstahl und den Mangel an etablierten Sicherheitsrahmen. Im Gegensatz dazu sind Themen wie der Schutz sensibler Daten, die von IoT-Geräten erzeugt werden, mit Technologien wie Verschlüsselung, Tokenisierung und Validierung der Integrität von IoT-Geräten erfassten Daten weitaus weniger problematisch in Europa als auf anderen Kontinenten. Dies ist der Fall, da damit verbundene Risiken in Europa grundsätzlich bereits seit längerer Zeit ernst genommen werden.

Big Data

Das Bild sieht jedoch etwas anders aus, wenn die Bedrohungen im Zusammenhang mit großen Datenmengen betrachtet werden. Europäische Organisationen sind hier am meisten über eine stärkere Verschlüsselung und Zugangskontrolle auf Systemebene und eine stärkere Zugangsauthentifizierung besorgt. Die Möglichkeit, verschlüsselte oder tokenisierte Daten in großen Umgebungen zu analysieren, wirkt auf die Unternehmen oftmals verwirrend.

Blockchain

Trotz des enormen Potenzials der verteilten Ledger-Technologie darf eine ganze Bandbreite neuer Sicherheitsprobleme nicht übersehen werden. Es können neue Gefahren entstehen wie Insider-Risiko, Kryptojacking und Volatilität der Online-Währung. Die Befragten in Europa scheinen besonders nervös zu sein und zeigen sich besorgter als die Teilnehmer in der globalen Stichprobe. Von den neueren Technologien, die hier vorgestellt werden, ist das Verständnis der Herausforderungen der Blockchain-Sicherheit wahrscheinlich am weitesten entwickelt. Es ist aber noch ein weiter Weg, bis dies eine zuverlässige, sichere Basistechnologie für Firmen weltweit darstellt.

Container

Was die Verwendung von Containern in der Entwicklung betrifft, so sind die europäischen Organisationen vor allem um die Sicherheit der gespeicherten Daten besorgt - gefolgt von der Verbreitung von Malware zwischen den Behältern und dem mangelnden Vertrauen in Container-Images von Dritten.

Diese neuen Technologien bieten ein bemerkenswertes Potenzial, die Art und Weise, wie Produkte und Dienstleistungen entwickelt, verwaltet, verkauft und konsumiert werden, zu verändern. So können Unternehmen die Komplexität bewältigen und mit weniger Aufwand mehr erreichen. Digitale Innovation spielt die tragende Rolle im Wettbewerb. Umso wichtiger ist es, diese neuen Bedrohungen im Auge zu behalten. Wenn die neuen Voraussetzungen geschafft werden, ist ein Schritt zur Sicherung der digitalen Transformationsprojekte als Ganzes und gleichzeitig der zukünftigen Wirtschaft getan.

Fazit

Die Studie zeigt auf, dass die digitale Transformation fundamentale Auswirkungen auf die Weltwirtschaft, insbesondere mit Blick auf Europa hat. Sie bietet Chancen, einen Wettbewerbsvorteil zu generieren, indem Prozesse effizienter gestaltet werden. Unternehmen sind in der Lage ihre Infrastruktur exponentiell zu steigern. Dennoch stellt die Digitalisierung den Bereich der Informationssicherheit vor neue Herausforderungen. Nicht nur das dynamisch wachsende Bedrohungsumfeld, sondern auch die zunehmend strengen Vorschriften konfrontieren Sicherheitsfachleute mit neuen Aufgaben. Die Implementierung neuer Technologien scheint notwendig, dennoch sollte stets auf bewährte Verfahren im Umgang mit sensiblen Daten gesetzt werden, um eine sichere digitale Transformation zu gewährleisten.

Thorsten Krüger

DIGITALSICHERHEIT muss 2019 großgeschrieben werden

Laut einer Studie von Gartner, die das disruptive Potenzial von zehn Technologien hervorhebt, sind Digitalethik und Privacy Schlüsselthemen des Jahres 2019. Aufgrund der immer stärker ausgebauten globalen Vernetzung werden auch Sicherheitsaspekte sowohl für Privatpersonen als auch für Unternehmen und Regierungen immer wichtiger.

Laut Gartners „Top 10 Strategic Technology Trends for 2019“ spielt Digitalethik eine prominente Rolle in vielen Unternehmen. Kein Wunder, soll es doch im kommenden Jahr insgesamt 14,2 Milliarden Connected Devices geben, die mit dem IoT verbunden und somit potenziellen Sicherheitsrisiken ausgesetzt sind. Doch die Privacy Issues erreichen ihren Peak noch lange nicht im Jahr 2019, denn bereits zwei Jahre später soll sich die Zahl der verbundenen Geräte auf 25 Milliarden erhöhen – Tendenz steigend. Dementsprechend müssen Vorsorgevorbereitungen bezüglich Infrastruktur-, Netzwerk- und Datacentersicherheit sowohl auf Soft- als auch auf Hardware-Ebene getroffen werden.

Wie groß ist die Gefahr in Bezug auf Cyber-Angriffe wirklich?

Beim Bundesamt für Sicherheit und Informationstechnik (BSI) gehen täglich Meldungen zu 390.000 neuen Schadprogrammen ein – eine Masse, bei der es schwer ist, hinsichtlich Gegenmaßnahmen Schritt zu halten. Die Zahl verdeutlicht die unfassbare Geschwindigkeit, mit der sich Viren, Trojaner und andere Schadprogramme im Internet vermehren. Hinzu kommen die neuen Errungenschaften des IoT, durch dessen Schnittstellen Malware-Programme eine Unzahl weiterer Einfallsmöglichkeiten in Software, Systeme und Netzwerke bekommen.

43,4 Milliarden Euro Schaden durch Cyberattacken zwischen 2016 und 2018

68 Prozent der deutschen Industrieunternehmen sind laut Bitkom zwischen 2016 und 2018 Opfer von Cyberattacken oder Spionage geworden. Sensible Daten werden gestohlen, interne Kommunikation ausgespäht, Daten verschlüsselt und Lösegeld erpresst. Bei 47 Prozent der Unternehmen entstanden dadurch Kosten – u. a. durch Malware (bei 24 Prozent), Exploits (bei 16 Prozent), Phishing (bei 16 Prozent), Passwort-Angriffe (bei 12 Prozent) und Spoofing (bei 6 Prozent). Allein in Deutschland verursachten Cyberattacken in den letzten zwei Jahren einen Gesamtschaden von 43,4 Milliarden Euro – eine ernstzunehmende Größe und Entwicklung.

Security by Design: Die Implementierung von Sicherheitskonzepten in alle Unternehmensbereiche

Punktuelle Virenabwehr und Netzwerksicherung gehört bei den meisten Unternehmen zum Standard. Das reicht allerdings heutzutage nicht mehr aus, denn ein holistischer Ansatz gegen Cyberattacken ist gefordert, um wirkliche Sicherheit zu gewährleisten. In diesem Zusammenhang kommt Security by Design ins Spiel. Hinter dem Begriff steht nichts anderes als die Integration von Sicherheitskonzepten in alle Unternehmensbereiche – bestenfalls schon bei der Architektur dieser Bereiche und nicht erst im Nachhinein. Dadurch werden Lücken in der Sicherheitsstruktur von Anfang an vermieden, was wiederum darin resultiert, dass es Angreifer schwerer haben, an sensible Daten zu gelangen.

Theorie und Praxis sind zwei verschiedene Paar Schuhe

Security by Design - ein schönes Vorhaben. Jedoch holt uns eine Studie der Wirtschafts- und Beratungsgesellschaft PwC aus dem Jahr 2018 schnell wieder auf den Boden der Realität zurück. Es wurden weltweit 9.500 Unternehmen nach Cyber-Sicherheitsmaßnahmen befragt. Lediglich 53 Prozent befolgten im Zuge ihres digitalen Transformationsprozesses den Ansatz Security by Design, um Sicherheitsaspekte in jeden Unternehmensprozess zu integrieren. Doch das ist (leider) noch nicht alles:

- eine durchdachte Daten- und Informationsstrategie können nur 56 Prozent vorweisen
- einen Überblick über den Stand personenbezogener Daten haben lediglich 51 Prozent
- über potenzielle Gefahrenquellen sind sich nur 31 Prozent im Klaren

Diese Daten stammen nicht aus den Anfängen der Internetzeit, sondern aus dem Jahr 2018, wo das Internet der Dinge nichts Neues mehr und damit die Digitalisierung in alle Aspekte des Lebens und der Gesellschaft vorgedrungen ist. Zudem handelt es sich

Gordon Herenz, Wissenschaftlicher Mitarbeiter an der Universität Potsdam, Content Marketing Manager bei der Peak Ace AG

bei Cyber-Security keineswegs um ein randständiges Phänomen, das im Vorbeigehen „mal mitgemacht" werden kann, sondern Informationssicherheit ist längst ein Schlüsselfaktor für das ökonomische Überleben.

Handeln auf Regierungsebene: Bund will Agentur für Cybersicherheit gründen

Neben Unternehmen treffen massive Hacking-Angriffe besonders oft Regierungen. Man denke nur an die Einmischung Russlands in den US-Wahlkampf 2016 oder an die Cyberattacken gegen zahlreiche deutsche und ausländische Unternehmen in den letzten Jahren. Geht es bei Privatpersonen um Persönlichkeitsrechte und ungewollte Werbung sowie Personalisierung, steht bei Regierungen die staatliche Souveränität auf dem Spiel. Cyber-Security ist längst zu einer Frage der nationalen Sicherheit geworden.

