THE MAGAZINE OF DIGITAL TRANSFORMATION

DIGITALE WELT

SCIENCE MEETS INDUSTRY

Issue 2 ▪ April ▪ May ▪ June ▪ **2020**

Quantum Computing

Become Quantum Ready!

Foundations

A Playful Introduction to Quantum Computing

Algorithms

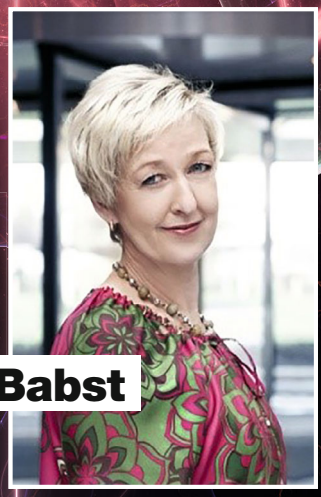
The Revolution of Quantum Information Technology

Applications

Knowledge Transfer from Science to Industry

CYBER SECURITY

About Data Loss and Cyber Risks



A NATO perspective on Technological Innovation and Change

Dr. Stefanie Babst

€ 19,50
€ 21,90

Digitale Stadt München e.V.

Jetzt Mitglied werden!

Stand: Sept. 2019

Digitale Stadt München e.V.:

Der Verein „Digitale Stadt München e.V.“ ist ein branchenübergreifendes Netzwerk im Umkreis der Digitalmetropole München. Als lebendige Plattform vernetzt er seine Mitglieder im Rahmen von drei Formaten:

DigiTalk

DigiTalks sind unsere regelmäßigen Themenabende. Unsere Mitglieder öffnen ihre Türen und laden zu einem aktuellen Thema der digitalen Transformation ein. Lernen Sie das Unternehmen kennen und erfahren Sie dessen Herausforderungen und Lösungsansätze.

AGs

Die Arbeitsgruppe „Smart City“ hat beispielsweise das Ziel, die Stadt München zu einer intelligenten Metropole zu entwickeln. Zu diesem Zweck werden Potenziale aus Wissenschaft und Wirtschaft identifiziert, um sie in das urbane Leben zu integrieren.

DIGICON

Die DIGICON ist großer Treffpunkt wenn jährlich 350 namhafte Experten und Entscheider zusammen kommen, um sich über aktuelle Themen der Digitalisierung auszutauschen.

Kontakt: Geschäftsstelle des Vereins „Digitale Stadt München e.V.“, Oettingenstraße 67, 80538 München
geschaeftsstelle@digitalestadtmuenchen.de 089/ 2180-9259 oder -9171
Mitglied werden unter: https://digitalestadtmuenchen.de/mitglied-werden/

DR. TRAVIS HUMBLE
Dr. Travis Humble is a Distinguished Scientist at Oak Ridge National Laboratory and Director of the lab's Quantum Computing Institute. He received his doctorate in theoretical chemistry from the University of Oregon before coming to ORNL in 2005. Dr. Humble leads the Quantum Computing Team in the Quantum Information Science Group. He is also an associate professor with the Bredesen Center for Interdisciplinary Research and Graduate Education at the University of Tennessee, Editor-in-Chief for ACM Transactions on Quantum Computing, and an Associate Editor for the Quantum Information Processing journal. As director of the QCI, Dr. Humble oversees research and development of Quantum Computing technologies. At the intersection of computing, physics, and information, his research focuses on the design, development, and benchmarking of new Quantum Computing platforms. These revolutionary new approaches to familiar computational problems include reducing algorithmic complexity, reducing the computational resource requirements like power and communication, and increasing the problem sizes to be tackled by state-of-the-art scientific applications.

The Beginnings of a Quantum World

The new paradigm of quantum information processing promises remarkable advances that may soon surpass conventional limitations in computing, communication, sensing and many other technologies. This includes methods for secure communication, energy-efficient computing, and high-resolution sensing. But this is only the beginning of how quantum information will change our world. Like the digital revolution of the past 70 years, quantum information is expected to transform our global community – but where will the quantum revolution lead us?

The technical and social disruptions expected from quantum information are unprecedented but not completely unknown. The original vision was to highlight the paradoxical nature of non-local correlations that define quantum mechanics. This paradox is illustrated by the case of a pair of dice that always roll to the same random value. This is highly suspicious within a classical context but exactly the type of entanglement observed when characterizing quantum particles. Reconciliation of this counter-intuitive quantum behavior evolved into conceptual experiments that soon came to define innovative applications to the theory of information. A leading example is the proposal by Nobel Laureate Richard Feynman to harness the quantum mechanics of individual atoms and electrons to simulate the dynamics of physical systems, a concept later known as Quantum Computing.

After decades of refinement, we are beginning to realize that the early visions of quantum information actually define a much more radical change. This is clearly illustrated by the discovery that Quantum Computing would enable new methods for solving important problems long thought to be near-impossible. For example, factoring large numbers had been considered too difficult to solve with conventional computers and it was widely adopted to secure public key encryption methods such as HTTPS. But the discovery of an efficient quantum algorithm for factoring changed this perspective by showing that a quantum computer enables an exponential speedup in the time needed to solve this problem. The radical change to the original computational assumptions now challenges the security of many secure communication networks, even though such a computer is not yet available. Similar advantages have been discovered for a number of other challenging problems, including unstructured search, machine learning, physical simulation, predictive modeling, logistics, and scientific discovery.

This potential for disruptive change recently made a leap forward with the demonstration of quantum computational supremacy. Quantum computational supremacy marks an achievement in which control over quantum physical systems known as qubits enables a computation that cannot be matched by conventional computing resources. The first example of quantum computational supremacy was demonstrated recently using a 53-qubit processor which performed a diagnostic test to confirm the chip was working as expected. This diagnostic computation was compared to the expected results calculated using the world's fastest supercomputer found at the US Department of Energy's Oak Ridge National Laboratory. Through a series of increasingly more difficult tests, the comparison concluded that the quantum processor performed the complete diagnostic test in approximately 200 seconds, whereas the conventional computer simulation would ultimately require approximately 10,000 years. Alongside the remarkable difference in time-to-solution, there was a corresponding difference in energy consumption – the quantum computer was approximately 10,000,000 times more energy efficient as compared to the HPC system.

The first demonstration of quantum computational supremacy as well as many other early advances offer a glimpse into the dramatic changes that await a "quantum world". These advances are now driving forward a global effort to harness the power of quantum information, and research laboratories across the world have begun to test and evaluate practical applications, with a few efforts testing first-generation products. Yet the technological race for a competitive edge has only just begun to build the workforce and infrastructure required for transformational change, where new skills and understanding are necessary to integrate quantum technologies into our existing information paradigms. Industry, governments, and professional societies are supporting efforts to train and educate quantum scientists and engineers while incentivizing the development of new ideas and products.

We are only seeing the beginnings of a quantum world that will herald big changes in the future for computing and other forms of information processing. As we continue to pass more technological milestones, we will integrate these concepts and drive forward to the competitive advantages offered by quantum information.

Photo: personal

DIGITALE WELT ISSUE 2 | 2020

22 **VERY DIGITAL PERSON:**
Faisal Shah Khan

The next DIGITALE WELT will be released on 03.06.2020

DIGITIZATION *in Numbers*

The **energy consumption** *of Core i9 10900K of Intel takes up to*

250 watts.

According to a study of 451 Research, **60 %** *of all companies use* **NoSQL databases.**

About **450** *developers at* **Intel** *have lost their job in Germany due to office closures.*

Applications in the **Amazon Cloud** *are expected to run up to* **40 %** *faster when using the ARM processor Graviton2 instead of M5 instances of Intel Xeon.*

IBM's quantum computers *achieve*

2 times

the quantum volume compared to the previous year.

Intel bought the Israeli AI chip manufacturer **Habana Labs** *for*

2 billion *US dollars.*

It is expected that in 2022 **chatbots will decrease company costs** *by about*

8 billion

dollars.

Residual neural networks *can be accelerated about*

10 times

using the QuantaFlow processor of PQ Labs Inc.

China invests

10 billion

dollars in **Quantum Computing research** *in Anhui province alone.*

Quantum Computers with **61 Qubits** *can be simulated via* **supercomputers** *and* **data compression.**

Photo: 123RF

WHY IS MENTAL WELLBEING SO "TRENDY" NOWADAYS?

In order to understand the emergence of mega trends it is quite interesting to look back in history. There is a saying of Abraham Lincoln: "The dogmas of the quiet past are inadequate to the stormy present. We have to change our paradigm …." (1860)

Stormy present in 1860?

There were clashes of cultures and civil wars, the invention of the steam engine, industralization, … The Kondratiev cycle theory demonstrates how economic and social developments happen in waves and as a result of overcoming some kind of shortage or bottleneck. In fact the shortage of transport capacity led to the invention of the railway; and the desire for universal access to the world's ever-growing knowledge base led to the development of the computer ...

Bottlenecks are common in the working world: in the 1960s, companies invested billions to teach German managers English for deployment in foreign markets. This is because in pre-and post-war Germany, students primarily learned humanistic languages. Or, let's jump into the 1980s and 1990s, when companies invested billions in equipping workplaces with computers, software and training. The former IBM boss Thomas Watson is credited with the quote: "I think there is a world market for maybe five computers". A radical rethinking has always been needed for previous thought patterns to be driven away and priorities completely reset.

The resulting leaps forward in development have always led to movement on many levels and triggered an economic boom. But people were also forced to rethink, cast aside old thought patterns, and set new priorities.

Do we need a new kind of thinking?

Yes definitely, and we are in progress. Today's world is comparable to other periods in history that saw shortages – they were in other areas, admittedly, but they were shortages nonetheless. And, of course, technologies, robotics, and revolutionary energy systems are under constant development – but these days, one of the scarcest resources in organisations is high-performing, creative, and socially skilled people ...

That is why a new way of thinking has become necessary – this time, to support the psychological and physical wellbeing of employees. Personal wellbeing, the search for balance has come into focus with the current discussions about digitisation, mobility, working in different time zones and generational shifts. Mental overload of employees affects productivity and quality, which leads to massive bottlenecks. When people permanently lose their personal balance, it becomes a cost factor for companies.

What society and businesses need today is to understand the importance of wellbeing or mental health, the knowledge of all the components of sustained health, and the will to keep this issue in focus in the long-term.

In specific terms, this means explicitly including the topic of mental wellbeing in corporate culture and, at the same time, promoting and demanding self-responsibility from all employees. In order to successfully change corporate culture, it's very important that leaders see it as their responsibility to take care of their own health and that of their colleagues.

Today's graduates are fluent in other foreign languages alongside English, and handle digital media as a matter of course. Unfortunately, what is not yet taught and trained in schools is mental strength for improved health and better performance.

Currently, many thousands of children in the Western world are 'treated' with Ritalin, so that they can better concentrate on their work. At the same time, non-drug therapies are providing great results when children and adolescents learn to use neurofeedback to manipulate their brain waves to focus on their work. The long-term effects of (often unnecessary) drug treatment can sometimes be very dramatic. There are clinical studies that show changes in the nervous system, withdrawal from the community, getting used to the – subsequent – increasing consumption or facilitated switching to other addictive substances.

On the other hand, neurobiological research underlines the effects of mental pictures controlling the hormones, neurotransmitters and the whole metabolism. Considering the power of thoughts influencing the metabolism, the brain waves in any direction, we must recognize that our brain is a treasure chest. We can easily find mental pictures that influence the outcome of our activities either positively or negatively, using a specific cocktail of dopamine, serotonin, endorphins and oxytocin.

As with previous skills gaps, businesses today must make their contribution to the maintenance of mental health until the other social areas follow suit.

Many companies understand and are on the way to establishing a culture of mental wellbeing. Whereas in schools we have to initiate more projects to build up a personal competence "mental strength".

I look forward to receiving your comments!

Dr. Petra Bernatzeder, psychologist, consultant, coach, director of upgrade human resources, www.upgrade-hr.com

This specialist book explains in a practical way how executives and HR managers keep their colleagues healthy, powerful, creative and innovative, and protect them from burnout – in a digital working world full of stress factors and psychological overload.

Photo: personal

"Welcome in the age of AI" was the headline for the first slot at DIGICON, which Dr. Volker Wetekam (Corporate Strategy Officer and Executive Vice President, Robert Bosch GmbH) introduced in an exciting way with his presentation on "Future Mobility".

From left to right: Robert Jacobi (Nunatak Group) in conversation with Dr. Volker Wetekam (Robert Bosch GmbH), Dr. Christoph Zindel (Siemens) and Dr. Dieter Nirschl (ADAC) – artificial intelligence illuminated from all perspectives

The use of AI also involves social responsibility, as Andrea Martin (Leader, IBM Watson IoT Center Munich) explained in her presentation on the second day of DIGICON.

A total of eleven companies presented their novel products, such as BioID with its Face Recognition Software, on the ground floor of Palais Lenbach at the "Marketplace of Innovations".

At a digital event in the middle of Munich, Munich's IT simply cannot be missing: Thomas Bönig, IT minister of the state capital, on Munich's position as a digital metropolis.

Prof. Dr. Paul Lukowicz (Head of the Research Department Embedded Intelligence, DFKI) impressively showed where AI research stands today and what can be expected in the future.

From left to right: Dr. Dieter Nirschl (Managing Director, ADAC), Dr. Volker Wetekam (Corporate Strategy Officer Robert Bosch GmbH), Prof. Dr. Claudia Linnhoff-Popien (LMU Munich and CEO Digitale Stadt München e.V.), Dr. Christoph Zindel (Member of the Managing Board, Siemens Healthineers) and Robert Jacobi (Managing Director, The Nunatak Group)

With a stethoscope, Dr. Christoph Zindel, (Member of the Board of Management, Siemens Healthineers) started his presentation at DIGICON 2019. His message? Artificial intelligence makes the daily work of doctors much easier: "Relieving physicians, humanizing medicine" the title of his speech.

For the first time, DIGICON hosted the ISAAI'19 science symposium: The picture shows Stephan Otshues, Executive Partner, Digital Strategy and IoT Consulting (IBM Global Business Services) who is giving a lecture on how to bring AI innovations to the market.

Premises of the event location "Palais Lenbach" offer an atmospheric ambience for the digital conference DIGICON. Culinary delicacies from Feinkost Käfer provided plenty of opportunity for networking.