Die Bundesregierung plant aus diesem Grund eine Agentur für Cybersicherheit, die in der Region Halle-Leipzig bis 2023 errichtet und von Innen- und Verteidigungsministerium getragen werden soll. Das Startkapital beträgt bis 2023 laut Regierungsangaben 200 Millionen Euro. Rund 100 Mitarbeiter sollen sich mit der Prävention von Cyber-Attacken beschäftigen. Des Weiteren wird es zu ihren Aufgaben gehören, passende Start-ups und Gründer zu identifizieren, die wertvoll für die nationale Informationssicherheit sind bzw. sein können. Ebenfalls ist geplant, mit der Agenturinitiierung den Wirtschaftsstandort Sachsen bzw. Sachsen-Anhalt zu fördern

Die Agentur für Cybersicherheit ist nicht die einzige vom Bund geförderte Institution, die sich der Bekämpfung von Cyber-Kriminalität widmet. So beschäftigt sich zum Beispiel der Cyber Innovation Hub seit 2017 damit, die Bundeswehr in das digitale Zeitalter zu hieven, relevante Start-ups zu identifizieren und im Anschluss mittels Bundesmitteln zu fördern.

Facebook gibt personenbezogene Daten an Partnerunternehmen weiter

Nicht nur Unternehmen und Regierungen sind von Cyber-Attacken betroffen, sondern auch Privatpersonen. User sind zunehmend besorgt, was mit ihren privaten Daten geschieht und wie diese von Unternehmen ausgewertet werden, um z. B. personalisierte Werbung einzuspielen. Und das zurecht. Es geht nicht nur um personalisierte Display Ads, sondern auch um das holistische Targeting, mit dem Unternehmen so viele Informationen wie möglich von einer Person in Erfahrung bringen. So lässt sich auf subtilere Weise werben, ohne dass es der User im ersten Moment als Werbung identifiziert.

Die Mittel, die Unternehmen dafür einsetzen, sind allerdings dubios bzw. illegal: So hat Facebook die Daten von Hunderten Millionen von Nutzern an externe Partnerunternehmen weitergegeben, darunter auch Apple, Amazon, Netflix und Spotify. Den letzten beiden sei es sogar möglich gewesen, private Nachrichten von Usern zu lesen. Die betroffenen Unternehmen geben vor, von diesem „Privileg" nichts gewusst bzw. keinen Gebrauch gemacht zu haben.

Wie stehts es um die Cyber-Sicherheit von Privatpersonen – speziell Kindern?

Wenn es Erwachsene nicht hinbekommen, wie sollen dann erst Kinder und Jugendliche sicher online mit ihren Informationen umgehen? Laut einer Befragung des BSI (Bundesamt für Sicherheit und Informationstechnik) sind die meisten Eltern im Gespräch mit ihren Kindern, wenn es um Online-Verhaltensregeln und Protektionsmaßnahmen geht. Allerdings dreht sich das Gespräch dann meist eher um In-App-Käufe (66%) und ungeeignete Inhalte (60%). Über Fälle von Cyber-Kriminalität sprechen weniger als die Hälfte der Eltern: Spam- bzw. Betrugsmails (47%), Schadprogramme (45%) und E-Mail-Postfachsicherheit (29%). Das ist riskant, denn Kinder und Jugendliche sind bereits früh zum Teil unbeaufsichtigt mit dem Smartphone online unterwegs – und das auch immer länger laut dieser Grafik:

Die Daten zeigen, dass Eltern bereits mit ihrem Nachwuchs über die Gefahren, die im Internet auf sie warten, sprechen, allerdings den Aspekt der Cyber-Security und Informationssicherheit teils ausblenden. Deswegen ist es nötig, dass gesamtgesellschaftliche Aufklärungsarbeit geleistet und für Cyber-Gefahren sensibilisiert wird.

Fazit – Datensicherheit ein entscheidender Punkt im Jahr 2019

Für die Digitalsicherheitsbranche sowie für Security-Entscheider in Unternehmen stellen sowohl die Weitergabe der Personendaten als auch die kostenintensiven und sicherheitsgefährdenden Angriffe auf Unternehmen ein überdeutliches Alarmsignal dar, 2019 dringend weiter an der Datensicherheit zu arbeiten. Zudem müssen Regierungen im öffentlichen sowie Familien im privaten Raum Präventionsmaßnahmen ergreifen, um sich zu schützen.

Die Technologie schreitet unaufhaltsam fort und proportional dazu sollten Cyber-Security-Maßnahmen und -Ausgaben Schritt halten, um die digitale und technologische Zukunft mit allen ihren Innovationen auch abzusichern. Deswegen liegt auch bei der Gartner-Studie neben anderen Technologien wie Blockchain, Smart Spaces und Automated Things ein spezifischer Fokus auf Digital Ethics und Privacy. Weltweit sollen die Spendings im Bereich Daten- und Informationssicherheit laut der Studie in zwei Jahren um 22 Prozent steigen – von 101,5 Milliarden (2017) auf 124,1 Milliarden US-Dollar (2019). Eine Investition in die Sicherheit von Daten ist eine Investition in die Zukunft.

Gordon Herenz

Smart Cities der Zukunft sichern

Die Zukunft der Weltbevölkerung ist urban. Im Jahr 2050 werden etwa zwei Drittel der Menschen in städtischen Gebieten leben – besonders in Asien und Afrika wird die Urbanisierung schnell vorangetrieben. Im Klartext bedeutet dies, dass in den kommenden drei Jahrzehnten voraussichtlich zusätzliche 2,5 Milliarden Menschen in unseren Städten leben werden. Neben der Beschaffung des nötigen Wohnraums, führen vor allem die Bereitstellung kritischer Infrastrukturen und städtischer Dienstleistungen zu großen Herausforderungen.

Technologie kann hier eine entscheidende Brücke schlagen und bessere, sicherere sowie effizientere Städte schaffen. In den Bereichen Versorgung, Transport, Verkehr, Abfallwirtschaft, Umweltverschmutzung, nachhaltiges Leben, Sicherheit, Gesundheitsfürsorge und Governance entstehen intelligente Städte als Antwort auf die stetig wachsenden urbanen Ballungsräume.

Smart City-Initiativen sind wahre Game Changer. Heizungen aus erneuerbaren Quellen in Yokohama, digitalisierte Abfallmanagementsysteme in Barcelona, intelligente Parklösungen in Canberra, Echtzeit-Überwachung des öffentlichen Verkehrs in Groningen oder ein dezentrales Luftqualitätsnetz in Nimwegen – um nur einige Beispiele zu nennen.

Interkonnektivität ist ein doppelseitiges Schwert

Smart Cities basieren auf zahlreichen vernetzten Sensoren und Internet of Things (IoT)-Endgeräten. Diese sind über das Internet und Cloud Computing-Architekturen miteinander vernetzt und kontrollieren interne sowie externe Systeme. Darüber hinaus werden persönliche und vertrauenswürdige Daten über unsichere Kanäle übertragen – dabei sind die Endgeräte oftmals nicht gepatcht und unterstützen keine Datenverschlüsselung. Diese Interkonnektivität, die eine Smart City am Laufen hält, schafft gleichzeitig substantielle Risiken in Sachen Cyber Security. Jeder Zugangspunkt erhöht die Anfälligkeit für die Gefährdung sensibler Daten – und digitale Angriffe haben bereits begonnen.

2018 traf beispielsweise Atlanta eine Ransomware-Cyberattacke. Der Angriff legte zahlreiche Geräte für fünf Tage lahm, behinderte die Strafverfolgung sowie die Vergabe von Geschäftslizenzen und stoppte sogar den Betrieb des wichtigsten Flughafens der USA. Ransomware-Angriffe zerstörten darüber hinaus einen Großteil der Server in Baltimore und sorgten im selben Jahr für die Abschaltung der 911-Notrufzentrale, was Schäden in Höhe von 18 Millionen US-Dollar verursachte.

Diese Angriffe betreffen nicht nur Städte in den USA. Beispielsweise war das Straßensystem in Dublin von einer Ransomware-Attacke betroffen, ebenso wie die Flugverkehrskontroll- und Eisenbahnfahrkartensysteme von Stockholm. Außerdem wurde die Stromversorgung in Johannesburg und Hyderabad nach einer Ransomware-Attacke gestört. Neben Ransomware setzen die Cyberkriminellen zahlreiche andere Techniken ein, darunter Angriffe aus der Ferne, das Stören von Signalen, aber auch bekannte Maßnahmen wie Malware, Datenmanipulation und Distributed Denial-of-Service-Attacken. Die digitalen Arsenale der Cyberkriminellen stammen aus dem Deep web und ihre Waffen sind voll automatisiert und ermöglichen Angriffe, die rund um die Uhr und sieben Tage die Woche ausgeführt werden können.

Leichte Ziele oder vermeidbare Verbrechen?

Städte sind ein leichtes Ziel für Cyberkriminelle, da sie beim Einsatz von Technologien oftmals hinterherhinken und die zugrunde liegende Technik – die die kritische Infrastruktur der Städte stützt – ist bestenfalls veraltet. Die technologische Beschleunigung, die

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

bestehende Städte in intelligentere Städte verwandelt, erhöht die Komplexität. Smart Cities werden nicht in einem Zug gebaut, sondern entwickeln sich im Laufe der Zeit weiter. Da oftmals Technologien eingesetzt werden, die zunächst experimenteller Natur sind, bleiben in vielen Fällen die Betaversionen langfristig im Einsatz, wodurch sich auch die Wahrscheinlichkeit von Pannen erhöht.

Städte erwirtschaften derzeit 70 Prozent des weltweiten Bruttoinlandsprodukts. Cyberkriminelle, die einen Weg finden die Verteidigung einer Smart City zu durchbrechen, haben damit eine gute Chance, sich finanziell bereichern zu können. Smart Cities müssen aus diesem Grund „secure by design" sein und nicht einfach nur angedockt werden, nachdem die Systeme bereits aufgesetzt wurden. Die Systeme sollten von Beginn an auf soliden, intuitiven und automatisierten Sicherheitsprotokollen und -richtlinien basieren. Dabei ist es wichtig, die Bürger in jeder Phase einzubeziehen, denn auf diese Weise lernen sie leichter, Eigenverantwortung in Bezug auf die Einhaltung der Datenschutzanforderungen zu übernehmen.

Cyberrisiko definiert durch die Konvergenz von Alt und Neu

Das Sicherheitsrisiko des Ökosystems einer Smart City wird von mehreren Faktoren beeinflusst. Die Konvergenz von Cyber- und Betriebssystemen platziert Geräte und Sensoren am „Edge" – diese wiederum können zu Einstiegspunkten für Cyberkriminelle werden. Harmlose Geräte wie energiesparende, automatische Beleuchtung oder Energiezähler werden so schnell zu potenziellen Einstiegspunkten. Sobald diese gehackt und mit Malware infiziert sind, öffnen sie weitere vernetzte Geräte und verursachen kaskadierende Schäden in der gesamten Infrastruktur.

Aufgrund der notwendigen Interoperabilität zwischen Legacy-Systemen und neuen digitalen Technologien müssen unterschiedliche Technologieplattformen für die Zusammenarbeit angepasst werden. Ohne konsistente Sicherheitsrichtlinien und -verfahren zur Regelung des operativen Rahmens setzen sie das gesamte Ökosystem verborgenen Sicherheitslücken aus. Verschärft wird diese Herausforderung noch durch fehlende allgemein anerkannte Standards für die Funktionsweise von IoT-fähigen Geräten am „Edge". Im Grunde beeinträchtigt also die Interoperabilität die Sicherheit.

Ein weiterer Einflussfaktor ist die Integration und Vernetzung verschiedener Services und Abteilungen innerhalb eines Smart City-Ökosystems. Die Services und Abteilungen arbeiten oftmals unabhängig in Silos und die Kombination aus Dienstleistungen und Systemintegration, Vernetzung und Datenaustausch schafft gemeinsame Schwachstellen. So kann ein Problem in einem Dienstleistungsbereich schnell andere Bereiche infizieren.

Integrierte Frameworks und umfassende Governance-Modelle

Um Bedrohungen der Cyber Security, die durch Konvergenz, Interoperabilität und Vernetzung verursacht werden, zu adressieren, erfordert es ein Framework für Cyberrisiken. Solche Frameworks müssen den Städten Managementprinzipien an die Hand geben, um die branchenweiten Cyber Security-Standards bereits in den Entwurf zu integrieren und sicherzustellen, dass die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit erfüllt werden. Die Frameworks sollten darüber hinaus rechtliche und regulatorische Anforderungen umfassen, die die Auswirkungen von Cyberrisiken auf alle Parteien des Ökosystems, Dienstleistungen, Infrastruktur und Prozesse bewerten. Dieser Rahmen muss entwickelt und in alle Planungs-, Entwurfs-, Implementierungs- und Transformationsentwürfe integriert werden sowie im Einklang mit der umfassenderen Smart City-Strategie stehen. Darüber hinaus muss er auch den Einfluss der einzelnen Systeme und Assets aufeinander bewerten.

IoT-Endgeräte und -Netzwerke werden durch Geräte-Authentifizierung, Patching, Datenverschlüsselung und Security-Monitoring vor Angriffen geschützt. Der Aufbau sicherer Kanäle sowie einer sicheren Vertrauenskette zwischen den miteinander vernetzten Geräten ist von entscheidender Bedeutung. Und auch physische Sicherheitsmaßnahmen, die IoT-Geräte vor unbefugtem Zugriff und Cyberangriffen schützen, sollten nicht vernachlässigt werden.

Smart Cities benötigen zudem ein umfassendes, formales Governance-Modell, das die Rollen und Verantwortlichkeiten für jede kritische Komponente im Ökosystem festlegt. Das Modell untermauert die kontinuierliche Angleichung von Politik, Gesetzgebung und Technologie im Hinblick auf das richtige Gleichgewicht zwischen Datenschutz, Transparenz und Nutzen.

Schließlich müssen Smart Cities ihr Netzwerk erweitern und sich beispielweise mit der Stadtverwaltung anderer Smart Cities sowie mit der Wissenschaft, dem Privatsektor und Start-ups verknüpfen, um ihre Interessen zu vertreten und die Smart City weiter voranzutreiben. Auch wenn ihr immenses Potenzial nach wie vor vorhanden ist, ist ein effektives Management der damit verbundenen Cyberrisiken von entscheidender Bedeutung, um das Versprechen der Smart City zu verwirklichen.

Vishal Salvi

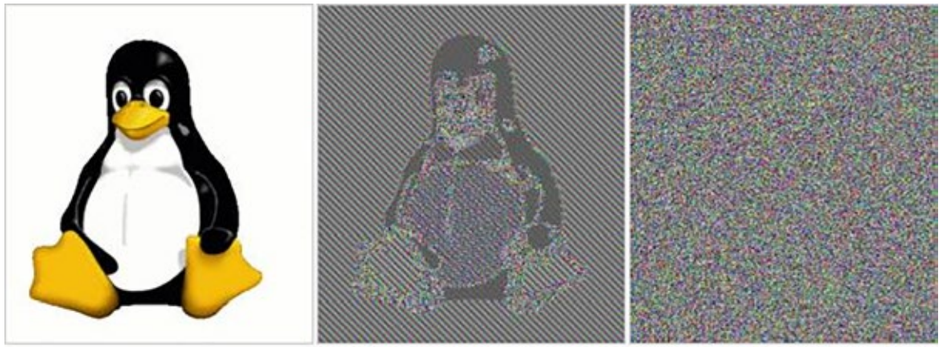


Abbildung 1

Die wichtigsten IT-Security Basics für Kryptographie

Kryptographie ist ein wichtiger Bestandteil der heutigen IT Welt. Sie ist essenziell, um die Schutzziele Vertraulichkeit, Integrität und Authentizität sicherzustellen. Aktuelle Kryptographie-Algorithmen gelten als mathematisch sicher. Selbst wenn sich NSA, Google und Amazon zusammenschließen, würden sie mehrere Milliarden Jahre benötigen, um Algorithmen wie AES-128 zu knacken. Wieso liest man trotzdem immer wieder von Sicherheitslücken mit Kryptographie Bezug?

Das Problem liegt meist in der Implementierung und Konfiguration. Genauer gesagt, lassen sich die häufigsten Probleme in folgende Kategorien unterteilen:

Konfiguration und Wahl der Parameter

Konfigurationsfehler oder schlechte Parameterwahl können ein Kryptosystem schwächen. Hier zwei Beispiele für symmetrische und asymmetrische Kryptosysteme:

1. AES (Advanced Encryption Standard – symmetrische Kryptographie) hat mehrere Verschlüsselungsmodi. Einer dieser Modi ist der Electronic Code Book (ECB) Modus. ECB verschlüsselt jeden Block mit demselben Schlüssel. Dies erlaubt das Erkennen von Mustern, hier am Beispiel einer Bilddatei (Abbildung 1).
2. Bei RSA (Rivest–Shamir–Adleman – asymmetrische Kryptographie) gibt es vielerlei Fallstricke. So sollte darauf geachtet werden, dass die Nachricht m hoch e größer als der Modulus n ist, da dieser sonst keinen Effekt hat. In diesem Falle lässt sich ein Ciphertext entschlüsseln, in dem einfach die „e"-te Wurzel genommen wird. Da e Teil des Public Keys ist, ist e in der Regel bekannt.

Verwendung schwacher kryptographischer Algorithmen

Häufig werden noch alte kryptographische Algorithmen verwendet, um kompatibel mit alten Geräten und Software zu sein. So empfehlen Mozilla und das BSI den Einsatz von TLS 1.2 und 1.3. Dennoch verwenden viele aus Gründen der Abwärtskompatibilität noch TLS 1.0 oder sogar SSLv3. Doch selbst TLS 1.0 kann noch ein akzeptables Sicherheitsniveau und dennoch eine große Kompatibilität bieten, wenn die unsicheren Ciphersuites entfernt werden. Chiffren, die Hash-Verfahren wie MD5, SHA1 oder Kryptoalgorithmen wie DES, RC4 und AES im ECB Modus verwenden, sollten nicht genutzt werden. Auf gar keinen Fall verwendet werden dürfen sogenannte Null, Anonymous oder Export-Verfahren. Null-Verfahren sind nur zu Testzwecken da, hier findet keinerlei Verschlüsselung statt. Anonymous-Verfahren authentifizieren den Server nicht. Dies kann sich ein Angreifer zunutze machen und sich unbemerkt in die Verbindung drängen (Man-in-the-Middle) und der anderen Seiten jeweils seine Public Keys übermitteln. Er kann nun den Inhalt der Nachrichten lesen und verändern, ohne dass dies auffällt. Export-Verfahren haben drastisch begrenzte Schlüsselgrößen und können mit entsprechender Hardware in wenigen Minuten geknackt werden.