Take a note: DIGICON 2020 will take place on November 18. - 19.

MUNICH

DIGICON 2019 – All about artificial intelligence.

Astonishing presentations, a pitch battle that couldn't be more thrilling, and an audience of 368 decision makers from top-class companies and scientific institutions, all gathered in Bavaria's capital city Munich, for one reason: the DIGICON 2019. From November 20 to November 21 the DIGITALE WELT CONVENTION (DIGICON) took place at the Palais Lenbach. For the fourth time in a row this LMU-initiated Digitalization Conference, a partner event of the association „Digitale Stadt München e.V.", called on important developments in the world of technology and digitalization. 2019's conference conference was all about artificial intelligence (AI). Under the moderation of the well-known ZDF host and author, Nina Ruge, experts such as Christoph Zindel (Member of the Managing Board, Siemens Healthineers), Dr. Stefanie Babst (Head of the Strategic Analysis Capability, NATO) and Ralph Schneider (CIO, Allianz SE) explained how they each make advantageous use of machine learning technologies and master challenges in their respective industries. The ideas that are brought together at the DIGITALE WORLD CONVENTION are trend-setting. New this year: The International Symposium on Applied Artificial Intelligence (ISAAI'19). Scientists from 14 countries (Asia, Africa, USA and Europe) presented more than 35 cutting-edge research findings on AI. "Science meets Industry" – is DIGICON's well-known claim. And it's just as well-known what the conference stands for.

Photos: Lennart Preiss


DIGICON 2019
Dr.
Stefanie Babst
NATO

Technological Innovation and Change – A NATO perspective

Dr. Stefanie Babst

Keynote speech at DIGICON 2019 in Munich

Good morning Ladies and Gentlemen,

I feel privileged to be part of this important and timely discussion. Connecting to the discussion about new technologies is extremely interesting.

As we have heard yesterday, AI, Quantum Computing, biotechnologies and the entire infrastructure of the Internet of Things will continue to shape our lives in many aspects. Yet it is also bound to alter geopolitics – hence I am glad to be able to offer you a perspective from NATO.

In only a few days from now, Alliance leaders will gather in London to mark NATO's 70th anniversary; they will remind us that we can celebrate seven decades of unprecedented peace in Europe – a peace which has made it possible for our citizens to live freely and safely, and for our nations and our economies to prosper. But peace, freedom and stability – and prosperity – must never be taken for granted. We cannot be complacent.

Global change is on NATO's mind every day. The macro trends shaping global affairs are well-known to us.

What we particularly see and feel is that our liberal world has increasingly become strained. Assertive and authoritarian powers and political strongmen are able to make gains in the international arena. They are defying the post-Cold War rules-based order in multiple ways and on many levels.

Russia is one of them. It looks at the world from a zero-sum game perspective and seeks to alter the balance of power in Europe and elsewhere in the world. Its illegal and aggressive annexation of Crimea and aggressive actions in eastern Ukraine are a case in point.

Russia is upgrading its military posture on all fronts; and it is testing the West's resolve in various ways at the same time. From applying coercive diplomacy to threatening with new weapons systems, and from waging cyber-attacks against our information systems to meddling in the domestic affairs of other countries, the leadership in Moscow seems to be determined to steadily solidify Russia's spheres of influence in Europe and beyond.

Moscow has long discovered the advantages that some of the new technologies bring for its military posture. It is investing heavily into autonomous weapons, hypersonic mis-

siles, Quantum Computing and, of course, AI. President Putin has already clearly expressed his understanding of the importance of the latter: whoever becomes the leader of AI, will become the ruler of the world, he said.

His view is seemingly shared by others. China, too, spends billions of dollars for the modernization of its military, aimed at making the People's Liberation Army the world's most advanced by 2050. China is also working on megaprojects designed to position itself as the world leader in artificial intelligence and other advanced technologies. This undertaking is not exclusively military in its focus, but every one of these advanced-technology megaprojects has military applications and benefits the Chinese doctrine of "military-civil fusion".

AI-driven mass surveillance and facial recognition technologies help suppress the Uighur minority in Eastern China and keep hundreds of thousands of them in so-called education camps. It also helps screen millions of Chinese children when they arrive at school every morning, analyzes what books they read and how they interact with their teachers, and monitors their level of concentration. In Guiyang, a city in southwest China of 3.5 million inhabitants, 10,000 cameras were able to track down a BBC journalist within 7 minutes. These are just a few examples how the Communist leadership in Beijing seeks to employ AI. Since it sells homemade AI technologies together with undersea cables and 5G technologies to non-democratic regimes across Asia, Latin America and the African continent – under the "Smart City" label -, we cannot and should not be complacent about this. China's technological endeavors have implications for our lives, our security and our strategic interests, too.

Dr. Stefanie Babst

Dr. Stefanie Babst has been a member of NATO's International Staff since 1998. She is currently the Head of the Strategic Analysis Capability for the NATO Secretary General and for the Chairman of the NATO Military Committee. In this capacity, she is responsible for preparing comprehensive assessments on potential upcoming crisis situations in geographical and functional areas of relevance and concern to NATO, as well as on their implications for the Alliance. Prior to joining SAC in 2012, she occupied various posts in NATO's Public Diplomacy Division, including that of NATO Deputy Assistant Secretary General for Public Diplomacy.

She began her career in 1991 as Assistant Professor for International Security Policy at the Institute of Political Science/ Christian-Albrechts-University in Kiel, Germany, moving on to become Professor of Russian and East European Studies at the Federal Armed Forces Command & General Staff College in Hamburg.

Stefanie is an internationally renowned publisher and speaker of international security issues. She is a member of a number of policy groups and security networks, including Women in International Security (WIIS) and the World Economic Forum. In recognition of her professional achievements, she has received several awards.

We must not be blind to the fact that our strategic competitors also seek to take advantage of frail democracies in Europe to achieve their strategic goals. Often using so-called "greyish or hybrid activities". Fueling populist revolts or running malign digital campaigns, aimed at undermining democratic societies, is much cheaper than waging war against your enemy. Indeed, you may not think of these and similar actions as forms of war, but I can assure you that Russia and China understand them as legitimate elements of warfare. Or, as the Chinese military strategist Sun-Tzu put it, centuries ago already, "useful tools to win war without fighting".

I am afraid this picture is quite gloomy. But it's not borne out of a sense of doom but realism and plausibility. Regardless of existing uncertainties, I believe the grand trends that I just described will likely prevail in years to come. This, in turn, implies that liberal democracies will have to operate in a highly contested space in the future. Strategic competition takes place on land, at sea, in the air, in space, and in the information, technological and cyber domains. And as already said, even within NATO countries, the hearts and minds of our own populations have increasingly become objects of competition.

A number of experts have already warned that we may face a large-scale and uncompromising technological arms race among the world's leading powers, and I personally believe that it has already begun. I sympathize with Eric Schmidt, CEO Alphabet, who has said that "a Silicon curtain of digital connectivity could replace the Iron Curtain", the end of which 30 years ago we commemorated earlier this month. This is certainly not what we want.

Seen from NATO, one of the most profound implications of the digital revolution will be on the future of warfare. The emergence of new technologies requires reconsidering how, with what, and by whom war is waged in the future. AI, autonomous systems, big data, and quantum science have already started to transform warfare. This does not mean that the nature of war will change. War will always be destructive and politically motivated, regardless of whether it involves a source code or a longbow. And it will remain composed of the same three elemental functions that new recruits learn in basic training: move, shoot, and communicate.

But in a world that is becoming one giant sensor, moving troops and weapon systems will be far more difficult. The amount of data generated by the Internet of Things and the proliferation of low-cost, commercial sensors that can detect more things more clearly over greater distances are already providing more real-time global surveillance than has existed at any time in history.

Technology will also radically alter how militaries shoot, both literally and figuratively. Cyberattacks, communication jamming, electronic warfare, and other attacks on a system's software will become as important as those that target a system's hardware, if not more so.

Eventually, hypersonic munitions (weapons that travel at more than five times the speed of sound) and space-based weapons will be able to strike targets anywhere in the world nearly instantly. Swarms of autonomous systems will not only be able to find targets everywhere, they will also be able to shoot them accurately.

The opening ceremony of the 2018 Winter Olympics in South Korea offered a preview of this technology when more than 1.200 autonomous drones equipped with lights collaborated to form impressive pictures in the night sky over PyeongChang. Now imagine similar autonomous systems being used, for example, to overwhelm an aircraft carrier or a battle tank.

Well, military modernization of this kind will not happen all at once. But as technological innovation is a fast-moving train, we must now be prepared to reflect on where we want to go from here.

So, how does the Alliance approach these future prospects, and more broadly technological innovation at large? Let me start answering this question with a general remark.

NATO and innovation are no strangers to each other. NATO at 70 can look back at a history of frequent change and adaption. Both our distant and more recent history is full of examples of how the Alliance successfully adapted its strategies, policies, approaches and, ultimately, also our military posture to a changing security environment. At the core of all this is our belief that innovation is an expression of a mindset. It is not an act. Science & technology (S&T) shared among and jointly developed by NATO member countries has always been a key driver of innovation; its military applications were translated in multiple civilian forms. This is changing now. Today private companies, from the giants to the start-ups, are leading technological innovation more than traditional defense industries in our countries. For the Alliance, this means that our innovation partnerships have become much larger.

But NATO is a multilateral enterprise, so our premier job is to bring 29 (soon 30) countries together. Just as with any other policy area in the Alliance, NATO member countries remain fully in the driver's seat when it comes to technological innovation and change. No NATO entity dictates terms to nations on S&T – and no one should.

We have already started with some important work. In October, the NATO Defense Ministers endorsed a Roadmap on Emerging and Disruptive Technologies that lays the ground for the organization's future work strands.

First and of utmost importance, we want to encourage the NATO member states to develop a common approach to, and understanding of, the opportunities and risks that derive from new technologies. In order to fully comprehend the breadth and scale of these technologies, we will engage with governments, national military authorities, industries, and the EU and UN.

Second, we will pay particular attention to how these technologies could possibly affect our concept of deterrence and defense and how they will impact on the existing arms control and non-proliferation regimes. I already mentioned that AI and other technologies will alter the future of warfare to a considerable degree; hence we must think ahead to how we can best equip our armed forces to meet the challenges we will face in the future. And given that countries like China and Russia spread these technologies on a large scale, we must think smartly about how we can establish new non-proliferation and arms control arrangements for some types of technologies.

Third, NATO will also examine how AI, big data, Quantum Computing, biotechnologies, automation and other technologies could influence the protection of critical infrastructure in our countries, as well as our civil preparedness and resilience.

Fourth, we will have to link some of these technologies to NATO's established process of capability planning. What we need to avoid is a potential technological capability gap, i.e. to have countries that invest heavily and others who don't.

And finally, NATO will also serve as a forum to discuss the critical questions of ethical and legal standards. We are determined to do this in close collaboration with the EU and other bodies that have already worked on setting standards.

Overall, we will want to make sure that our defense concepts and capabilities are adequately geared towards meeting the technological challenges and security risks that we are facing now, and in the future. For sure, NATO aims to maintain its technological edge.

While all this describes an important political process, we don't limit ourselves to talking. We are also testing some of the new technologies. Exercise Trident Juncture at the end of 2018 was a showcase of the Alliance's ability to innovate. For those of you who haven't followed it, Trident Juncture was the largest NATO exercise in decades, bringing together around 50.000 personnel from 31 NATO Allied and partner nations. We tested in real time 3D printing of spare parts for vehicles, to increase speed and efficiency. We tested some of the smallest drones in the world, controlled by artificial intelligence. And we used radar, thermal imaging and video tracking to disrupt opposing unmanned systems.

Ladies and Gentlemen, we are in the thick of a large-scale revolution in technology. Many of the new technologies, including AI, will undoubtedly bring many opportunities for people and businesses. But our democratic countries are to a certain degree handicapped when it comes to their applications. In contrast to authoritarian and non-democratic regimes who are less scrupulous about applying new technologies against their citizens, our privacy policies and frameworks protect what is dearest to us: our individual liberties and freedoms. We must not compromise them. Instead we must find like-minded states to spearhead international regulation and non-proliferation; and we must work to enhance our efforts to strengthen our resilience against malign attempts to destabilize our societies from outside, with the support of new technologies. All that said: the Alliance embraces technological innovation with an open but vigilant mind. I look forward to discussing some of these issues further with you.

Thank you very much for your attention.

The opinions expressed are not the official position of NATO, but reflect the personal opinions of the author.

Photos: Lennart Preiss, personal

Alle Konten im Griff.

Ein Zugang für alles: Nutzen Sie unser Online-Banking jetzt auch für Ihre Transaktionen von Konten und Depots anderer Finanzinstitute.

sskm.de/multibanking

Stadtsparkasse München

Die Bank unserer Stadt.

Marcus Raitner works as an agile transformation agent and agile coach at BMW Group IT. In his blog "Experience leadership!" he has been writing about leadership, agility, digitalization, and much more since 2010.

Context Not Control

What does Netflix have in common with a nuclear submarine? Although at first glance they couldn't be more different, they share an exceptional leadership culture. Reed Hastings, CEO of Netflix, prides himself on making as few decisions as possible and preferably none at all for an entire quarter. And Captain David Marquet decided to stop giving orders on the nuclear submarine USS Santa Fe. Both rely on context instead of control and are very successful with it.

For over a year David Marquet prepared himself for his new task as captain of the USS Olympia. He learned every detail about this nuclear submarine. Everything went as planned until he had to take command of the USS Santa Fe at short notice. And as the USS Santa Fe was a much newer type, David Marquet knew little about it when he took command.

Nevertheless David Marquet went to work and gave commands as captains are trained to do. After all the USS Santa Fe was at that time the submarine with the worst performance and morale in the Navy and therefore the situation demanded a strong leader. Didn't it?

During a drill in the first month of his command, David Marquet realized the danger of a team trained in obedience and a boss with limited knowledge. The drill simulated the failure of the main reactor and thus the USS Santa Fe had to run on a battery-powered electric propulsion motor until the reactor was repaired. To challenge the crew a little bit, David Marquet gave his officer of the deck the order "Two thirds ahead!" The officer immediately passed the order on to the helmsman and … nothing happened!