Schlechte Pseudozufallszahlen

Moderne symmetrische Kryptographie baut auf der Verschlüsselungsidee des OneTimePad auf. Da es wenig praxistauglich ist, mit dem Empfänger erst einmal Schlüsselmaterial in der Länge der Nachricht auszutauschen, werden Pseudo Random Number Generator (PRNG) verwendet. Nicht ausreichend gute Zufallszahlen können jedoch dazu führen, dass die Verschlüsselung geknackt wird, wie beim Debian OpenSSH Debakel geschehen. Selbst wenn gute Zufallszahlen auf dem System generiert werden, müssen noch entsprechende Funktionen verwendet werden. Die meisten Programmiersprachen bieten mehrere Methoden an, um Zu-

Wilfried Kirsch, Senior Consultant, softScheck GmbH

Prof. Dr. Hartmut Pohl, CEO, softScheck GmbH

Abbildung 2

fallszahlen zu generieren. Nur Funktionen, die auf den Entropy-Pool des Betriebssystems zugreifen, eigenen sich für Kryptographie. In Java muss beispielsweise die Funktion java.security.SecureRandom anstelle von java.util.Random verwendet werden.

Das wohl bekannteste Beispiel für nicht verwendete Zufallszahlen ist die PlayStation 3. Zum Signieren ausführbarer Dateien nutzt diese den auf Elliptischer-Kurven-Kryptographie basierenden ECDSA (Elliptic Curve Digitial Signature Algorithm). In die Berechnung der Signatur fließt eine Nonce (zufällige Zahl, welche nur einmal verwendet werden sollte), k, ein. Diese zufällige Zahl k war bei der PlayStation 3 allerdings konstant. Gelingt es einem Angreifer zwei Signaturen mit gleichem k zu erhalten, so kann er den Wert von k ermitteln. Kennt er k, kann er den privaten Schlüssel berechnen. Somit kann der Angreifer eigene Programme signieren und im Falle der PlayStation die Beschränkung zur Nutzung offizieller Software umgehen.

Unpassender Algorithmus für den Anwendungszweck

Ein weiterer Fallstrick ist die Fülle verschiedener Algorithmen die existieren und unter denen sorgfältig ausgewählt werden muss. So sollten Passwörter beispielsweise gehasht und gesaltet gespeichert werden. Es gibt Hash Algorithmen wie Argon2 oder Scrypt, die extra für das sichere Hashen von Passwörtern entwickelt worden sind. Zum Hashen größerer Datenmengen sind diese allerdings aufgrund ihrer langsamen Geschwindigkeit ungeeignet.

Aufgrund der Vielzahl an möglichen Sicherheitslücken im Bereich der Kryptographie und des potenziell großen Schadens der entstehen kann, empfiehlt es sich, einen Experten hinzuziehen, der die Anwendung der Kryptographie im Produkt untersucht.

Seitenkanalangriffe

Kann ein Angreifer physisch auf die Hardware zugreifen, in der Kryptographie-Operationen stattfinden, so kann er Seitenkanalangriffe versuchen. Bei einer Seitenkanalattacke, wird nicht der Algorithmus selbst angegriffen, sondern dessen physische Implementierung: Der Angreifer versucht aus Daten, die der Chip bei Kryptographie Operationen erzeugt, Rückschlüsse auf den verwendeten Schlüssel oder den Klartext zu erlangen. Diese Daten können die Dauer (Timing Attack), der Stromverbrauch oder die elektromagnetische Abstrahlung während der Operation sein. Es ist sogar möglich, anhand der Geräusche, die der Chip erzeugt, Rückschlüsse zu ziehen. Folgende Bilddatei (Abbildung 2) zeigt den Stromverbrauch bei einer Potenzrechnung.

Um diese möglichst schnell zu berechnen, wird häufig die binäre Exponentation angewandt. Hierbei wird der Exponent in Einsen und Nullen zerlegt und dann schrittweise durchgegangen. In diesem Bild ist der Exponent 11000 also 24 im Dezimalsystem. Für jede 1 wird quadriert und multipliziert. Bei einer 0 hingegen nur multipliziert. Dies benötigt unterschiedlich viel Strom bzw. dauert unterschiedlich lange. Mit geübtem Auge lässt sich somit anhand der Stromverbrauchsanalyse der Exponent ableiten. Exponenten spielen beispielsweise bei RSA eine große Rolle. Textbook RSA verschlüsselt eine Nachricht m wie folgt: c = me mod n. Die Entschlüsselung geschieht durch m = cd mod n. Durch die Analyse kann ein Angreifer e oder d herausfinden. Kann er eine Stromanalyse beim Entschlüsseln durchführen, so gelangt er in Besitz des Private Key d und kann die Nachricht entschlüsseln.

Noch effektiver ist die Differential Power Analysis. Diese beruht darauf, dass das Verarbeiten von Zahlen unterschiedlich viel Strom verbraucht. Je mehr Einsen enthalten sind, desto höher der Stromverbrauch. Dieser Effekt ist allerdings so minimal, dass die Schwankungen es unmöglich machen, dies zu erkennen. Führt man die Messung allerdings mehrere 100 Male aus, so kann man die Schwankungen herausrechnen. Damit ist es Beispielweise möglich, den 16 Byte Schlüssel von AES zurückzurechnen.

Die vorgestellten Seitenkanalangriffe lassen sich relativ leicht durch zufällige Dummy Operation massiv erschweren. Es gibt auch eine Reihe an Seitenkanalangriffe, welche auf Fehlerinduzierung beruhen, sowie Mitigationen dagegen.

Fazit

Trotz sicherer Kryptosysteme kommt es aufgrund vielerlei Dinge die beachtet werden sollten, doch häufig bei Entwicklern unbekannt sind, zu Fehlern. Auf keinen Fall sollten Entwickler allerdings resignieren und eigene Kryptographie Systeme entwickeln, da die Erfahrung zeigt, dass diese häufig noch Fehler anfälliger sind. Es müssen aktuelle, sichere Kryptoalgorithmen verwendet und nach Best-Practice Richtlinien implementiert werden. Soll auf Nummer sicher gegangen werden, ist es ratsam dies später von externen Penetrationstestern und Kryptographen testen zu lassen.

Wilfried Kirsch, Prof. Dr. Hartmut Pohl

1.7 DATEN-SICHERHEIT

Defekte RAID-Datenträger – ungeahntes Datenmissbrauchsrisiko!

Der Ausfall von Datenträgern im Dauerbetrieb ist kein außergewöhnliches Ereignis: Gerade bei RAID- und Server-Systemen werden laufend defekte Festplatten und SSDs ausgetauscht – in großen Rechenzentren tägliche Routinearbeit. Der Ausfall eines einzelnen Mediums bedeutet bei modernen Systemen mit Redundanz keinen Datenverlust, der defekte Datenträger wird einfach durch eine neue Festplatte oder SSD ersetzt.

Doch was geschieht mit den defekten Datenträgern?

In vielen Unternehmen ist es üblich die defekten Datenträger zu sammeln. Dies geschieht entweder in der internen IT-Abteilung oder aber extern in Systemhäusern oder bei EDV-Betreuern. Die ausgefallenen Medien werden somit häufig außer Haus gebracht, meist ohne Wissen um die potentielle Gefahr. Ist die Garantie der Festplatten oder SSDs noch nicht abgelaufen, werden diese zum Austausch an den Hersteller gesendet, in anderen Fällen über Auktionsplattformen verkauft. Dieses Risiko lauert auch bei Managed Serverhousing oder Cloud-Diensten: Der Kunde bemerkt überhaupt nicht, wenn seine Datenträger ausgetauscht werden.

Datenrettung ist sogar von nur einer einzelnen RAID-Festplatte möglich

RAID-Systeme verteilen die Daten in Blöcken abwechselnd über alle Datenträger. Man könnte somit dem Trugschluss erliegen, dass eine einzelne Platte aus dem RAID-Verbund für einen potentiellen Missbrauch gar keine verwertbaren Informationen enthält. Die Größe der einzelnen Blöcke beträgt meistens zwischen 32 und 128 kByte, das entspricht im Durchschnitt der Größe eines Textdokuments oder einer Tabellenkalkulation. Somit ist es möglich, auch von nur einem einzelnen Datenträger eines RAID-Verbundes unternehmenskritische Informationen zu gewinnen, welche in falsche Hände gelangen können. Auch bei der Speicherung von Datenbanken ist es so möglich, viele sensible Datensätze zu extrahieren.

Wie schütze ich meine Daten vor Missbrauch?

Ein sicheres Löschen des ausgefallenen Datenträgers ist vor dem Garantieaustausch meistens aufgrund des Defekts nicht mehr möglich. Viele Hersteller bieten deshalb gegen Aufzahlung spezielle Supportverträge an, bei denen der Kunde defekte Datenträger nicht zurückgeben muss, sondern diese behalten darf. Idealerweise wird der Datenträger bereits bei Inbetriebnahme des RAIDs sicher verschlüsselt. Bei einem späteren Ausfall kann dieser dann gefahrlos außer Haus gegeben werden. Generell ist es wichtig, klare Richtlinien festzulegen, was mit defekten Datenträgern passieren soll, egal ob es die interne oder externe IT oder den Betreiber eines Rechenzentrums betrifft.

Dipl. Ing. Nicolas Ehrschwendner

Dipl. Ing. Nicolas Ehrschwendner, Geschäftsführender Gesellschafter, Attingo Datenrettung

Trügerische Sicherheit: Datenverlust trotz RAID

RAID-Systeme, also ein Verbund von mehreren Datenträgern wie Festplatten oder SSDs, sind gemeinhin der Standard für vermeintlich sichere Datenspeicherung. Sie werden sowohl in Server- und NAS-Systemen als auch bei Workstations eingesetzt – von Privatpersonen über KMUs bis hin zu großen Konzernen. Im Gegensatz zu einem PC oder Laptop besteht bei einem RAID-Verbund aufgrund der höheren Anzahl von Datenträgern paradoxerweise auch eine erhöhte Wahrscheinlichkeit für den Ausfall einer Festplatte oder SSD. Ohne Zugriff auf die wichtigen Daten kann im Worst Case der gesamte Betrieb stillstehen – Datenbanken, E-Mails und Dateiablagen sind mit einem Schlag offline!

Ein RAID ist kein Ersatz für Datensicherung!

RAID-Systeme erzeugen mit Hilfe teils komplizierter Algorithmen gezielt redundante Informationen. Dadurch bleibt beim Ausfall – je nach RAID-Level – einer oder mehrerer Festplatten die Funktionalität gewährleistet und nach Ersetzen des defekten Datenträgers kann im Optimalfall durch ein Rebuild der ursprüngliche Zustand wiederhergestellt werden. Diese Redundanz darf jedoch keineswegs mit einer Datensicherung verwechselt werden.

IT-Administratoren und EDV-Spezialisten sind nicht selten über den plötzlichen Verlust der Daten

überrascht, ein teures Enterprise-Storage wurde angeschafft und es gab im Vorfeld keine Anzeichen eines baldigen Defektes. Des Rätsels Lösung ist oft ein multipler Ausfall von Festplatten oder SSDs. Meistens haben die Datenträger in den Storages den gleichen Lebenslauf: Produktion, Transport sowie Betriebsumgebung sind für alle im RAID vorhandenen Datenträger identisch. Auf all diesen Etappen lauern potentielle Gefahren:

Produktion
Defekte können bereits in der Produktion beim Hersteller auftreten. Oft weisen ganze Chargen von Festplatten Serienfehler auf. Diese können im Bereich der Firmware (interne Software eines Datenträgers), der Mechanik oder der Elektronik liegen. Da in RAID-Systemen nahezu immer Festplatten derselben Charge verbaut werden, können etwaige Serienfehler innerhalb eines kurzen Zeitraums auftreten. Gerade in der Nacht oder am Wochenende wird der erste Defekt oft nicht bemerkt oder sogar ignoriert – sobald dann auch der zweite Datenträger defekt wird, ist ein RAID5 bereits nicht mehr verfügbar.

Transport
Eine weitere Ursache für den nahezu gleichzeitigen Ausfall von mehreren Festplatten ist der Transport der Datenträger von der Fabrik über Reseller bis zum Einsatzort der Server oder RAIDs. Durch überhitzte Container, Erschütterungen oder anderen Umwelteinflüssen können hier bereits Schäden entstehen, die später im Betrieb zum Ausfall führen. Auch hier gilt: Selbe Charge bedeutet identische Probleme.

Betriebsumgebung
Nicht zuletzt spielt auch der laufende Betrieb eine wesentliche Rolle: Erschütterungen, Überhitzung und Überspannung können die Lebenszeit der Festplatten im RAID-Verbund wesentlich verkürzen, wiederum mit der gleichen Auswirkung auf alle Datenträger.

Elementarereignisse
Gewitter, Hochwasser, Feuer oder Erschütterungen (beispielsweise von Erdbeben oder Bauarbeiten vor der Tür) zerstören immer wieder mit einem Schlag mehrere Datenträger in einem RAID.

Der Ausfall eines RAID-Systems ist also durchaus wahrscheinlicher als man gemeinhin annehmen würde.

Ausfallsprävention bei RAID-Systemen

Zunächst scheint es sinnvoll, einfach Datenträger verschiedener Hersteller in RAID-Systemen einzusetzen. Dies kann jedoch zu Performance- und Kompatibilitätsproblemen führen. Die einzig sinnvolle Lösung ist das Anlegen einer externen Datensicherung, denn auf ein RAID-System alleine darf man sich nicht verlassen.

Darüber hinaus sollte Folgendes beachtet werden:
- Laufende Datensicherungen auf anderen externen Systemen abspeichern und nicht auf dem RAID selbst.
- Die Sicherungen in regelmäßigen Abständen auf deren Vollständigkeit und Funktionalität überprüfen.
- Konstantes Monitoring betreiben, um bereits beim Ausfall der ersten Platte eine Benachrichtigung per E-Mail, SMS oder Messenger-Dienst zu erhalten.
- Vor dem Einspielen von Firmware-Updates ein vollständiges Backup anlegen und auf Integrität prüfen.
- Falls eine Datensicherung vorhanden ist, sollten die Daten nicht auf die ursprünglichen Datenträger des RAID-Systems zurückgespielt werden, sondern neue Datenträger verwendet werden. Denn sollte die Datenrücksicherung doch nicht funktionieren oder nicht alle Daten vollständig gesichert worden sein, können professionelle Datenrettungsunternehmen die fehlenden Daten von den ursprünglichen RAID-Datenträgern meist noch rekonstruieren.

Dipl. Ing. Nicolas Ehrschwendner

IT-Sicherheit und Datenschutz: Die Gesetzeslage in den USA und Deutschland im Vergleich

Dieser Beitrag stellt keine Rechtsberatung dar und ist nicht von einem Rechtsanwalt oder Datenschutzexperten verfasst worden. Eine tieferreichende Analyse kann deshalb nicht geleistet werden. Er soll zunächst nur einen Überblick über die verschiedenen Gesetze und Verordnungen in den beiden vorgestellten Ländern geben.

Mit der DSGVO und dem IT-Sicherheitsgesetz hat die Bundesregierung in Zusammenarbeit mit der Europäischen Kommission in den letzten Jahren zwei wichtige Projekte für mehr IT-Sicherheit und Datenschutz in Deutschland eingeführt. In den USA gibt es zwar keine ähnlichen Gesetze, aber dafür zahlreiche Regelungen und Standards, die von den dortigen Unternehmen befolgt werden. Strafen sind bislang nur bei der DSGVO vorgesehen.

Die Lage in den USA
Die Gesetze zur IT-Sicherheit und Datenschutz in den USA sind relativ flexibel und im Vergleich weniger streng gehalten. Sie sind aus hundert Jahren Erfahrung mit Datenschutz- und Strafrechtsnormen erwachsen und haben sehr wenig mit dem Schutz der Vertraulichkeit und der Integrität von Systemen, Personen, Netzwerken und Daten zu tun. Die Normen wurden im Laufe der Zeit überarbeitet, um den heutigen Anforderungen an die IT-Sicherheit und den Datenschutz gerecht zu werden. Außerdem hängt die Verordnung von Datenschutzgesetzen stark von staatlichen Reaktionen auf Vorfälle und private Klagen gegen Unternehmen ab. Dieses Konstrukt des US-amerikanischen Rechtssystems führt dazu, dass die Gesetzeslage zur IT-Sicherheit und zum Datenschutz nur als ein „Framework“ von Regeln und Vorschriften betrachtet wird, welches keinen zuverlässigen Schutz der Privatsphäre gewährleistet.

Die Gesetze betreffen Unternehmen je nach Branche und geografischem Standort. Besonders auffällig ist, dass es kein übergreifendes Bundesgesetz gibt, das Unternehmen dazu zwingt, angemessene Sicherheitsmaßnahmen umzusetzen. Das Gesetz, dass dem am nächsten kommt, trat im Jahr 2014 mit dem Cybersecurity Enhancement Act als Bundesgesetz in Kraft. Es verpflichtet das National Institute of Standards and Technology (NIST), branchenspezifische Richtlinien und Best Practices für Privatunternehmen weiter zu entwickeln. Das Dokument behandelt die 20 wichtigsten Schritte, die Unternehmen befolgen sollten, um die IT-Sicherheit kontinuierlich zu erhöhen. Die NIST-Richtlinien sind sehr Praxis-orientiert und werden weltweit anerkannt. In der Zwischenzeit verlangt der Cybersecurity Act (2015), dass private Anbieter Informationen über Angriffe mit anderen Anbietern und der Behörde austauschen, während sie die Vertraulichkeit und die Integrität aller Informationen bewahren. Der Federal Cybersecurity Enhancement Act (2016) und der Federal Information System Modernization Act, 2014 (FISMA) weisen das Homeland Security-Ministerium an, kritische Cybersecurity Services und -entsprechende Infrastrukturen bereitzustellen, sodass Bundesbehörden Notfallpläne leicht umsetzen können. Darüber hinaus konzentrieren sich der Gramm-Leach-Bliley Act (1999) und der Electronic Communications Privacy Act (ECPA) überwiegend auf den Datenschutz und die Privatsphäre. Sie schreiben vor, wie Unternehmen mit Daten von Privatpersonen umgehen sollten – bei der Zusammenstellung, Anwendung und Offenlegung von personenbezogenen Informationen¬. Auf Bundesebene sieht die Lage so aus, dass Kalifornien das erste Bundesland war, das ein Meldepflichtengesetz (2003) bei Sicherheitsverletzungen durchgesetzt hat. Unternehmen sind demnach verpflichtet, Personen deren private Daten gefährdet oder unsachgemäß erfasst wurden, rechtzeitig zu benachrichtigen. Im Januar 2019 wurde darüber hinaus ein neues Gesetz verabschiedet, indem Unternehmen verpflichtet sind bei Ransomware-Angriffen die Betroffenen und die Staatsanwaltschaft innerhalb von 30 Tagen zu informieren. Das neue Gesetz ist eine Reaktion auf den North Carolina Data Breach Report 2018, der mehr als 1.057 Datenschutzverletzungen aufdeckte.