When David Marquet asked the helmsman why he had not executed the order, he was told that – unlike on his previous submarines – on this ship there was no "two-thirds ahead". Everyone on board knew this except David Marquet. Especially the officer of the deck knew this, but he nevertheless passed the order because he was trained in obedience. This was the moment when David Marquet realized that with his limited knowledge and experience he was a dangerous bottleneck, and at the same time he realized the potential hidden in the collective experience, intelligence and creativity of his crew. Potential he wanted to unleash.

After this epiphany he refused to give orders. Except for the use of nuclear missiles, David Marquet let his crew decide. In order to make these decisions he provided the full context and then acted as a coach. When an officer asked for permission to submerge the ship, for example, he made the officer think about whether it was safe on the one hand and on the other hand whether it was now the right thing to do in terms of the overall mission. Gradually fewer and fewer officers asked for permission, but began to think like David Marquet.

With this remarkable leadership style, David Marquet succeeded in turning the ship around (which is why his very recommendable book is entitled "Turn Around the Ship!"). The USS Santa Fe went from worst to best in the US Navy and remained so after David Marquet retired in 2009.

Despite this stunning evidence of the impact of this "leader-leader" paradigm (instead of the far more common "leader-follower" paradigm), examples of this leadership culture in large hierarchical organizations are still difficult to find. However, at Netflix, the seventh largest Internet company in the world, one will easily spot this in their legendary Culture Statement, which Patty McCord published as former Chief Talent (sic!) Officer in 2009. In the revised version on the Netflix website it becomes unmistakably clear who decides at Netflix and what the task of leadership is:

> *We want employees to be great independent decision makers, and to only consult their manager when they are unsure of the right decision. The leader's job at every level is to set clear context so that others have the right information to make generally great decisions.*
>
> Netflix Culture Statement

Photo: personal

The book "Manifest für menschliche Führung" ("Manifest for human leadership") is available as paperback and e-book on Amazon

1. QUANTUM COMPUTING

Quantencomputing bietet eine völlig neuartige Möglichkeit, komplexe Berechnungen sehr viel schneller und oftmals überhaupt erst auf praktische Weise durchzuführen.

Diese bahnbrechende Entwicklungen, die in den letzten Jahren große Sprünge in der Praxis erlebt hat, geht auf zwei wissenschaftliche Revolutionen des frühen 20. Jahrhunderts zurück. Die erste Revolution wurde um 1930 durch die radikal neuartige Theorie der Quantenmechanik ausgelöst, die unsere Auffassung von Realität drastisch verändert hat. Die zweite wissenschaftliche Revolution erfolgte in den 1940er Jahren, indem die Grundlagen für den Bau erster programmierbarer Computer gelegt wurden, welche die Basis aller Rechentecnik ist, wie wir sie heute von Smartphones bis Großrechner kennen. In den letzten beiden Jahrzehnten wurden diese beiden Wissenschaften zusammen geführt und es entstand der interdisziplinäre Zweig des Quantencomputings.

Quantencomputer sind Rechenmaschinen, welche die Effekte der Quantenmechanik verwenden. Dies beinhaltet die Fähigkeit mehrere Zustände gleichzeitig zu besitzen (Superposition), mit einer Operation viele Zustände gleichzeitig zu verändern (Verschränkung) sowie unwahrscheinliche Lösungen zielstrebig zu erreichen (Tunneling). Neben universellen Quantencomputern spielen sogenannte Quantenannealer eine immens wichtige Rolle, da sie besonders dafür konzipiert sind, Optimierungsprobleme zu lösen.

In dieser Ausgabe erwarten Sie Artikel rund um das Thema Quantencomputing. Die Themen fokussieren technische Hintergründe, mögliche Anwendungsfälle sowie visionäre Gedanken.

INHALT

Ein spielerischer Einstieg in Quantum Computing

Dr. Jan-Rainer Lahmann, Thomas Haag

1. Quantum Computing und Spiele – wie passt das zusammen?
Die Funktionsweise von Quantencomputern beruht auf quantenmechanischen Effekten wie Superposition und Verschränkung (engl. „Entanglement“), die wenig anschaulich sind, ja teilweise sogar unserer Anschauung und alltäglichen Erfahrung widersprechen. Aktuelle Forschungsergebnisse lassen erwarten, dass Quantencomputer – sobald sie mit genügend vielen, qualitativ hochwertigen „Qbits“ gebaut werden können – für bestimmte Fragestellungen klassischen Computern weit überlegen sein werden. Die Algorithmen für Quantencomputer beruhen allerdings auf ganz anderen Prinzipien als klassische Algorithmen. Es ist eine andere Welt, in der klassisches Denken – d.h. unser Verständnis aus der klassischen Newtonschen Physik – nur sehr begrenzt weiterhilft.

Dieser Artikel gibt einen ersten Einblick in die seltsam anmutende Welt des Quantum Computing, indem Spiele (sog. „Quantum Games“) betrachtet werden, die Quanteneffekte ausnutzen und anschaulich – teilweise sogar unterhaltsam – darstellen. Eines dieser Spiele, ein Münzspiel, wird eingehend beschrieben – inkl. Regeln, (Quanten-)Theorie und einer online zugänglichen Implementierung basierend auf dem Quantum Computing Framework „Qiskit“.

2. Quantum Games
Das Spektrum an Quantum Games ist groß. Es reicht von Smartphone Apps wie „Hello Quantum“ (https://hello-quantum.mybluemix.net) über Brettspiele wie „Entanglion“ (https://entanglion.github.io) bis hin zu wissenschaftlichen Artikeln wie dem von Vassili N. Kolokoltsov (https://arxiv.

IBM Quantencomputer

org/abs/1909.04466v1) mit einer mathematischen Betrachtung mehrerer Quantum Games. Dieser Artikel geht u.a. auf „Meyer's quantum penny-flip game" ein, das auch die Basis für einen TED Vortrag von Shohini Ghose („A beginner's guide to Quantum Computing") (https://www.ted.com/talks/shohini_ghose_quantum_computing_explained_in_10_minutes) ist. Dieses „Quantum Münzspiel" wurde erstmals im Jahr 1998 von David A. Meyer in seinem Artikel „Quantum Strategies" (https://arxiv.org/abs/quant-ph/9804010v1) als „PQ Penny Flip" betrachtet. Die Namensgebung ist angelehnt an die Charaktere Picard und Q aus der Serie „Star Trek: The Next Generation".

3. Das Quantum Münzspiel

Die Regeln des Spiels sind einfach: Eine Münze wird verdeckt in eine Box gelegt mit der Seite „Kopf" nach oben. Zwei Spieler – wir nennen sie Alice und Bob – sind abwechselnd am Zug und dürfen die Münze entweder unverändert lassen oder umdrehen. Es werden insgesamt drei Züge gemacht, also zwei von Alice und dazwischen einer von Bob. Die Münze wird erst am Ende wieder aufgedeckt. Zeigt sie „Kopf", so gewinnt Alice, zeigt sie dagegen „Zahl", so gewinnt Bob.

Das Spiel scheint zunächst wenig spannend, und man überlegt sich schnell, dass es weder für Alice noch für Bob eine Spielstrategie gibt, so dass sie mit mehr als 50% Chance gewinnen.

Vereinfacht gesagt kann Alice nicht wissen, ob die Münze vor ihrem letzten Zug mit Kopf oder Zahl oben liegt. Sie kann im letzten Zug also nur raten und hat damit eine Chance von 50/50 zu gewinnen.

Interessant wird das Spiel, wenn wir Quanteneffekte einführen. Aber zunächst wollen wir das Spiel in mathematische Formeln fassen. Für die klassische Version des Spiels erscheinen die Formeln zu komplex. Die Darstellung wird aber später – bei Berücksichtigung von Quanteneffekten – sehr hilfreich sein.

Wir beschreiben den Zustand der Münze in einem zweidimensionalen Vektorraum. K steht für den Zustand Kopf, Z für Zahl. (Die notwendigen Mathematischen Grundlagen sind im folgenden Abschnitt kurz zusammengefasst.)

$$K = \begin{pmatrix}1\\0\end{pmatrix}, \quad Z = \begin{pmatrix}0\\1\end{pmatrix}$$

Die Züge, d.h Umdrehen der Münze oder Liegenlassen, können nun durch Matrizen dargestellt werden. L für Liegenlassen und U für Umdrehen:

$$L = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \quad U = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}.$$

Das Ergebnis eines Zuges ergibt sich durch Multiplikation der entsprechenden Matrix mit dem Zustand vor dem Zug. Es gilt wie erwartet:

$$LK = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = K, \quad UK = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = Z,$$

$$LZ = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = Z, \quad UZ = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = K.$$

D.h. U („Umdrehen") ändert den Zustand, L („Liegenlassen") dagegen nicht.

Ein konkreter Spielverlauf kann nun folgendermaßen aussehen: Die Münze liegt zunächst mit Kopf oben. Alice dreht sie um, Bob ebenfalls, im letzten Zug lässt Alice die Münze liegen. Wegen der Reihenfolge der Matrix-Multiplikationen (von rechts nach links) kann dies geschrieben werden als

$$LUUK = LUZ = LK = K.$$

D.h. auch die Formeln zeigen, dass die Münze nach dem dritten Zug mit Kopf oben liegt und Alice gewinnt.

Neue Möglichkeiten ergeben sich, wenn wir vom klassischen Spiel zu einem Quantum Game übergehen und Alice erlauben, auch Quantenzustände der Münze zu erzeugen. Wir werden später versuchen, diese neuen Zustände (es handelt sich um eine Superposition der Zustände Kopf und Zahl) zu veranschaulichen. Wir führen sie aber zunächst mit Hilfe mathematischer Formeln ein, bzw. einer weiteren Matrix H, die einen neuen Zug – einen Quantenzug – ermöglicht.

Wir definieren die Matrix H als

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}.$$

Wenn Alice den neuen Zug „H" in ihrem ersten Zug anwendet (die Münze liegt davor mit Kopf oben), so ist die Münze danach in folgendem Zustand:

$$HK = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}.$$

Dieser Zustand ist eine Linearkombination der Zustände Kopf und Zahl, mit der Gewichtung von jeweils 1/√2 :

$$HK = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix}\right) = \frac{1}{\sqrt{2}}(K + Z).$$

Diesen Zustand können wir uns nicht anschaulich vorstellen; in der Quantenmechanik ist dies jedoch ein eindeutig definierter Zustand – eine Superposition von Kopf und Zahl. Viele populärwissenschaftliche Artikel versuchen dies zu veranschaulichen, indem sie davon sprechen, die Münze sei „gleichzeitig im Zustand K als auch im Zustand Z".

Für Anwendung von H auf den Zustand Z (Zahl) ergibt sich analog:

$$HZ = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}(K-Z).$$

Nach etwas Überlegung bemerkt Alice, dass ihr der neue Zug einen großen Vorteil verschafft. Wenn sie ihn zweimal verwendet gewinnt sie das Spiel immer, egal ob Bob in seinem Zug zwischendrin die Münze umdreht oder liegenlässt!

Denn es gilt:

$$\begin{aligned} HLHK &= HL\left(\frac{1}{\sqrt{2}}(K+Z)\right) = \frac{1}{\sqrt{2}}H\big(L(K+Z)\big) = \frac{1}{\sqrt{2}}H(LK+LZ)\\ &= \frac{1}{\sqrt{2}}H(K+Z) = \frac{1}{\sqrt{2}}(HK+HZ)\\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(K+Z)+\frac{1}{\sqrt{2}}(K-Z)\right)\\ &= \frac{1}{2}\big((K+Z)+(K-Z)\big) = K. \end{aligned}$$

Und ebenso (da $Z+K=K+Z$):

$$\begin{aligned} HUHK &= HU\left(\frac{1}{\sqrt{2}}(K+Z)\right) = \frac{1}{\sqrt{2}}H\big(U(K+Z)\big) = \frac{1}{\sqrt{2}}H(UK+UZ)\\ &= \frac{1}{\sqrt{2}}H(Z+K) = \frac{1}{\sqrt{2}}H(K+Z) = \cdots = K. \end{aligned}$$

Alice hat in dem Spiel einen enormen Vorteil erzielen können, da sie Superposition genutzt hat, also den Zustand $\frac{1}{\sqrt{2}}\binom{1}{1} = \frac{1}{\sqrt{2}}(K+Z)$, sowie einen weiteren Effekt der Quantenmechanik, die Interferenz, bei der sich Zustände „aufheben“ können. In der letzten Zeile der Rechnung zur ersten Zugfolge heben sich nämlich die Zustände Z und $-Z$ auf:

$$\frac{1}{2}\big((K+Z)+(K-Z)\big) = \frac{1}{2}(K+Z+K-Z) = \frac{1}{2}(K+K+Z-Z) = K.$$

4. Exkurs: Mathematische Grundlagen

Die hier gewählte mathematische Darstellung des Münzspiels benötigt lediglich elementare Lineare Algebra. Als Erinnerung die grundlegende Vorgehensweise der Matrix-Vektor- Multiplikation für reelle oder komplexe Zahlen a, b, c, d, x, y:

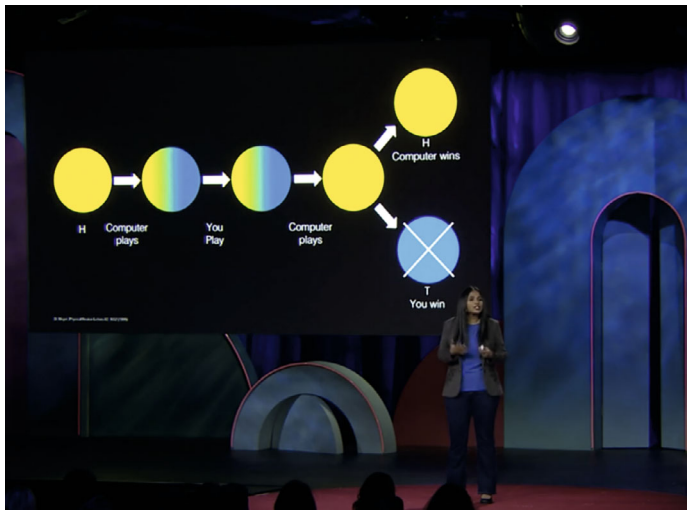
$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}ax+by\\cx+dy\end{pmatrix}.$$