Regulierungen in der Finanz- und Gesundheitsbranche
Beide Sektoren sind in den USA sowohl auf Bundes- als auch Bundesstaatebene gesondert geregelt. Das Consumer Financial Protection Bureau (CFPB) arbeitet mit verschiedenen Finanz- und staatlichen Versicherungsaufsichtsbehörden zusammen, wobei sie bestimmte Regeln für Finanzdienstleister auf Grundlage des Gramm-Leach-Bliley Act (GLB) und des Electronic Communications Privacy Act (ECPA) aufstellen. Die Securities and Exchange Commission (SEC) überwacht die Einhaltung von IT-Sicherheitsanforderungen sowie die Arbeit aller Händler und Anlageberater. Diejenigen, die die IT-Sicherheitsrichtlinien und Verfahren nicht einhalten, werden dafür bestraft. Ein ehemaliger Makler von Charles Schwab & Co. wurde von der Financial Industry Regulatory Authority, Inc. (FINRA-beaufsichtigt von SEC) zu einer Geldstrafe von 5.000 US-Dollar verklagt. Zudem wurde er für 90 Tage suspendiert, weil er fast 800.000 US-Dollar fälschlicherweise an jemanden überwiesen hat, der sich als ein Kunde von ihm ausgegeben hat. Auf Bundeslandebene hat das New York State Department of Financial Services im Jahr 2017 neue Reglungen zum Schutz von Kundeninformationen und Informationstechnologiesysteme für Finanzdienstleister festgelegt. Das Gesetz verpflichtet jeden Finanzdienstleister, sein spezifisches Risikoprofil zu bewerten und eine passende Risiko-Controlling-Maßnahme zu entwickeln. Im Bereich des Datenschutzes gibt es noch nicht viele Gesetze und vor allem noch weniger, die personenbezogene Daten schützen. Ein aktuelles Datenschutzgesetz im Bundesstaat North Carolina verlangt ebenfalls, dass Finanzdienstleister die Zustimmung ihre Kunden einholen müssen, wenn sie diese auf Kreditwürdigkeit prüfen.

Die Gesundheitsbranche unterliegt dem Health Insurance Portability and Accountability Act (HIPAA) von 1996, der im Einklang mit dem Gramm-Leach-Bliley Act (GLB) und dem Electronic Communications Privacy Act (ECPA) steht. Das HIPAA gilt für Krankenkassen, Gesundheitszentren und alle Gesundheitsdienstleister, die Gesundheitsinformationen in elektronischer Form unter sich und mit ihren Geschäftspartnern teilen. Das Gesetz zielt darauf ab, Gesundheitsinformationen und die Privatsphäre der Patienten zu schützen. Wie bereits angedeutet, sind die Regelungen sehr flexibel und skalierbar gestaltet, sodass jedes Unternehmen die Freiheit hat, die Richtlinien, Verfahren und Informationstechnologien umzusetzen, die am besten zu seiner Größe, Unternehmensstruktur und Risikopotential passen.

Cyberkriminalität und Strafen in den USA
In der Regel führen Verstöße gegen Bundes- und Bundesstaats-Datenschutzgesetze zu zivil-, aber nicht strafrechtlichen Strafen. Das Gesetz sieht vor, dass Privatpersonen Unternehmen vor Gericht ziehen dürfen, wenn sie der Meinung sind, dass ein Unternehmen gegen die Gesetze verstoßen hat. Cyberkriminalität in den USA umfasst Phishing, Hacking, Identitätsbetrug, elektronischer Diebstahl, der Besitz von Hard- und

Detlev Weise, Managing Director, KnowBe4

Software für cyberkriminale Aktivitäten, die Infizierung von IT-Systemen mit Malware und Ransomware sowie Kinderpornographie (nach dem Computer Fraud and Abuse Act von 1986). Straftäter bekommen eine Strafe von bis zu 20 Jahren Gefängnis und/oder eine Geldstrafe, je nach Art und Schwere der Straftat.

Der Deutsche Ansatz für IT-Sicherheit und Datenschutz

Die EU-Datenschutzgrundverordnung (EU-DSGVO) dient als Grundlage für alle nationalen Gesetze, die sich mit Fragen zur IT-Sicherheit und zum Datenschutz innerhalb der Europäischen Union (EU) beschäftigen. Im Gegensatz zu den US-amerikanischen Gesetzen, die viel entspannter und manchmal widersprüchlich sind, ist die EU-DSGVO viel strukturierter, strenger und sie betrifft alle Unternehmen, die innerhalb der EU tätig sind. Die EU-DSGVO betrifft auch Unternehmen, außerhalb der EU, die Informationen von EU-Bürgern verarbeiten. Art. 5 Abs. 1 und Art. 32 der EU-DSGVO verpflichtet Unternehmen dazu alle erforderlichen IT-Sicherheitsmaßnahmen einzusetzen, um Vorfälle rechtzeitig zu erkennen, zu überwachen, im besten Fall zu verhindern und deren Folgen abzumildern. Alle Maßnahmen müssen sicherstellen, dass die Vertraulichkeit und die Integrität personenbezogener Daten und Systeme im Unternehmen gewahrt bleiben. Zusätzlich müssen Unternehmen einen Datenschutzbeauftragten benennen sowie den Stand der IT regelmäßig überprüfen und aktualisieren. Die EU-DSGVO verlangt, dass Unternehmen bis spätestens 72 Stunden nach der Kenntnis des Sicherheitsvorfalls, diesen Vorfall an die zuständige Datenschutzbehörde melden müssen. Zusätzlich sind Unternehmen verpflichtet, Informationen in Bezug auf den Umfang des Sicherheitsvorfalls, den Folgen der Datenschutzverletzung sowie die eingesetzten Maßnahmen zur Behebung des Vorfalls bei der zuständigen Behörde anzugeben. Personen, deren private Daten von der Verletzung betroffen sind, müssen ebenfalls rechtzeitig informiert werden.

Auf staatlicher Ebene regelt die EU-DSGVO den allgemeinen Umgang mit personenbezogenen Daten, die in Informations- und Kommunikationssystemen oder manuell innerhalb Deutschlands verarbeitet werden. Zur Sicherstellung der Einhaltung der Gesetze sind u.a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) und je nach Bundesland das Landesamt für Sicherheit in der Informationstechnik (LSI) zuständig.

Das BSI stellt u.a. mit dem IT-Grundschutz Richtlinien und Empfehlungen auf, die als Richtlinien für Unternehmen dienen sollten. Das Landesamt bietet Schulungen und Beratungsdienste sowie technische Unterstützung für Kommunen, Privatpersonen und Unternehmen, bezüglich der IT-Sicherheit und des Datenschutzes im Bundesland an. Aber, eine reibungslose Zusammenarbeit zwischen den Behörden auf Bundes- und Landesebene ist in der Regel nicht immer der Fall.

Kritische Infrastrukturen

Neben der EU-DSGVO gilt seit 2016 das IT-Sicherheitsgesetz für kritische Infrastrukturen nämlich für die Sektoren Informationstechnik und Telekommunikation, Gesundheit, Energie, Finanzen und Versicherung, Transport und Verkehr, Wasser und Ernährung. Dieses Gesetz wird dieses Jahr noch einmal eine Aktualisierung erfahren und dadurch an die Vorgaben der EU-DSGVO angepasst werden. Darüber hinaus steht außerdem noch die eprivacy Verordnung des Europäischen Parlaments vor der Tür. Für viele Branchen gelten darüber hinaus auch noch branchenspezifische Gesetze. So müssen Finanzdienstleister im Einklang mit § 25a Kreditwesengesetz und § 33 Wertpapierhandelsgesetz stehen. Beide Gesetze verlangen, dass Finanzdienstleister ein IT-Risikomanagementsystem entwickeln. Bei der Nichteinhaltung können sie eine Geldstrafe von bis zu 5 Millionen Euro erhalten. Unternehmen können auch dazu aufgefordert werden, bestimmte Arten von Geschäften ganz oder teilweise nicht oder nur eingeschränkt durchzuführen. Hinsichtlich der Meldepflicht müssen sich kritische Infrastruktur-Betreiber in Fällen von Sicherheitsverletzungen beim BSI melden, um Angaben zur erheblichen Störung der Verfügbarkeit, Vertraulichkeit und Integrität ihrer IT zu geben.

Cyberkriminalität und Strafen in Deutschland

Grundsätzlich sieht das deutsche Gesetz vor, dass jede Person und jedes Unternehmen, das im Falle eines Sicherheitsvorfalls einen Schaden erlitten hat, zivilrechtliche Klage gegen den Straftäter einleiten kann. Die Cyberkriminalität in Deutschland ist derjenigen in den USA sehr ähnlich. Die Straftäten werden von ein bis zu zehn Jahre Gefängnis oder eine Geldstrafe bestraft, je nach Straftat natürlich. Unter dem deutschen IT-Sicherheitsgesetz können Unternehmen bei Verstößen mit einer Strafe von bis zu 100.000 Euro belegt werden. Bei der Nichteinhaltung verhängt die EU-DSGVO eine Geldstrafe von bis zu 10 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Kürzlich wurde Google von der französischen Behörde CNIL zu einer 50 Millionen Euro Strafe verurteilt, weil es die Daten seiner Nutzer nur unzureichend schützt.

„Wir können die absolute, die totale Sicherheit gerade im Bereich der Cybersicherheit nicht versprechen," betonte Horst Seehofer, Bundesminister des Innern, für Bau und Heimat anlässlich des Datenskandals um gehackte Politiker-E-Mailkonten. Mit anderen Worten, Privatpersonen sollten sich nicht nur auf das Gesetz verlassen, um ihre Privatsphäre zu schützen. Jeder muss sich um seine Privatsphäre sorgen und Unternehmen können ihren Mitarbeitern dabei helfen, ihre Sicherheitssysteme weiter zu verstärken. Genau genommen brauchen Unternehmen eine menschliche Firewall, die letzte Verteidigungslinie gegen Sicherheitsangriffe. Das „New School Security Awareness-Training" besteht aus simulierten Phishing-Angriffen, die von der IT-Abteilung des Unternehmens spontan und regelmäßig an die Mitarbeiter geschickt werden. Sie sollen diese dazu zu bringen, Phishing-E-Mails leicht zu erkennen und weniger empfänglich gegenüber solchen betrügerischen und bösartigen E-Mails zu sein. Laut einer Umfrage haben 64 Prozent der Befragten in den USA festgestellt, dass das Security Awareness-Training ihren Unternehmen geholfen hat, Sicherheitsangriffe frühzeitig zu identifizieren und zu vermeiden, indem sie entweder auf einen Hackerversuch oder eine potenzielle Schwachstelle aufmerksam gemacht wurden.

Fazit

Die Gesetzeslage zur IT-Sicherheit und zum Datenschutz in Deutschland sind deutlich strenger im Vergleich zu den eher weniger verbindlichen Rechtsvorschriften in den USA. Trotzdem befinden sich noch Lücken im Gesetz, genauso in den Sicherheitssystemen von Unternehmen und Behörden, die Cyberkriminelle zu ihren Vorteilen nutzen können.

Detlev Weise

Q&A für Digitale Welt über Cybersicherheit bei Geldautomaten

Elida Policastro, Regional Vice President – Cybersecurity Division bei Auriga, erklärt im Gespräch, wie es aktuell um die Sicherheit von Geldautomaten steht und was Geldinstitute tun können, um ihre Geräte zu schützen und Finanzbetrug vorzubeugen.

1. Wie ist der aktuelle Stand der Cybersicherheit bei Geldautomaten?

Cyber-Angriffe auf Geldautomaten und die Systeme, die Geldautomaten steuern, wie z.B. zentrale Server, stellen weltweit eine akute und wachsende Bedrohung dar. Einige Formen von Cyber-Angriffen führen zum Diebstahl persönlicher Daten wie Kontonummern und PIN-Codes. Um diese Daten jedoch in Geld umzuwandeln, sind weitere Anstrengungen nötig. So ist es für Cyber-Kriminelle, die es auf Geldautomaten abgesehen haben, viel attraktiver, sich das Bargeld direkt an dem Geldautomaten zu beschaffen. Sogenannte „Jackpotting"-Angriffe auf Geldautomaten, bei denen physische und softwarebasierte Schwachstellen ausgenutzt werden, um den Geldautomaten zur Bargeldausgabe zu überlisten, sind beliebt, da sie eine sofortige Belohnung bieten. Finanzinstitute auf der ganzen Welt haben allein in den letzten fünf Jahren Millionen durch Jackpotting verloren. So hat beispielsweise die Bankautomaten-Malware Ploutus, die erstmals 2013 in Mexiko entdeckt wurde, weltweit Verluste von über 450 Millionen Dollar (ca. 398 Millionen Euro) verursacht.

2. Wie groß sind die Schwachstellen bei Geldautomaten für Cyber-Angriffe?

Auf Geldautomaten werden sowohl physische (z.B. Skimming, Gas) als auch logische Angriffe (z.B. Malware, Blackbox) verübt. Sie sind für Angreifer aus verschiedenen Gründen ein attraktives Ziel: Zum einen ist das enthaltene Bargeld ein Anreiz sowie die vertraulichen Informationen (Kredit-/Debitkarten und PINs), die ebenfalls in Geld umgewandelt werden können.

Zum anderen haben die Geräte einige Schwachstellen, die Kriminelle für ihre Zwecke ausnutzen. Geldautomaten sind oftmals schlecht überwacht und es werden wenige logische Maßnahmen ergriffen, um die Sicherheit der Daten zu gewährleisten. Eine weitere Schwachstelle sind die zahlreichen Akteure (Finanzinstitute, Dienstleistungsanbieter, Entwickler, Installateure...), die im Bereich Cybersecurity tätig sind. Nicht alle Beteiligten arbeiten zuverlässig und auch, dass zu viele Akteure Admin-Rechte besitzen, kann eine potenzielle Gefahrenquelle sein.

Das Ökosystem „Geldautomaten" ist komplex, es besteht aus heterogener Hardware und Software und oftmals fehlen in den Organisationen proaktive Aktualisierungsrichtlinien und ein zentraler Überblick über die Sicherheitsstruktur. Veraltete Hardware und Software können sogar dazu führen, dass die PCI-Regeln nicht 100% erfüllt werden, obwohl Banken dazu verpflichtet sind.

Finanzinstitute stehen vor einer Vielzahl von Herausforderungen, um Geldautomaten rund um die Uhr verfügbar zu machen und gleichzeitig die größtmögliche Sicherheit zu gewährleisten. Einerseits gilt es, den Aufwand der SW-Bereitstellung und der HW-Wartung zu reduzieren und den Überblick und die Kontrolle über Änderungen der Software und der Hardware zu behalten. Andererseits müssen Sicherheitsrichtlinien umgesetzt und eingehalten werden und die integrierte Sichtbarkeit und Verwaltung des GAA-Sicherheitsstatus gewährleistet werden.

3. Wie aktiv sind Cyberkriminelle beim Angreifen von Geldautomaten und wie erfolgreich sind sie?

Cyberkriminelle haben erkannt, dass Geldautomatennetzwerke oft eine Schwachstelle in der Sicherheitsinfrastruktur einer Bank sind. Einer der Hauptgründe dafür ist, dass es in Geldautomatennetzwerken eine Menge veralteter Hard- und Software gibt, weil diese sehr teuer und schwer zu aktualisieren ist. Leider heißt das auch, dass diese Systeme wahrscheinlich unsicher sind. Viele Geldautomaten laufen noch unter Windows 7 oder sind dabei, auf Windows 7 zu migrieren, das von Microsoft nicht mehr unterstützt wird. Das bedeutet,

Elida Policastro, Regional VP – Cybersecurity Division, Auriga

dass Windows-7-Nutzer anfällig für Angriffe sind, da sie keine Updates von Microsoft mehr erhalten, die sie vor neuen Bedrohungen schützen. Wir schätzen, dass etwa 40 Prozent der Geldautomaten weltweit mit einem noch älteren Betriebssystem (OS) arbeiten, das von Microsoft seit 2014 nicht mehr unterstützt wird, nämlich Windows XP. Diese Geräte sind dann noch anfälliger für Angriffe.

Neben den Schwachstellen des Betriebssystems ist einer der Hauptangriffsvektoren auf Geldautomaten die XFS-Schicht, die Standardschnittstelle, die es Multivendor-Software ermöglichen soll, auf den Geldautomaten und anderer Hardware der Hersteller zu laufen. Die XFS-Schicht verwendet Standard-APIs zur Kommunikation mit Self-Service-Anwendungen. Es gibt jedoch keinen automatischen Authentifizierungsprozess, der damit einhergeht, so dass Kriminelle in der Lage sind, diese Schwachstelle auszunutzen. Cyber-Kriminelle setzen Malware auf Hardware-Geräten wie Geldautomaten ein, um „Auszahlungsbefehle“ anzufordern und Bargeld auszugeben, auf dem Kartenlesegerät, um Kartennummern zu stehlen, und auf dem Pinpad, um Pin-Nummern zu erhalten. Das macht die XFS-Schicht zu einem sehr attraktiven Ziel.

4. Was sind Ihre Top-Tipps für Banken, bei denen ein hohes Risiko für Finanzbetrug besteht?

Die Bank sollte sich Expertenwissen von Spezialisten einholen, um ihre Sicherheitspläne und -prozesse zu überprüfen und beispielsweise Penetrationstests durchzuführen.

Wichtig ist auch die Implementierung eines umfassenden Cyber-Sicherheitsbewusstseinsprogramms für Bankmitarbeiter und Kunden sowie regelmäßige Schulungen. Obwohl Banken viele Anstrengungen unternehmen, ihre Sicherheit zu verbessern, sind die Angreifer ständig auf der Suche nach Innovationen. Die Bedrohungslandschaft verändert sich ständig und entwickelt sich immer weiter. Das bedeutet, dass die Organisationen bei der Implementierung und Prüfung ihrer Cyberabwehr proaktiv vorgehen müssen.

Cyber Threat Intelligence (CTI) kann als Frühwarnsystem genutzt werden, um potenzielle Bedrohungen zu erkennen und einzudämmen, bevor sie zu Vorfällen werden. Dieses Programm ist für jedes Unternehmen von zentraler Bedeutung, da Bedrohungen der Cybersicherheit zunehmend wahllos auftreten.

Sobald relevante Bedrohungen und Schwachstellen identifiziert werden, wird deutlich, wo und wie diese ausgenutzt werden können und welche Auswirkungen dies sowohl auf das Unternehmen als auch auf Einzelpersonen haben kann. CTI gibt Organisationen Einblick in die Gefahren und zeigt auf, welche Bereiche vorrangig behandelt werden müssen.

Während Banken sich mit der neuesten Art von Schadsoftware befassen müssen, werden viele der Angriffe versuchen, bestehende Schwachstellen auszunutzen, die möglicherweise bereits gepatcht wurden. Ein großer erster Schritt im Rahmen eines präventiven Ansatzes ist die Kombination von Schwachstellenmanagement und Aufklärung über Bedrohungen.

Wenn es um Geldautomaten geht, reichen generische Technologien zum Schutz der Endpunkte, wie Anti-Malware-Lösungen, nicht aus, da solche Technologien zum Schutz von PCs und Laptops entwickelt wurden.

Man benötigt eine zentralisierte Sicherheitslösung, die GAA-Netzwerke schützt, überwacht und kontrolliert, damit Finanzinstitute das gesamte Geldautomatennetzwerk an einem Ort verwalten können, um Malware-Versuche oder betrügerische Aktivitäten an infizierten Geldautomaten zu verhindern. Das spart wiederum Zeit und Geld.