Dies wird oftmals in folgender Form dargestellt, bekannt als „Falksches Schema“:

$$\begin{array}{cc} & \begin{pmatrix}x\\y\end{pmatrix}\\ \begin{pmatrix}a & b\\ c & d\end{pmatrix} & \begin{pmatrix}ax+by\\cx+dy\end{pmatrix}. \end{array}$$

Und analog für die Multiplikation von Matrizen:

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x & u\\ y & v\end{pmatrix} = \begin{pmatrix}ax+by & au+bv\\ cx+dy & cu+dv\end{pmatrix}.$$



TED Vortrag von Shohini Ghose: „A beginner’s guide to Quantum Computing“

Spielverlauf für die Zugfolge U(mdrehen) U(mdrehen) L(iegenlassen)

Veranschaulichung des Spielverlaufs für die Zugfolge „H L H“

Veranschaulichung des Spielverlaufs für die Zugfolge „H U H“

```
# create the quantum circuit with the chosen coin moves
q = QuantumRegister(1) # create a quantum register with one
qubit
# create a classical register that will hold the results of
the measurement
c = ClassicalRegister(1)
qc = QuantumCircuit(q, c) # creates the quantum circuit
backend = BasicAer.get_backend('qasm_simulator') # define
the backend

# 1. move of A
qc.iden(q[0]) if (moveA1 == 0) else qc.x(q[0])

# 1. move of B
qc.iden(q[0]) if (moveB1 == 0) else qc.x(q[0])

# 2. move of A
qc.iden(q[0]) if (moveA2 == 0) else qc.x(q[0])

qc.measure(q, c) # Measure the qubits
qc.draw(output='mpl') # plot the circuit
```

Quantenalgorithmus in Qiskit für den Spielverlauf „U U L“

```
# execute the quantum circiut (coin moves) and identify the
winner

job = execute(qc, backend, shots=200) # run the job simula-
tion

result = job.result() # grab the result

counts = result.get_counts(qc) # results for the number of
runs

print(counts); # print the results of the runs
who_wins(counts); # celebrate the winner

{'0': 200}
The winner is A
```

Ergebnis für den Spielverlauf „U U L“

```
# create the quantum circuit with the chosen coin moves
q = QuantumRegister(1) # create a quantum register with one
qubit
# create a classical register that will hold the results of
the measurement
c = ClassicalRegister(1)
qc = QuantumCircuit(q, c) # creates the quantum circuit
backend = BasicAer.get_backend('qasm_simulator') # define
the backend

# 1. move of A
if   moveA1 == 0 : qc.iden(q[0])
elif moveA1 == 1 : qc.x(q[0])
elif moveA1 == 2 : qc.h(q[0])

# 1. move of B
if   moveB1 == 0 : qc.iden(q[0])
elif moveB1 == 1 : qc.x(q[0])

# 2. move of A
if   moveA2 == 0 : qc.iden(q[0])
elif moveA2 == 1 : qc.x(q[0])
elif moveA2 == 2 : qc.h(q[0])

qc.measure(q, c) # Measure the qubits
qc.draw(output='mpl') # plot the circuit
```

Quantenalgorithmus in Qiskit für den Spielverlauf „H U H“

```
# execute the quantum circiut (coin moves) and identify the
winner

job = execute(qc, backend, shots=200) # run the job simula-
tion

result = job.result() # grab the result

counts = result.get_counts(qc) # results for the number of
runs

print(counts); # print the results of the runs
who_wins(counts); # celebrate the winner

plot_histogram(counts) # Visualise the results


{'0': 200}
The winner is A
```

Ergebnis für den Spielverlauf „H U H“

5. Versuch einer anschaulichen Deutung

Die Quantenmechanik verschließt sich an vielen Stellen einer anschaulichen Deutung. Wir wollen dennoch eine anschauliche Darstellung des Münzspiels versuchen, die jedoch zwangsläufig Lücken hat.

Die Münze liege zunächst flach vor uns – natürlich verdeckt und mit Kopf nach oben. Das normale Umdrehen wird durch eine Drehung um 180° um die Achse, die von uns wegzeigt, realisiert. Der „Quantenzug“ von Alice ist dann eine Drehung um 90° um die „Querachse“ der Münze, die dann sozusagen „auf der Kante steht“. Egal ob Bob die Münze in seinem Zug liegenlässt oder dreht (um die Achse, die von vorne durch die Münze hindurch zeigt), die Münze bleibt auf der Kante. Der letzte Zug von Alice legt die Münze von der Kante wieder flach hin – und zwar mit Kopf nach oben. Hier versagt die Anschauung leider etwas, denn der Zug H ist selbstinvers und kippt die Münze bei der zweiten Anwendung nicht um weitere 90° nach vorne, sondern um 90° nach hinten. Es gilt $HH = L$.

6. Das Quantum Münzspiel als Online-Spiel

Nach den sicher sehr interessanten, aber doch eher theoretischen Betrachtungen des Quantum Münzspiels wollen wir eine Möglichkeit vorstellen, dieses Spiel online zu spielen. Auch dabei steht das Kennenlernen verschiedener Aspekte des Quantum Computing im Vordergrund. Das Münzspiel ist nunmal kein MMOG (Massive Multiplayer Online Game).

Eine Implementierung des Quantum Münzspiels ist verfügbar auf http://ibm.biz/QiskitCoinGame . Es wurde vom Autor auf Basis des IBM Quantum Computing Frameworks „Qiskit“ implementiert (https://qiskit.org). Qiskit basiert auf Python und Jupyter Notebooks und ermöglicht neben der Nutzung von Quantencomputer Simulatoren auch die (kostenfreie) Nutzung von realen Quantencomputern über die Cloud. Die Bezeichnungen im QiskitCoinGame unterscheiden sich etwas von denen in diesem Artikel und sind eher an die im Quantum Computing üblichen Begriffe angelehnt. Neben Qiskit wird mybinder verwendet (https://mybinder.org), ein ebenfalls kostenfreier online Service, in dem Jupyter Notebooks ausgeführt werden können, sowie RISE, eine Erweiterung von Jupyter Notebooks um Slideshow/Screenshow Funktionen. Alle Elemente und deren Bedienung werden auf http://ibm.biz/QiskitCoinGame erklärt. Der Start dauert bis zu einer Minute, danach ist die Umgebung recht agil und lädt dazu ein, selber Änderungen am Python Code vorzunehmen und so erste Erfahrungen mit einem eigenen Quantenprogramm zu machen. Für weitere Schritte ist die Literatur am Ende dieses Artikels sehr zu empfehlen.

7. Die Brücke zur Quantenmechanik

Die Darstellung in diesem Artikel ist bewusst einfach gewählt. Um „echte“ Quantenalgorithmen zu verstehen oder sogar selber erstellen zu können, ist eine ausführlichere Beschäftigung mit den Grundlagen der Quantenmechanik und der „Quantum Information Science“ erforderlich.

An dieser Stelle wollen wir nur einen kurzen Einblick zu Zuständen von Quantensystemen und deren Messung geben.

Wir betrachten nur Quantensysteme, die aus einem einzelnen Qubit bestehen und nicht aus mehreren (wir hatten im Münzspiel ja auch nur eine einzelne Münze).

Wir haben bereits einige mögliche Zustände kennengelernt, nämlich Kopf, Zahl und einen Superpositionszustand:

$$K = \begin{pmatrix}1\\0\end{pmatrix}, \quad Z = \begin{pmatrix}0\\1\end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}.$$

Ein allgemeiner Quantenzustand ψ hat die Form

$$\psi = \begin{pmatrix}\alpha\\\beta\end{pmatrix}, \text{ oder gleichbedeutend } \psi = \alpha K + \beta Z$$

mit komplexen Zahlen α, β, die folgende Bedingung erfüllen (eine Art Normierung auf die „Länge eins“):

$$|\alpha|^2 + |\beta|^2 = 1.$$

Die Quantenmechanik besagt, dass es nicht möglich ist, den Zustand eines solchen Quantensystems ψ exakt zu bestimmen, d.h. die exakten Werte von α und β zu messen. Bei einer Messung des Zustands von ψ kann als Ergebnis immer nur der Zustand K oder Z festgestellt werden. Der Ausgang der Messung erscheint dabei zunächst zufällig.

Präpariert man das Qubit jedoch mehrfach in denselben Zustand ψ und führt dann jeweils eine Messung des Zustands durch, so ergibt sich ein Zusammenhang zwischen der Häufigkeit der Ergebnisse K und Z mit den Koeffizienten α und β. Es gilt: die Häufigkeit des Ergebnisses K ist gleich $|\alpha|^2$, und die Häufigkeit des Ergebnisses Z ist gleich $|\beta|^2$. α und β sind verallgemeinerte Wahrscheinlichkeiten, sogenannte „Wahrscheinlichkeitsamplituden“ (man beachte: α und β sind komplexe Zahlen).

Der Zustand ψ ist also wohldefiniert und beinhaltet selber keine Unsicherheit oder Wahrscheinlichkeit. Erst im Rahmen der Messung treten verschiedene Ergebnisse mit gewissen Wahrscheinlichkeiten auf.

Als Beispiel sei $\psi = \alpha K + \beta Z$ mit $\alpha = \beta = 1/\sqrt{2}$, also $\psi = \frac{1}{\sqrt{2}}K + \frac{1}{\sqrt{2}}Z$, und damit der bereits zuvor betrachtete Superpositionszustand von K und Z. Die Wahrscheinlichkeit, bei einer Messung den Zustand K festzustellen, ist nun $|\alpha|^2 = 1/2 = 50\%$, und analog für den Zustand Z ebenfalls 50%.

Eine Superposition muss jedoch nicht gleiche Wahrscheinlichkeitsamplituden für α und β besitzen, sondern es ist z.B. auch folgender Zustand möglich (und unendlich viele weitere): $\psi = \alpha K + \beta Z$ mit $\alpha = 1/2$ und $\beta = \sqrt{3}/2$, also $\psi = \frac{1}{2}K + \frac{\sqrt{3}}{2}Z$. Die Wahrscheinlichkeit, bei einer Messung den Zustand K festzustellen, ist nun $|\alpha|^2 = 1/4 = 25\%$, und für den Zustand Z: $|\beta|^2 = 3/4 = 75\%$.

Eine ausführlichere Darstellung der Grundlagen der Quantenmechanik, des Quantum Computing und auch eine Darstellung des bekannten Quantenalgorithmus von Grover mitsamt seiner Implementierung findet sich in dem Buch von Andrew Thomas „Hidden In Plain Sight 10: How To Program A Quantum Computer“.

8. Ist das Spiel fair?

Zum Abschluss wollen wir diskutieren, ob das Spiel fair ist – und falls nicht, wie dies zu deuten ist.

Da Alice andere Züge verwenden darf als Bob, ist das Spiel nicht fair. Man kann dies jedoch auch anders betrachten: und zwar nicht als Spiel, sondern als Algorithmen. Bob wendet einen klassischen Algorithmus an; Alice jedoch einen Quantenalgorithmus unter Verwendung von Superposition und Interferenz. Wie wir gesehen haben, ist der Algorithmus von Alice mächtiger als der von Bob. Das bestätigt uns in der Erwartung, dass Quantenalgorithmen Aufgaben lösen können, die mit klassischen Algorithmen und klassischen Computern unerreichbar sind. Es sind bereits etliche Quantenalgorithmen bekannt, die Superposition, Interferenz und Verschränkung geschickt ausnutzen. Man geht jedoch davon aus, dass es hier noch viel zu erforschen und zu entdecken gibt. Es lohnt sich daher, sich mit den Grundlagen und dem Potential des Quantum Computing zu beschäftigen!

Qiskit Coin Game erreichbar unter:
https://tinyurl.com/QiskitCoinGame

Literatur: 1. Jan-Rainer Lahmann, Qiskit Coin Game, http://ibm.biz/QiskitCoinGame **2.** Shohini Ghose, A beginner's guide to Quantum Computing, https://www.ted.com/talks/shohini_ghose_quantum_computing_explained_in_10_ minutes **3.** David A. Meyer, Quantum Strategies, https://arxiv.org/abs/quant-ph/9804010v1 **4.** Vassili N. Kolokoltsov, Quantum games: a survey for mathematicians, https://arxiv.org/abs/1909.04466v1 **5.** Andrew Thomas, Hidden In Plain Sight 10: How To Program A Quantum Computer, ASIN: B07GPRBYVC **6.** Qiskit Games, https://github.com/Qiskit/qiskit-community- tutorials/tree/master/games **7.** Qiskit Tutorials, https://github.com/Qiskit/qiskit-iqx-tutorials **8.** IBM Quantum Computing, https://www.ibm.com/quantum-computing/ **9.** Anton Zeilinger, Einsteins Spuk: Teleportation und weitere Mysterien der Quantenphysik, ISBN-13: 978-3442154357 **10.** J. von Neumann, „Zur Theorie der Gesellschaftsspiele“, Math. Ann. 100 (1928) 295- 320.

Dr. Jan-Rainer Lahmann

Studium der Technomathematik an der TU Clausthal, Promotion am KIT Karlsruhe über Angewandte Mathematik und Strömungsmechanik. Seit 1999 bei IBM in der technischen Vertriebsunterstützung (Hardware, Analytics/BigData, Cloud). Mitglied der IBM Academy of Technology und Qiskit Contributor.

Thomas Haag

Studium der Informatik an der Fachhochschule Frankfurt am Main. Seit 2002 bei der deutschen Lufthansa, verantwortlich für Datamanagement, BI und Analytics in der LH Group.

Foto: IBM, TED, J.Lahmann, Privat

Very Digital Person: FAISAL SHAH KHAN

Quantum Computing (QC) brings a lot of hopes and new perspectives. When will QC replace our conventional smartphones, laptops and tablets?

To reach this stage of quantum ubiquity, a thorough understanding of how to interface conventional and quantum computational processes is needed. This is because any useful quantum computer has to be programmable. But this is a difficult task because the quantum realm is fickle, and objects in it decohere almost instantaneously upon interaction with the realm of conventional devices and programmers. Imagine trying to pass a thread through the head of a needle the size of a dust particle. Programming a quantum processor is orders of magnitude more challenging. But just like one can further imagine splitting the thread into finer and finer strands until reaching a strand thin enough to pass through our miniscule needle head, so can one imagine layers of physical processes starting with one that is conventional but with each additional layer transitioning toward the quantum realm. Ultimately, one imagines a layer of physical processes that bridge the quantum and classical realms. The collection of these processes serves to interface the classical programmer and the quantum computer. Quantum computing will replace conventional devices such as laptops and smartphones when scientists and engineers fully understand the interface of quantum and classical computational realms.