Leider wird es immer wieder Fälle geben, in denen Ransomware erfolgreich ist. Es ist daher von entscheidender Bedeutung, dass Banken ein tragfähiges Konzept zur Geschäftskontinuität und Wiederherstellung im Katastrophenfall haben, das Teil eines umfassenden operationellen Systems der Widerstandsfähigkeit ist. Darin sollte auch enthalten sein, wie auf solche Vorfälle zu reagieren ist, sowie Möglichkeiten zur schnellen Wiederherstellung betroffener Daten und Systeme mit minimalen Auswirkungen auf den Geschäftsbetrieb.

Effektive Cybersicherheit wird immer wichtiger werden. Angesichts der Tatsache, dass Finanzinstitutionen ein ständiges Ziel von Kriminellen sind, müssen sie ihre Anstrengungen maximieren, um mit dieser dynamischen Bedrohung Schritt zu halten und um zu verhindern, dass durch Angriffe auf große Datenbanken die Daten Hunderttausender Menschen in die falschen Hände geraten.

Da Banken zunehmend auf Cloud-Technologien setzen, ist es wichtiger denn je, dass auch Cloud-Dienste den Cyber-Sicherheitsstandards entsprechen müssen, die die Integrität der Daten der Nutzer und Unternehmen, die die Dienste in Anspruch nehmen, garantieren.

Elida Policastro

Wir brauchen ein Manifest für Digitalen Optimismus

Im Jahr 1965 prophezeite ein junger Amerikaner, dass die Leistungsfähigkeit von Computern sich alle 1-2 Jahre verdoppeln wird. Was wir da noch nicht wissen: dieses „Moore'sche Law" wird unsere Innovationsdoktrin - und wird unser Leben grundlegend verändern.

Seitdem haben sich die Herzen von Computern so miniaturisiert, dass sie bald fast so häufig zu finden sind, wie Sandkörner am Strand. Dadurch ist eine gigantische Geschwindigkeit entstanden. Ein Antriebsrad, das unser Leben zu einem Ritt auf dem Drehteller macht.

Unternehmen wie Amazon, Google und Tencent wachsen dank dieser Entwicklung. Doch die meisten Firmen rutschen an den Rand der „Töpferscheibe". Genauso verhält es sich bei den Staaten. Während China, Kalifornien und Südkorea gedeihen, geraten andere Länder in schwere Nöte und haben Angst, abgehängt zu werden. Während die einen digital im Aufwind sind, drohen den anderen analoge Abwinde.

Auch in Deutschland macht uns die Beschleunigung zu schaffen. In Ausbildungseinrichtungen, der Verwaltung, der Politik und in unseren Unternehmen.

Während unser Bruttosozialprodukt von 9% im Jahr 1950 auf 0% Prozent in 2019 gesunken ist, startet China heute mit 6% Plus weiter durch. Durch die Pandemie sind zusätzlich weite Teile unserer Wirtschaft in die Rezession geraten.

Dabei geht uns doch in großen Teilen gut. Wir sind ein Land mit viel Talent, Können und Erfahrung. Wir sind leistungsfähig. Jetzt brauchen wir einen Diskurs, wie und wovon wir in Zukunft leben wollen.

Mit der Energiewende haben wir einen gewaltigen Anstoß in die Welt getragen: Solche innovativen Ansätze brauchen wir auch in anderen Feldern. Mit KI, Blockchain, CrisprCAS9, G5 sind spannende Technologien greifbar – und damit auch Chancen, Einnahmen und die Lösung vieler Probleme.

Jetzt müssen wir – trotz oder gerade wegen der Pandemie – in den Machermodus kommen.

Es gibt kaum ein Land mit so viel Liebe zur Technik wie Deutschland. Lasst uns als Optimisten die Welt weiterentwickeln. Lasst uns proaktiv die Zukunft gestalten, anstatt uns bibbernd an den Rand der Töpferscheibe zu klammern. Es gilt, das digitale Lenkrad in die Hand zu nehmen und beherzt zu steuern.

Uwe Walter ist Storytelling- und Change-Experte für Medien- und Industrieunternehmen. Er berät so unterschiedliche Kunden wie YouTube-Stars, Start-ups, Blogger, Verlage, Radio- und Fernsehsender sowie Filmproduktionen. Seine Expertise: Wie generiere ich Reichweite durch zukunftssicheres Erzählen?

Foto: Privat

CALL FOR CONTRIBUTION

für den DIGITALE-WELT-Blog

Die nächste DIGITALE WELT erscheint am 03.03.2021

Werden Sie Teil unserer hochkarätigen Autorenschaft und platzieren Sie Ihre Digitalthemen von morgen auf der Plattform von heute mit bislang **1.790.000*** Klicks.

UNSERE AKTUELLEN BLOG-RUBRIKEN:

- ✓ **Machine Learning**
- ✓ **Quantum Computing**
- ✓ **Internet of Things**
- ✓ **Digital Transformation**
- ✓ **Cyber Security**
- ✓ **Human Resource**

INTERESSE GEWECKT?

Dann melden Sie sich bei der DIGITALE WELT-Redaktion per E-Mail: **blog@digitaleweltmagazin.de**

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 30. November 2020.**

Leitfaden zur Veröffentlichung von Fachbeiträgen

FÜR IHRE EINREICHUNG SIND FOLGENDE DINGE ZU BEACHTEN:

1. Ihr Fachbeitrag erfüllt folgende Anforderungen:
   - Inhaltliche Orientierung an den Blog-Rubriken der DIGITALEN WELT
   - Titel mit max. 60 Zeichen inkl. Leerzeichen
   - Umfang: 7.000-15.000 Zeichen inkl. Leerzeichen
   - Exklusiv für DIGITALE WELT verfasst
   - Alle Grafiken und Bilder sind rechtefrei
   - Enthält keinerlei Werbung
2. CV und Bild des Autors:
   Um Sie als Autor vorzustellen, benötigen wir:
   - Ihren vollständigen Namen
   - eventuelle akademische Titel
   - Position im Unternehmen (max. 40 Zeichen)
   - Name Ihres Unternehmens (max. 25 Zeichen)
   - Portraitbild mit min. 300 DPI Auflösung
   - CV mit max. 300 Zeichen inkl. Leerzeichen
3. Consent to Publish:
   Für die Publikation in Magazin & Online-Medien benötigen wir die vollständig ausgefüllte und unterzeichnete Einverständniserklärung.
   Diese finden Sie unter
   digitaleweltmagazin.de/erklaerung

DAFÜR KOMMEN SIE IN DEN GENUSS FOLGENDER LEISTUNGEN:

- Ihr qualitativ hochwertiger Beitrag wird in unserem Online-Blog des DIGITALE WELT-Magazins veröffentlicht
- Die besten Beiträge werden additiv im Magazin präsentiert
- Unterstützung einer hohen Reichweite durch Verbreitung über Social-Media
- Dieser Service ist für Sie selbstverständlich kostenlos

Schicken Sie uns Ihre vollständigen Unterlagen an **blog@digitaleweltmagazin.de** oder nutzen Sie unser Online-Tool unter **digitaleweltmagazin.de/fachbeitrag-einreichen**

Eine Auflistung unserer aktuellen und vergangenen „Call-For-Contributions“ finden Sie unter digitaleweltmagazin.de/calls

Wir freuen uns auf Ihren Fachbeitrag mit Ihrem Expertenwissen.

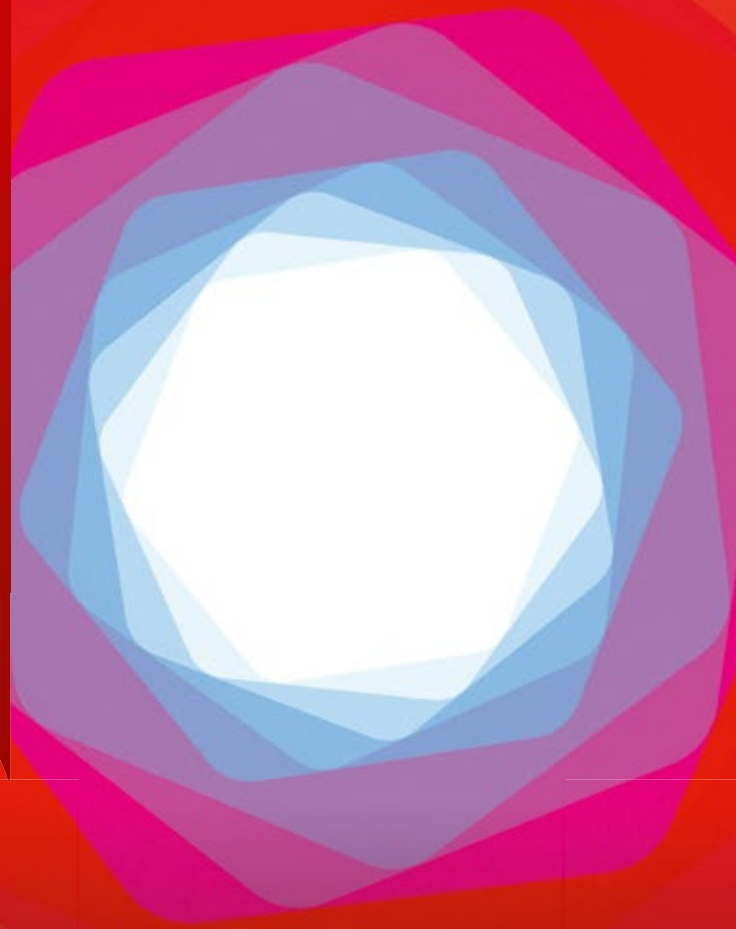
Ihr DIGITALE WELT-Team

shaping tomorrow with you

FUJITSU

Human Centric Innovation

Driving a Trusted Future



Wir begleiten Sie auf dem Weg durch die digitale Transformation

Weitere Information:
www.fujitsu.com/de/financial-services/