Where are we today in QC's development path? What are some current problems? Which kinds of problems do you work on?

The current stage of development of Quantum Computing is roughly similar to the stage at which conventional computing was during and immediately after the 2nd World War. This was the time of massive computing machines like the ENIAC (Electronic Numerical Integrator and Computer) and the MANIAC (Mathematical Analyzer Numerical Integrator And Computer Mode) which would take up large rooms to fit, but which would calculate solutions to only the simplest of problems. This is also the situation with respect to the current, first generation of quantum processors, which also physically take up large spaces but can only solve a small class of problems or problems of simple nature. This is largely due to the heuristic philosophy that has driven the development of this generation, which has left open problems relating to fully optimizing its development and performance. For Quantum Computing to evolve into a more efficient next generation, it is essential that the lessons learned from the efforts put into developing current Quantum Computing platforms be cast into formal mathematical machinery such as algebraic geometry, differential geometry, and topos theory. And these same lessons, combined with the insights gained from the mathematical machinery they are cast unto, must be used to foster developments in physics and materials science and engineering so that platforms for the next generation of Quantum Computing are closer to realizing the full potential of this technology.

"The current stage of development of Quantum Computing is roughly similar to the stage at which conventional computing was during and immediately after the 2nd World War."

I approach the problem of optimizing the next generation of Quantum Computing from a differential geometric point of view. More specifically, I am interested in the work of the late Nobel laureate John Nash. While Nash is more famous for his work in game theory where he developed the notion of Nash equilibrium, it is his work on the isometric embedding of Riemannian manifolds (the model for Quantum Computing) into Euclidean spaces (the model for conventional computing), that interests me. In particular, I want to understand Nash's embedding as a solution to the problem of interfacing quantum and conventional computing paradigms, with specific focus on:

i) Fabrication of hardware architectures that perform Quantum Computing, but which necessarily reside in Euclidean space.
ii) Understand what firmware for quantum computing is required.
iii) Develop robust cyber-security protocols resistant to Quantum Computing attacks.

Other mathematically formal approaches I am pursuing in this context include non-commutative geometry, topos theory, and a theory of fixed-points in the quantum computational domain. The latter is interesting to me because it may allow the application of Nash's Noble prize-winning work on equilibrium in games to constrain-optimize the performance of quantum processors.

After having solutions, what are the future major impacts of QC?

Let me start with the Nash equilibrium. In strategic interactions between "players", Nash equilibrium is an outcome that no player wishes would change. In other words, given the strategic choices made by all the players, Nash equilibrium is an outcome of the interaction where each player is most satisfied. This idea serves as a solution concept in many applied areas, including economics, computer science, evolutionary biology, and politics. As ubiquitous as its usefulness is, the problem of calculating Nash equilibrium outcomes in interactions with a large and practically meaningful number of players is computationally intractable for conventional computing. The ability to quickly solve for

Nash equilibrium using Quantum Computing will have a dramatic effect on all areas of strategic decision making, with finance, politics, and biological sciences potentially being revolutionized due to the fundamental role Nash equilibrium plays in these fields.

Another major impact would be on computing solutions to problems in fundamental sciences. This was the idea behind Richard Feynman's original proposal for a quantum computer, where the properties of a complicated quantum physical or chemical system were simulated on a simpler one which was easier to control. This allowed quick solutions to problems that were intractable using conventional computers. Consider for instance the problem of water desalination (or water purification in general). While membrane technologies using the idea of reverse osmosis exist and function efficiently from several practical points of view, it is nonetheless fruitful to ask what the minimal energy for separating the molecules of salt and water is. Quantum computing can answer this question. When combined with techniques in artificial intelligence, a quantum computer can be trained to calculate the separation efficiency as a function of the molecular components. Resulting insights have the potential to make current and future desalination technologies socio-economically optimal by suggesting the feasibility of any separation process on the basis of the thermodynamic barrier for molecular separation.

Is the quantum computer a risk for our conventional security keys?

Yes, absolutely! Especially those security keys that are constructed using prime number multiplication and taking discrete logarithms. These two mathematical procedures, which have formed the backbone of secure key generation for the past several decades, have been conclusively shown to be trivial to break using a sufficiently large and fully functioning quantum computer. While the current first generation of quantum computers is not a threat to security keys, I imagine that this threat would be very real within a decade, and maybe even less. However, several methods have been forwarded to thwart Quantum Computing attacks on security keys, and these include making keys using alternative mathematic methods such as lattices, or using the quantum physical phenomenon of ideal randomness that even a quantum computer cannot discern patterns in.

"So while somewhat indirectly connected to the question of Quantum Computing and computer games, this discussion points to another improvement Quantum Computing can offer to the theory of games in general."

What's the connection between QC and the modern computer game?

There are two perspectives I would like to give here. The first one deals with graphical representation and image resolution. In modern computer games, three-dimensional features and motion are depicted onto a two-dimensional screen. This dimensionality reduction is not so much the problem as is the Gimbal lock, a situation affecting rotations in three-dimensional space where one degree of freedom is lost. The Gimbal lock manifests in computer graphics as an abrupt, discontinuous motion that is aesthetically unpleasant and which can adversely affect the user experience. The way to avoid Gimbal lock in computer graphics is by first representing three-dimensional rotations as four-dimensional objects known as quaternions, and then projecting these quaternions into the two-dimensional graphics space. The result is a smooth, continuous motion in two dimensions that may in fact enhance the user experience beyond what is experienced in reality.

The connection of all of this with Quantum Computing becomes clear when one notes that an important subset of the quaternions, the unit quaternions, is in fact mathematically equivalent to Quantum Computing! In other words, when one enhances two-dimensional computer graphics using quaternionic algebra, in effect, one is simulating a quantum computation on a conventional computer! Given that conventional computers have limited capacity in simulating quantum computations, one can only imagine the enhancement to computer graphics that can result from interfacing this process with an actual quantum computer.

The other perspective relates to the topic of Nash equilibrium that I mentioned earlier. Board games and computer games are entertaining because their makers either ensure that at least one player wins, or they try to build an interesting Nash equilibrium outcome. Take Tic-Tac-Toe for example; either one player wins this game, or both players end in a draw, which is a Nash equilibrium. However, this is hardly an interesting equilibrium outcome. What scientists studying the theory of "quantum games" have shown is that if a conventional game is enhanced using quantum computational techniques, then enhanced and interesting Nash equilibrium outcomes manifest. For example, in the famous game of Prisoner's Dilemma, where a pair of conspiring thieves are arrested and interrogated by police in separate rooms, the Nash equilibrium outcome is one where each thief implicates the other and spends the maximum amount of time in jail. This situation can be im-

Faisal Shah Khan

Faisal Shah Khan currently serves as an Assistant Professor of Mathematics and Principal Investigator in the Center on Cyber-Physical Systems at Khalifa University, Abu Dhabi.

He has a PhD in Mathematical Sciences from Portland State University, earned under the supervision of Professors Steven Bleiler and Marek Perkowski.

Khan has supervised graduate and undergraduate students on projects involving Quantum Computing, imaging, and non-cooperative game theory.

His research work involves studying the Nash embedding theorem, using differential geometry as a mechanism:

a) for developing programming paradigms that will allow a classical programmer to program a quantum computer, in a mathematically and physically robust way.

b) for identifying fixed-point stability in quantum games with applications to locating equilibrium and optimal performance of quantum computations.

proved upon in a quantum mechanical version of the game. So while somewhat indirectly connected to the question of Quantum Computing and computer games, this discussion points to another improvement Quantum Computing can offer to the theory of games in general.

Is there a connection between QC and artificial intelligence?

I will refer here to the persuasive work of Johnjoe Mcfadden and Jim Al-Khallili's. These two physicists consider quantum physical effects like entanglement and measurement to have played an indispensable role in the development of life, its evolution, and the emergence of consciousness. If quantum physics can play a role in the development of a higher order of natural intelligence, that is, consciousness, then I don't see why quantum computation would not play a fundamental role in the development and emergence of the much simpler notion of artificial intelligence.

A glimpse at the future: what is your vision of a quantized world?

The science fiction icon, Isaac Asimov, proposed the idea of computers and robots with artificial consciousness all the way back in the 1950's. In fact, two robotic protagonists in his novels consciously conspire to bring about the development of humanity as a galaxy-faring species. Unlike conventional electronics even back in the 1950's, Asimov's robots had brains that processed positrons instead of electrons. I have decided over the years that this was Asimov's way of expressing his premonition of quantum computers! But he more accurately expressed his vision of a quantized future in a short story titled *The Last Question*, where he envisioned generations of humanity and the artificially intelligent computers it builds, evolving in tandem until the computer and its creators merge into one, giving the computer sentience, and ultimately, a form of godhood.

While I share Asimov's vision of a future quantized world, I like to think that I am a bit more conservative. I certainly feel that Quantum Computing will play a crucial role in the development of fast and accurate artificially intelligent agents that may also evolve a certain level of consciousness. But unlike those who predict a Skynet-style termination of the human species due to AI, I like to think that conscious AI will be benevolent. For consciousness is an essential pre-requisite for the development of culture, and a culture requires, at the very least, a selfishly-motivated concept of altruism to be successful. I think AI and QC will be abundant in the quantized world of the near future, and that this will produce a wonderful and bright future for humanity.

"I certainly feel that Quantum Computing will play a crucial role in the development of fast and accurate artificially intelligent agents that may also evolve a certain level of consciousness."

Interview: Hannes Mittermaier

Photo: personal

The Physics Behind the Quantum Computer

Prof. Dr. Gerhard Kirchmair on the smallest of the biggest

In order to be able to execute complex algorithms, quantum computers rely on the laws of quantum physics. This gives them an enormous power potential, which could soon give quantum computers the possibility to surpass conventional computers. Prof. Gerhard Kirchmair, who conducts research on superconducting quantum circuits and superconducting qubits at the Institute of Experimental Physics at the University of Innsbruck, explains which physical foundations are hidden behind a quantum computer.

Physics deals – among other things – with the smallest particles. The term "quantum" is now on everyone's lips. From a physical point of view, what stands behind "quantum"?

A "quantum" is something that can only occur as an integer multiple, which, if you like, can always be found as a "packet". Examples of this would be: electrons, photons (i.e. light particles), but also, for example, vibration quanta, which are called phonons. Quanta cannot be divided, so there are no half-photons or electrons. In experiments, for example, it can be shown that light can behave both as an electromagnetic wave and as a particle (photon).

This leads to the assumption: light = particles.

Exactly! In quantum physics, there is the so-called "wave-particle-dualism": particles behave like waves, and vice versa. Thus, one can observe wave phenomena such as interference on individual particles that respond to quantum physics. Whether we consider quanta to be a particle or a wave depends on the experiment and the realized measurement.

Is the world of quanta the physical attempt to reduce the world to energy-loaded particle portions?

This is one aspect of the whole, whereby the concept of the particle can be seen here more abstractly. A good example of this is vibration quanta in a solid. The vibrations are quantified by many atoms in the solid at the same time, yet only certain packets of energy, i.e. phonons, can be brought into this collective vibration.

Quantum physics also allows for phenomena that do not exist in classical physics, which means in our everyday life. For example, quantum physics allows a particle to be in two places or in two states at the same time. This is called a superposition. Experiments show that we can actually realize such and even more exotic conditions. When we measure the position of a particle in such a superposition, it randomly picks one state or the other. The measurement thus brings the particle into one of the two states – one speaks of a "projection".

"Quantum physics also allows for phenomena that do not exist in classical physics, which means in our everyday life. For example, quantum physics allows a particle to be in two places or in two states at the same time."

What does the "Planck constant" have to do with the quanta?

The Planck constant is a natural constant that occurs whenever one wants to describe effects in quantum physics or to specify properties of the quantum. A simple example would be the energy of a photon, which is calculated by its frequency, i.e. the light color, multiplied by the Planck constant.

What is the difference between "quanta" and "qubits"?

Qubits are created, for example, by quantizing energy in a potential. Ultimately, a qubit is a system that can assume the two discrete states— analogous to a classic bit— 0 or 1. The difference, however, is that a quantum bit assumes both states at the same time. This simultaneity is then called superposition. Several qubits can then be in multiple states at the same time. For example, for two qubits, that would be "00 + 01 + 01 + 11". For n-qubits it would be 2n states. You can use quanta (e.g. electrons or photons) to build qubits.

How are qubits made?

There are many ways to produce qubits. Three examples are:

1) Ions/atoms: Two energy levels in the atom are used as a qubit. To understand this, one has to remember the shell model for atoms from school chemistry. Electrons occupy different states/shells in the atom. Now, for example, you can use a laser to lift an electron from one shell to another shell. With this, one has realized its two states and thus the qubit – the electron in one shell is the 0, in the other the 1. With the help of a laser, one can then create superpositions of these states.
2) Superconducting qubits: Here electronic components such as coils and capacitors and the so-called tunnel contact are used to create a two-state system. This tunnel contact is a very thin, non-conductive layer between two superconductors. Electron pairs – or rather Cooper pairs in the superconductor – can tunnel through this barrier without loss. This allows you to bring a Cooper pair to the "plate" of a capacitor. If the Cooper pair is missing, then that is the state 0, if it is there, then it is the state 1.
3) Photons: Quantum information or qubits can also be encoded in properties of photons. For example, in the polarization of a photon, i.e. the direction of the electric field of the light wave.

After that, can we say that the quantum computer is an organized machine of quantums that react to external stimuli? What physical framework conditions does a quantum computer need in order to function at all? Why does it need them?

Yes, in a way, a quantum computer consists of very well-controlled quanta, which are specifically manipulated from the outside. However, it is necessary to ensure that the environment cannot come into contact with the quantum system, otherwise all quantum effects will disappear. By interacting with the environment, the qubits would be measured and the superpositions would disappear.

So you have to make sure that the quanta are shielded from the environment. This can be achieved for atoms, for example with vacuum appliances and lasers. In addition, you have to make sure that all qubits start in a well-defined state (for example at 0) so that the computational operations also make sense. For this you usually have to cool the qubits, so take all the suggestions and energy out of the system. Depending on the technology you use, these requirements for the quantum computer vary.

Quantum computers only operate at a certain temperature, which is very expensive to produce. Do you see physical solutions in the foreseeable future to be able to use the quantum computer even at room temperature?

There are approaches to how the quantum computer could also be operated at room temperature: a quantum computer made of photons, for example, works at room temperature. However, even in practice, cooling is not a real obstacle to the realization of a quantum computer.

Why can physics itself benefit from the use of a quantum computer?

It turns out that it is very difficult or even impossible to calculate the properties of quantum systems with classical computers. For example, it would be interesting for pharmacy and chemistry to calculate binding energies in molecules (a quantum system consists of several bound atoms), since reaction rates and the like can be derived from them. With such a quantum computer, one could also better understand large bio-molecules and thus develop new drugs or better understand the properties of known medicine.

You can also better understand solids with a quantum computer and try to answer open questions in physics. Among these questions, for example: why is there a high-temperature superconductor, and is superconductivity possible at room temperature?

"There are approaches to how the quantum computer could also be operated at room temperature."

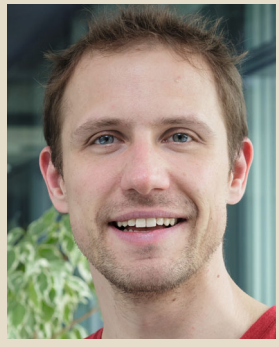
Which inventions already used in everyday life today are based on the assumptions of quantum physics?

A modern Nuclear Magnetic Resonance (NMR) system works because we can specifically influence states in molecules with magnetic fields. One of the most sensitive magnetic field sensors available commercially is a so-called "Superconducting Quantum Interference Device", or SQUID. As the name suggests, its function is based on quantum effects. This technology is used, for example, in brain current measurements or generally for measuring very small magnetic fields.

In the new definition of our SI units, many sizes are determined using quantum effects. For example, the second is defined by the period of electromagnetic radiation that a cesium 133 atom brings from one state to another. So you can build very accurate clocks with quantum effects and atoms. For example, each GPS satellite carries an atomic clock with it in order to determine the duration of a signal from the satellite to the receiver as precisely as possible. All other watches would be far too inaccurate and would cause deviations of many kilometers.

Interview: Hannes Mittermaier

Prof. Dr. Gerhard Kirchmair



Gerhard Kirchmair was born in 1981 in Hall i.T., Austria. He studied physics at the University of Innsbruck, where he also completed his master's thesis in the group of Prof. Rainer Blatt. For his PhD thesis, he continued his research in the group of Prof. Blatt, where he works on the realization of protocols for quantum information processing and quantum simulation with calcium ions in a linear Paul trap. He received his doctorate in 2010 under the auspices of the Federal President Heinz Fischer. From 2010 to 2013 he conducted research in the group of Prof. Rob Schoelkopf at Yale University in the USA. There he got to know the area that he now wants to re-establish in Innsbruck: quantum research with superconducting circuits. In March 2013, he took up a professorship in Innsbruck and since the beginning of 2018 he has been a professor at the Institute of Experimental Physics. In 2016, he received a Starting Grant from the European Research Council (ERC) and a Fellowship from the Canadian Institute for Advanced Research. The research of the working group led by G. Kirchmair focuses on superconducting quantum circuits and superconducting qubits.

Photo: personal

PlanQK – Quantum Computing Meets Artificial Intelligence

How to make an ambitious idea reality

The project has just been born. Admittedly, the idea is highly ambitious, but it is precisely for this reason that PlanQK – which stands for "platform and ecosystem for quantum-assisted artificial intelligence – wants to combine the two technologically alien areas of Quantum Computing (QC) and artificial intelligence (AI) to build a community through innovative solutions, from which the small and medium-sized enterprises in particular should benefit industrially. Although there are a large number of algorithms for quantum computers, e.g. on websites, textbooks and scientific publications, deciding which algorithm can be used in which situation and how AI methods and algorithms can be used on a specific-manufactured quantum computer requires a comprehensive understanding of theory and technology. Scientific research and applied practice are expected to interact over the next three years to realize PlanQK. The concept is supported by the German Federal Ministry of Economics.

Prof. DDr. Frank Leymann is the Scientific Director, i.e. the architect of the platform that is to be created in PlanQK and enables the inclusion of algorithms from sources such as the web, published articles or books. In addition to ML- and QC-algorithms, data also plays a central role and should be able to be disseminated and distributed via the platform. Such data pools can come, for example, from publicly accessible sources or from users and customers of the PlanQK platform. These algorithms and data pools are stored in a special database, the QKI-Algorithm & Data Content Store.

How did the idea of PlanQK come about? How did you become part of PlanQK?

I am a mathematician and astrophysicist, but after my doctorate I moved to IBM and became a computer scientist there, then I moved to the University of Stuttgart as a professor of computer science. There I work a lot with the local industry, and almost three years ago one of the executives of a company said: "You are a mathematician and physicist – and also a computer scientist. Can't you work with us on Quantum Computing?" Soon I realized that this has potential to change the industry! Since I have been working on BMWi-funded projects for many years, I thought it was extremely important to illustrate the emerging practical maturity of the technology on several occasions. Then, at the beginning of the year, there was the AI-Innovation-Competition, and I thought, what is more innovative than the combination of AI and QC?! So I was able to convince a small consortium to submit a joint application to be supported by BMWi for the development of a roadmap in the area. We were successful and were able to develop this roadmap by late summer, put together a large consortium and apply for a project.

Who is involved in the project today and how are the partners tied to the project?

The consortium consists of four research partners (Universität Stuttgart, Ludwig-Maximilians-Universität München, Freie Uni-

versität Berlin and Fraunhofer) and eleven companies of different sizes, from startups to SMEs to large international companies. However, we also have a lot of associated partners who have promised us support. The research partners are concerned with solving the technical challenges as much as possible. The industrial partners will bring in use cases that they will solve using different techniques of machine learning, using the special algorithms on quantum computers. The industrial partners also contribute components to the platform and verify the coherence of the ecosystem. The benefits for industrial partners stem from the advantages of quantum computers and quantum algorithms. A number of these quantum algorithms are much faster than classical algorithms or have higher precision. There are also problems that cannot be solved in practice on conventional computers, but can be solved with quantum computers – although today's machines have to start with smaller problems. But the consulting business also seems interesting, because at the very beginning of the use of quantum computers, companies do not yet have the necessary skills and therefore need external help.

"What is more innovative than the combination of AI and QC!"

What is PlanQK's new technical approach? Where do you see the biggest challenges?

First of all, we want to provide machine learning solutions, created with the help of quantum computers, and make them "digestible" for companies. For this purpose, we automatically collect algorithms from the scientific literature that describes corresponding algorithms and present these algorithms uniformly in the form of a sample language.

However, these algorithms must be analyzed and evaluated to provide results on quantum computers that die in the next two to three years. The quantum effects on which these computers are based are very sensitive, because the corresponding components do not hold data for very long, interfere with each other slightly and become so with longer calculations. We want to develop a component that tells an algorithm whether and on which specific machine the algorithm can solve a given application problem. That is the biggest challenge we face.. This is the biggest challenge we face! But we will also solve problems in a classic and quantum computer way to build up knowledge of which types of problems quantum computers can actually solve. All of this is then to be done on a platform that is accessible to everyone. Such features, which allow users to find appropriate solutions, are another challenge. Then, of course, we will implement the algorithms on quantum computers as well. It should be noted, however, that a comprehensive solution will always be hybrid, i.e. it will be data from conventional computers such as quantum research. Where and how to split the solution is the next challenge. In addition, the next step is to ensure that a quantum program is run "at the touch of a button" on a quantum computer. Overall, this is a lot of new territory that we are going to do, but I am confident because, as a consortium, we have a lot of competences to be successful here.

How does communication within the project with employees and partners work?

We have given ourselves a governance structure that we believe will work between the use case partners, the research partners and the consultants. There are also regular meetings in the consortium to discuss the use cases and their possible solutions. Meetings will also be held with existing associate partners to strengthen the community and promote the use of the platform. But new associated partners are also very welcome. To this end, we have appointed our own "Community Manager" to organise events and conduct appropriate marketing for them.

Why are SME companies so important to PlanQK?

Because it is precisely small and medium-sized (SME) enterprises that suffer from staff shortages in the field of artificial intelligence and can benefit from the ecosystem that emerges in PlanQK. You may have heard about Quantum Computing here, but you can't think of anything concrete about it, because the people who know the field are even rarer than AI specialists, who are difficult to get to.

How exactly could PlanQK be used in a few years?

For example, a company that finds quality control issues and has initial ideas that could be solved with AI can contact the marketplace, which is also being created in PlanQK. This is a commercial platform and an ecosystem where, for example, experts are found who can solve the problem. This allows the company to purchase appropriate consulting services or development services. Or a company has found a quantum algorithm on the freely accessible platform that solves one of its problems, but lacks the knowledge to implement it on a quantum computer. Developers can then be sought for implementation in the marketplace.

Frank Leymann

Frank Leymann is Professor of Computer Science and Director of the Institute of Architecture of Application Systems at the University of Stuttgart. His research interests are in service-oriented architecture and middleware, workflow management and business processes, sample languages, cloud computing, the Internet of Things, integration technologies, and transaction processing. Frank Leymann worked for the IBM Software Group for twenty years in the development of database systems and middleware products. Parallel to these activities, Frank Leymann worked since the end of the eighties on all questions of workflow technology and became "father" of the workflow products of IBM. As an IBM Distinguished Engineer and elected member of the IBM Academy of Technology, he was a member of a small team responsible for the architecture and strategy of IBM's entire middleware portfolio. He was also responsible for the architectural aspects of on-demand computing (now known as cloud computing) for the IBM Software Group. Since 2000, Frank Leymann has worked as a co-architect of the Web Service Platform. He is a co-author of numerous Web Service specifications and standards from the BPM and cloud sectors. Frank Leymann is a member of the European Academy (Academia Europaea). He has published numerous articles in journals and conference volumes and is co-author of four books. He holds nearly 60 patents, especially in the areas of workflow management and transaction processing. For many international conferences he has been a member of the Programme or Organization Committee, and he is (associated) editor of some journals. From 2006 to 2011 he was a member of the scientific director of Schloss Dagstuhl (Leibniz Center for Computer Science).

The platform to be developed with PlanQK provides access for customers, service providers and experts. It should also produce the interfaces to the various quantum hardware components. The project management is carried out jointly by Frank Leymann and Andreas Liebing, where Liebing takes care of the technical coordination as product owner. He is particularly responsible for the production and implementation process of this platform.

A year and a half ago, Andreas Liebing took part in a scientific summer camp at the University of Stuttgart. This is also where the basic idea of PlanQK came into being. Since the first publications on Quantum Computing, Liebing has been fascinated by this completely new technology. In the combination of artificial intelligence and Quantum Computing, Andreas Liebing also sees one of the greatest challenges, but at the same time an enormous appeal of this project.

How would you personally like to create this connection in your role as project coordinator?

There are a number of AI methods that are very computationally time-consuming. This extends to procedures that can be calculated theoretically, but not in practice, or at least not yet. A quantum computer allows a very different approach to solving these problems. So it will be about the intelligent combination of AI methods with Quantum Computing: can one map processes completely? Is it possible to map parts of it? Is this a significant acceleration of computational processes that have taken a very long time to date? In a series of nationwide workshops with numerous companies, we got to know a wide range of problems that are currently insoluble.

Why do you use the quantum computer here?

The quantum computer offers an enormous increase in speed, and – as it stands today – is already on a par with the largest supercomputers on earth. This speed will increase many times over due to the technical progress of the coming years, thus allowing for operations that are still unthinkable today. For example, I can think of the calculation of new molecular chains for batteries, which will play a decisive role in electromobility. Perhaps it will soon be possible to produce significantly better batteries in terms of resources and ecology. This also explains why car manufacturers, for example, are very interested in these new technologies.

In addition, a quantum computer itself is already more environmentally-friendly than conventional computers, because it needs much less electricity.

How innovative is PlanQK's approach?

At present, as far as we know, there is only one approach comparable to PlanQK in the US. As far as we can tell, PlanQK is definitely at the forefront.

We are absolutely convinced of the innovative power of our idea. Shortly after the announcement of our project, numerous companies along the entire value chain – users, consultants, service providers, software developers and hardware providers – as well as the leading universities, all expressed their interest in participating in this project. This means that we are well positioned to establish our platform and the associated ecosystem on a permanent basis and to strengthen Germany as a location in this future market.

When can you imagine presenting concrete results?

The project is officially designed for three years. By the end of the project at the latest, we will have built a powerful platform and the corresponding community. Due to the very high degree of complexity and a wide range of problems, we can also imagine expanding the project and extending it beyond this period. We are all betting on the next technological leaps. This starts with the quantum computer itself, which will certainly be much more powerful in a year or two. Currently, there are only around a handful of relevant suppliers that are eligible for our technical requirements. A lot will happen here, too.

"Perhaps it will soon be possible to produce significantly better batteries in terms of resources and ecology."

And if PlanQK works? What concrete work situation with PlanQK could become a reality?

We want to build a customer base that ranges from small and medium-sized companies to large corporations. Consultants, developers, service providers and hardware manufacturers can place their offerings on the platform. In this way, everyone can benefit from PlanQK, whether as a provider of services or as a user. Smaller companies in particular have the opportunity to use the new technologies of Quantum Computing and AI on a case-by-case basis and at a reasonable cost. All in all, we then offer a communicative exchange service in which the participating companies are guided to their individual solutions by trained personnel. Our stated goal is to become the preferred European platform for quantum-assisted artificial intelligence.

Andreas Liebing

Andreas Liebing, a native of Berlin, is the founder and CEO of StoneOne AG. With more than 30 years of experience in the IT business, he is now one of the German visionaries in the field of information management and cloud computing. Already during his studies at the Technical University of Berlin (Mathematics and Computer Science), he began to deal with the central administration of information. In 1985, Andreas Liebing founded SAPERION AG, which he headed as CEO until 2005. During this time, the company successfully established itself in the areas of workflow, document management and archiving.

At the beginning of 2007, he launched StoneOne AG, which specializes in Platform as a Service (PaaS) and Cloud Computing. Andreas Liebing made numerous contributions on the topic of cloud computing, for example in the BITKOM publication "Industrialization in Outsourcing" on the topic "New Opportunities for Providers and Customers through Software as a Service (SaaS)". At the Berlin University of Technology and Economics, he lectured on the topic of business applications on the web. In 2004 Andreas Liebing was nominated and awarded as Entrepreneur of the Year by Ernst&Young and Manager Magazin, together with Dr. Mathias Petri.

FCE Frankfurt Consulting Engineers GmbH (FCE) is a mathematically-oriented engineering firm based at Frankfurt Airport in the "House Of Logistics and Mobility (HOLM)". FCE was founded in 2004 as a German limited liability company, based on the experience of its founder, Dr. Wolfgang Mergenthaler, which includes 12 years as an independent engineer, and 20 years as an employee in the automotive industry in Germany and the USA. FCE has extensive experience in the industrial application of mathematical statistics, mathematical optimization, pattern recognition, etc. As a consortium member, the FCE is involved in the PlanQK project. Dr. Wolfgang Mergenthaler explains the reasons for this:

How did you hear about the idea of PlanQK? How did the first contact came about?

I am a former employee of Daimler AG, which expressed its interest in Quantum Computing in 2017. In this context, a former colleague established contact with Professor Frank Leymann. Everything came together at several workshops in Stuttgart, to which we as a company made some contributions. In May 2019, we as a company were invited to join the PlanQK consortium, which we immediately decided to do with conviction.

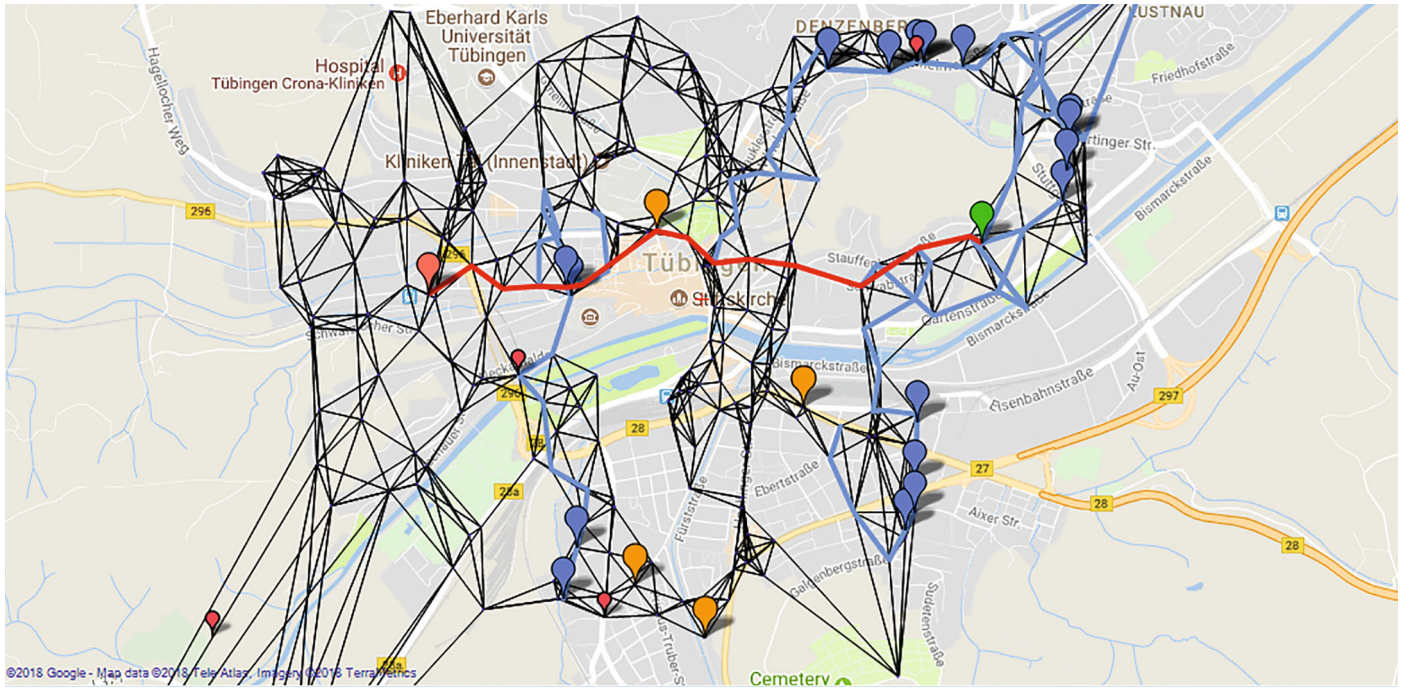
What substantive argument convinced you to join PlanQK?

We have been working for many years in just two mathematical fields: On the one hand, we deal with pattern recognition in the field of preventive maintenance, such a of locomotives and large-scale plants – and there above all with the method of supervised learning; on the other hand, we are working on integer nonlinear optimization tasks, especially in the field of production planning. PlanQK's goal meets our many years of experience with algorithmic performance in combinatorial optimization tasks, and ideally meets our interest in a quantum leap in solving these tasks.

What contribution do you make to the development and development of PlanQK?

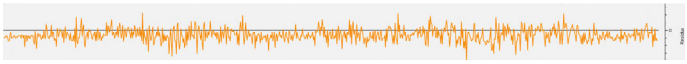
In many places we will help with the work packages defined by PlanQK. This applies both to the development of algorithms and to verification in the sense of the four-eye principle. In addition, there are independent contributions, which we will design ourselves. We have summarized these in two use cases from the field of integer optimization (UC1) and linear algebra (UC2). Use Case 1 is primarily about routing topics such as DVRP (= Dynamic Vehicle Routing Problem), but also about relatives of the Travelling-Salesman problem or more generally about permutation optimizers. What hides behind "linear algebra" is a very exciting field: For example, we are developing a very complex Monte Carlo simulation program for a large German plant manufacturer to calculate the shortfall in a large plant, such as a cement plant. This is based on a graph in which a large number of matrix operations are due. We are confident – although the proof has yet to be provided – that we can solve these matrix operations with the quantum computer faster than before. My anchor on the topic: If we had an effective quantum algorithm for solving matrix-matrix and matrix-vector multiplications as well as for solving linear equation systems, the calculation time could be about 10%

"PlanQK's goal meets our many years of experience with algorithmic performance in combinatorial optimization tasks and ideally meets our interest in a quantum leap in solving these tasks."



The so-called DVRO (Dynamic Vehicle Routing Problem) occurs with the optimal control of demand-responsive transport services (also known as 'dial-a-ride' services). The DVRP is a rolling TSP (= Travelling Salesman Problem). The goal of the DVRP is to optimally balance the distance travelled with the passengers on board. A minimum distance usually has the visualizable property of the lowest possible medium curvature.

of the current value. We do not know when exactly this will be, to be honest. What is certain is that it will happen at some point.



Deviation of the actual arrival date from the promised arrival date: A maximum adherence to the appointment has the graphical effect that the average deviation of the actual from the promised arrival date is small.

What do you think is the biggest challenge PlanQK has to overcome to make the platform marketable?
In addition to the quantity or qubit problem, it is above all the construction of a universal computer structure that will be a challenge. The goal must be to build a universal computer that you can use at some point like a PC. We have been working on the IBM quiskit platform for six months now and have not yet found the place where you could effectively perform everyday arithmetic operations. That alone means a great deal of effort. With a universal computer, you would have to get all the arithmetic as a minimum. Either it is as difficult as we think at the moment, or we simply do not see the solution to the problem yet.

Do you have a specific timetable for implementing your approaches?
The question can be answered with the criterion "closeness of reality": UC1 is likely to be added in 2020 with reasonable effort. UC2 is, in terms of time, open. I am talking to a lot of people at the moment, and we are also conducting intensive literature research ourselves. We are very deep in the matter and are intensively looking for examples from linear algebra. If this problem is solved, then implementation could be very rapid. An application example: An insurer insures a large plant defect and needs a premium calculation to do so. The current practice must be more transparent: the policyholder wants to be convinced of the method. The best way to do this is to use simulation, and in the future it will only have to take place on a very powerful computer, such as a quantum computer, for large plants for performance reasons.

"My anchor on the topic: If we had an effective quantum algorithm for solving matrix matrix and matrix vector multiplications as well as for solving linear equation systems, the calculation time could be about 10% of the current value."

In which economic sectors do you see a particular relevance for PlanQK? Why?
There are already some applications from industry in which the quantum computer has established itself – for example in quantum chemistry. But that is not our area of work. We see the whole thing more from the perspective of logistics, for example in production planning or in other sub-projects of PlanQK, such as the quantum presentation of pattern recognition methods. In any case, this involves route planning, navigation, preventive maintenance and plant simulations. Here I really see potential that can be implemented with PlanQK.

How does communication within the PlanQK consortium work?
We do not yet know that ourselves! There are a large number of bulletin boards and workshops, as well as publications and conferences, which are planned within PlanQK. All of this starts in January 2020. We have to wait and see how well this will work out. In essence, I see the organization tied to the workshops. However, we will still need practical experience to develop an advantageous workflow. In the beginning, there will probably be a bit of a bump, and there will be disillusionment, but there is a lot of enthusiasm among everyone.

Are you concerned that other large companies with more capital could pre-empt your project?
I have been the head of an SME for about 40 years. I have repeatedly stated that if you are prepared to take on all the mathematical complexity of the world, then the air is relatively thin: here the large tankers are usually slower than us. But as soon as you reduce your own ambition – it's a step cheaper! – you lose the advantage of maneuverability. From that point on, they have faced competition. The people who work in large companies, for example, have an enormous horizon of experience and resources, but leave their jobs at 5 p.m. to get home. At an SME, if a problem is not solved, then you stay until 10p.m. I don't know if that's a good answer, but it's the best and most honest I can offer you at the moment.

And if PlanQK works? What specific work situation with PlanQK could be a reality, in which your contribution is used in an applied form?
At the moment, dial-a-ride projects are sprouting up like mushrooms in many cities. In public transport, there are permanent travelling salesman problems. Imagine a city like Munich: if you had 200 dial-a-ride buses instead of 50 large-capacity buses, then the dial-a-ride operators would demand a quantum computer in the foreseeable future simply because the number of requests will increase massively, and this is exactly what a quantum computer can handle best. PlanQK's routing includes several work packages that address order issues that are located on the PlanQK platform. That, at least, is the vision!

Dr. Wolfgang Mergenthaler

Dr. Wolfgang Mergenthaler is Managing Director and owner of FCE Frankfurt Consulting Engineers GmbH in Frankfurt am Main. In 1973 he obtained his diploma in physics from the Technical University of Munich (TUM) and in 1978 his doctorate in applied mathematics, also at the TUM. In his current position, Dr. Mergenthaler leads a team of mathematicians and computer scientists working in pattern recognition, mathematical statistics, probability calculus, and Combinatorial Optimization with Industrial Applications. Plant simulation is one of its strengths, both operationally and in planning terms. Other important areas of work include sequencing and scheduling in production planning, and generating response surfaces from process data.

Christoph Roch is doing his PhD at LMU Munich at the Chair for Mobile and Distributed Systems, with a focus on optimization problems and their solutions through Quantum Computing. The computer scientist is also a member of the Quantum Applications and Research Lab (QAR-Lab) and contributes his knowledge to various industrial projects, research and teaching. In addition, he will also participate in the BMWi-funded PlanQK project.

Christoph Roch (LMU Munich) at the PlanQK booth at the Digital Summit 2019.

At the QTOP19 workshop organized by the LMU, contact was made with Frank Leymann, who told Christoph Roch about the PlanQK project and a BMWi AI tender. It was already known that the chair at which Christoph Roch works has experience with D-Wave programming.
For Christoph Roch, the commitment came in handy because he deals with both research fields, QC and AI, in his doctorate, with Quantum Computing being preferred:

"I was convinced about preparing German SMEs for the new topic of Quantum Computing and identifying the possibilities and interfaces between AI and QC. There has been a recent discussion in the AI community about the extensive use of computing resources in research. Pioneering experiments that open up new applications in the field of AI require ever-increasing computing time. That is why we are currently looking for new ways to meet the increasing computing needs with new hardware. New calculation models, such as Quantum Computing, could remedy this. In my opinion, the combination of QC and AI will be inevitable in the future."

The LMU also has many years of experience in the areas of AI and QC. In addition, they had access to D-Wave's Quantum Annealer and thus already gained practical experience with the programming of QC hardware. Within the PlanQK project, the use case partners will above all be supported in the requirements analysis and implementation of Quantum-Assisted Artificial Intelligence (QKI) methods to solve or optimize their fields of application. In addition, the LMU is strongly represented in building the community. At workshops, the hurdle for QKI should be removed from the user, associated partners and generally interested companies. The aim is to build an ecosystem around the platform and to prepare SMEs for the new technologies in the long term.

"The biggest challenge for the marketability of the platform lies indirectly in the scaling and solution quality (the relatively high error rate of gate operators and the short coherence time of the qubits must be taken into account) of the QC hardware. In my opinion, however, it is only a matter of time before such sources of error can be minimized, and then it is good to have a German SME affine to QKI that benefits from the platform."

Communication between so many associated partners is not easy. The consortium is led by StoneOne, a medium-sized company from Berlin. Numerous internal meetings are scheduled for the course of the project, in which use cases and platform components are analyzed. These meetings are also used for team coordination and synchronization. In addition to these meetings, numerous events and workshops with associated partners, users and interested parties are also planned. In addition, QKI knowledge is to be transferred, the benefits of the platform explained and community building promoted.

"Will PlanQK play a special role internationally? I see more opportunities for cooperation with other similar projects. With the QC flagship initiative for quantum technologies, the EU is currently promoting developments in particular of basic technologies and quantum hardware. PlanQK can fill an important gap by offering the opportunity to also develop software and to integrate numerous possible users into a community. With the FUB and HQS, two PlanQK project partners are involved in prominent flagship projects on quantum technologies, both via superconducting quantum computers (OpenSuperQ) and programmable quantum simulators and so-called near-term devices (PASQuanS). The connection of the hardware manufactured by APIs is actively monitored by PlanQK."

Matthias Rosenkranz is involved in PlanQK as a project manager for the d-fine GmbH project. This is a European management consultancy with a focus on the implementation of analytical and technological issues. Expertise in the field of Quantum Computing is bundled in their Quantum Lab. For PlanQK, d-fine contributes the use cases in the finance and energy sector and supports the development of relevant quantum algorithms and community building.

How did you find out about the idea of PlanQK? How did the first contact come about?

The first contact was made through an appeal to participate in the PlanQK workshops of Prof. Dr. Dr. Frank Leymann. I became aware of this through contact with one of the founding partners of PlanQK, HQS Quantum Simulation. The idea of PlanQK was introduced to us during the workshop.

What was the crucial point then to join PlanQK?

What convinced us at d-fine was the idea of a cross-industry platform for testing quantum-based machine learning processes and the integration of industry and research partners. The merging of diverse experts in quantum hardware via quantum algorithms to artificial intelligence and software development is currently difficult for individual companies, and especially small ones. For us as a management consultancy, such a platform offers the opportunity to support our customers at an early stage in the development of specific Quantum Computing solutions. By participating in PlanQK, we can also exchange our expertise in Quantum Computing with other experts. We can then pass on the knowledge gained to our partners.

At the moment, several startups are also developing platforms that pursue an idea similar to PlanQK. However, compared to these providers, PlanQK offers our customers greater future security, as PlanQK is supported by a broad consortium instead of a single provider.

In your view, what is the biggest challenge that PlanQK has to overcome to make the platform marketable?

In my opinion, three factors are essential for the success of the platform on the market:

1. Ease-of-use. It is important that the "translation" of business problems into suitable algorithms on the appropriate quantum hardware is as simple as possible. This can be partly automated or with the help of the platform's experts and consultants. Part of our advisory service for users of the PlanQK platform will therefore be to explore the opportunities of quantum-based methods for the respective business case without raising unrealistic expectations, and then to develop them according to the needs of the users on the platform.

"What convinced us at d-fine was the idea of a cross-industry platform for testing quantum-based machine learning processes and the integration of industry and research partners."

2. Relevant use cases. The use cases that are made available on the platform must be tailored to the needs of the users. In the initial phase, the use cases initially provided must be convincing and should cover a broad industrial cross-section.

3. Targeted research funding. Despite the rapid advances in the commercialization of Quantum Computing, decisive research successes are still necessary for broad market viability. This applies both to the development of practical quantum algorithms that are tailored to today's quantum computers, which are still prone to errors, and to the improvement of quantum hardware. PlanQK is ideally positioned for the development of quantum algorithms thanks to the participation of leading research groups worldwide. At the same time, several manufacturers such as IBM or AQT could be won as associated partners that drive the improvement of the quantum hardware.

Who are the addressees of the community that is to be created for PlanQK? Why?

Our target companies are primarily those whose business model depends largely on the availability of high computing power or advanced computing methods. These can be companies from the energy and mobility sector, logistics, telecommunications, production or the financial sector, for example, who are increasingly using advanced optimization algorithms or machine learning methods. At the same time, these companies often do not have the necessary expertise to develop Quantum Computing solutions themselves. The PlanQK community can support this. Interesting addressees are also companies from the chemical and pharmaceutical industries as well as material development. A key problem in these sectors is the simulation of quantum systems. This problem was the original motivation for the development of quantum computers and today serves as a motivation for several quantum-based machine learning methods.

How do you go about building the community?

We maintain contacts with customers in various industrial sectors. Our customer base is characterized quantitatively and technologically and is therefore an ideal basis for community members. We are therefore planning to gain parts of these customers as users of the PlanQK platform through workshops and prototypical implementation of use cases. We also plan to broaden the idea of the platform through lectures at conferences and trade fairs.

How do you go about developing the relevant quantum algorithms? What technical know-how do you use? What are the concrete development steps?

Of course, d-fine has a not-onconsiderable head start. Of our 900 experts, 50% have a degree in physics, 40% in mathematics and 10% in computer science or equivalent. In our internal d-fine Quantum Lab, we have been following the Quantum Computing market and academic research on quantum-based machine learning and optimization algorithms for a long time. Specifically, we implement prototype-relevant quantum algorithms in the relevant programming languages of quantum hardware manufacturers such as IBM Qiskit or Rigetti Forest. In addition to the extensive know-how of our colleagues through doctorates or master's theses in the field of Quantum Computing and related topics, our colleagues are familiar with the practical challenges in the design and integration of new systems in a company infrastructure and in the establishment of related business processes from daily project business. In the PlanQK project, we therefore see our role as a link between industrial users and academic partners.

Which specific use cases do you contribute to PlanQK? Can you give examples?

German Chancellor Angela Merkel at the Digital Summit 2019 together with Prof. Frank Leymann, the scientific director of the PlanQK project (2 from right).

We contribute use cases from the finance and energy sector. The modeling of energy systems and the optimization of energy networks are playing an increasingly important role in electricity production and distribution due to the energy transition. Electricity fed into power grids is now generated by a large number of regenerative, strongly fluctuating energy sources (such as solar, wind or hydropower) as well as by non-regenerative energy sources (fossil fuels, nuclear energy). The production of each source must be controlled in such a way that the electricity demand is covered at all times, and at the same time the economy of energy production is preserved. Due to the energy and transport turnaround and the associated more fluctuating energy sources, it is to be expected that in the future more and more small producers and consumers will feed electricity into the energy grid or ask for it, such as in the form of renewable energy sources or smart charging solutions for electric cars. The optimization of these production and feed cycles requires considerable computing resources. This use case is intended to investigate how quantum-based solutions can counteract this high resource expenditure.

Do you have a schedule for all of your development steps that you design with PlanQK? How do you coordinate your tasks within your ranks?

We plan to create requirement analyses for the use cases mentioned in the first half of 2020 and then start implementing the use cases. The implementation is followed by the integration of the use cases on the platform. We also support you in the development of quantum algorithms. The pilot operation on the platform will start in 2021. The coordination within our company follows the established processes of our project work.

How do you personally see the development of quantum computers and artificial intelligence in Germany in the next few years?

Germany is well positioned on the part of potential users of Quantum Computing. For example, the local automotive industry is one of the pioneers in testing Quantum Computing in practical applications. In contrast, North American companies and research institutions are the leaders in the production of quantum computer hardware, although European quantum computer startups such as AQT or IQM and large research projects such as OpenSuperQ are working to overcome this advantage. I see very good opportunities in Germany over the next few years – especially in the development of practical quantum algorithms through the interaction between industrial users and research.

“Germany is well positioned on the part of potential users of Quantum Computing. For example, the local automotive industry is one of the pioneers in testing Quantum Computing in practical applications.”

Dr. Matthias Rosenkranz

Dr. Matthias Rosenkranz is manager at the management consultancy d-fine GmbH. His focus as head of the d-fine Quantum Lab is on applications of Quantum Computing in industry. Dr. Rosenkranz joined d-fine in 2013 after completing a PhD in quantum simulation at the University of Oxford and a research stay at the National University of Singapore. He has a diploma in physics from the Technical University of Darmstadt and a master’s in mathematical finance from the University of Oxford.

**Prof. Rudolf Gross,
spokesperson of the MCQST**

“Munich Takes the Lead In Quantum Science.”

MCQST works on a scientific connectivity between quantum physics

The newly-founded Munich Center for Quantum Science and Technology (MCQST) is a Cluster of Excellence funded by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG). With a multidisciplinary profile, ranging over disciplines like physics, mathematics, computer science, electrical engineering, material science, and chemistry, it comprises seven research units covering all areas of Quantum Science and Technology (QST) from basic research to applications.

Its main goal is to build a world-leading center in QST by addressing important scientific and technological questions, attracting renowned scientists as well as young talents to Munich through an ambitious guest program and carefully designed structural measures, and fostering the exchange between research in academia and industry. The aim is to create a unique research environment for quantum science and technology in Munich. Spokesperson Prof. Rudolf Gross reveals how this should work.

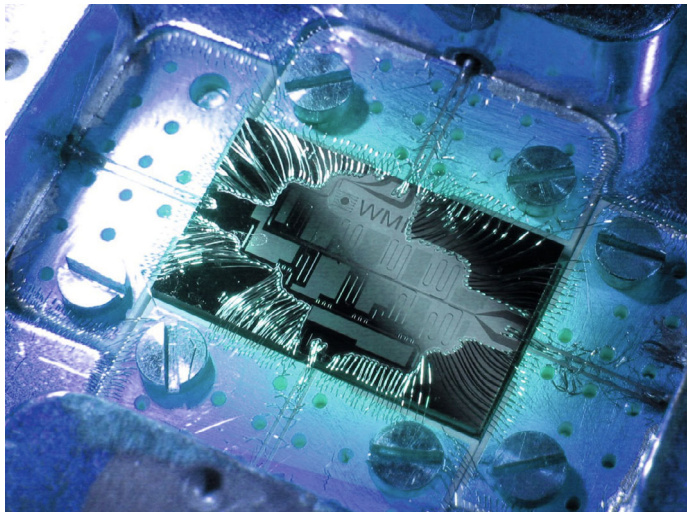
How does the history of quantum physics relate to MCQST?

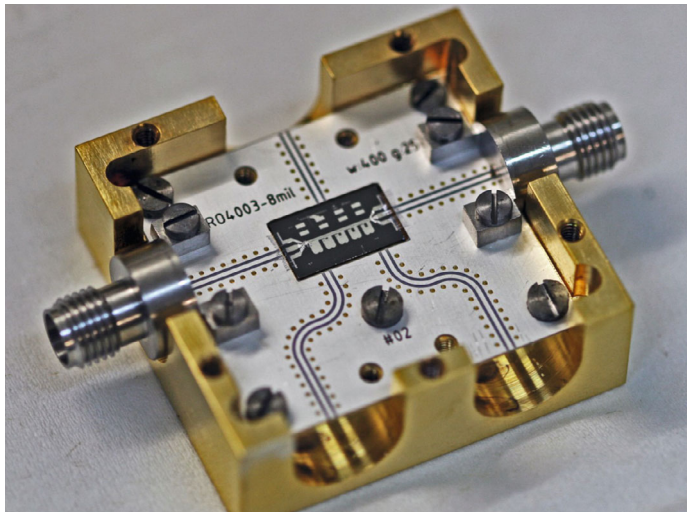
Without the history of quantum physics, of course, MCQST would not exist today. Munich has a very long tradition in quantum physics. For example, here at the Walther-Meißner-Institute, flux quantization was discovered way back in 1961. The continuous development of well-known research and technological advances then permeates the history of quantum physics to the present day. The preparatory work for MCQST then came partly from Collaborative Research Centers (Sonderforschungsbereich, SFB). The idea came in the early 2000s to establish a strong research effort on quantum physics and technology in Munich In 2003, the first Collaborative Research Center started: “Solid State-Based Quantum Information Processing”. Actually, this was the first coordinated activity on this subject in Germany at the time.

“I believe that the Nobel Prize will be awarded to quantum scientists when quantum computers show their power in practical application.”

Such Collaborative Research Centers run for a maximum of twelve years. This is why it expired in 2015. Of course, already in the course of this Collaborative Research Center, we were planning for the future. Because quantum physics has developed so greatly over the decades, especially in Munich, we decided to apply for a Cluster of Excellence within Germany’s excellence strategy. After several years of hard work we succeeded, and MCQST finally started on January 1, 2019. To prepare for the cluster application, we founded the Munich Quantum Center (MQC) in 2014 without any financial support: we basically created a website to collect and combine the quantum activities in Munich, coordinated graduate education and or-

Photo: Robert Brembeck





Superconducting quantum circuit fabricated at Walther-Meißner-Institute

ganized meetings for all quantum researchers twice a year. As a result, the research groups of the different institutions started exchanging and collaborating more and more. This has been an ideal starting point for our Cluster of Excellence.

What does MCQST look like today? How does the institution organise itself? How is the exchange of affiliated partners handled?

MCQST now has about 60 principal investigators and about 300 scientists in total. Our organizing principle is self-organization. In the research proposal we defined seven research units, and found many connections between the different topics and research groups overarching different disciplines. The cluster management fosters these collaborations. For example, we place junior researchers (postdocs) primarily at interfaces to stimulate joint efforts of different research units.

"Working with children is especially important to us. They will be the researchers of tomorrow."

As a Cluster of Excellence, we do not have to meet strict milestones at a certain point in time. Our research agenda rather follows a general vision, which we would like to implement within the next 14 years. This vision covers all important topics of quantum science and technology: quantum information theory, quantum simulation, Quantum Computing, quantum communication, quantum metrology and sensing, quantum matter as well as explorative research directions. The goal is to make Munich the most successful place in Europe in quantum physics.

How does Munich already stand in international comparison?

Very well! Although an objective comparison on an international level is a subtle problem. However, if you look at the quantitative and qualitative impact of publications, Munich, from a global point of view, is in an excellent position. For example, Ignacio Cirac is one of the most important researchers in quantum physics. His proposal of the Cirac-Zoller Controlled-NOT Gate is one of the pioneering inventions. Cirac's name is also often mentioned when colleagues discuss future Nobel Prize winners. I believe that the Nobel Prize will be awarded to quantum scientists when quantum computers show their power in practical application. Cirac is also a good example for the strength of the Munich ecosystems in promoting the career of talented young scientists.

How do you deal with the competition from Google, IBM and other industry giants?

We do not see these companies as competitors. They put so much money into the development of superconducting quantum computer that we cannot compete, even if we focus all our resources on this particular field. What we are doing here is something different. We do basic research, for example, by developing new kinds of quantum bits or gates with better performance or improved readout schemes. This is important since even the big players like Google cannot develop several technology platforms in parallel. They strongly profit from the development of alternative technological solutions in basic science. Of course, we are interested in cooperating with Google or IBM. In our cluster we presently establish a communication platform to stimulate exchange between research institutions and industry. We also hope to move people back and forth between industry and research institutions.

How is MCQST anchored with the public?

It is important for us to engage the public in quantum technology and discuss its possible impact on our everyday life in the future. We already organized a couple of events following this idea like public lectures by Hartmut Neven from Google and John Preskill from the California Institute of Technology (Caltech), both highly recognized experts in the field of Quantum Computing. Another example is our participation in the "Garchinger Gespräche" or events in grammar schools. It is fascinating to

talk to a colorful mix of professors, lay people and pupils – all listening intently to the complex topic of quantum physics. In addition, we are also engaged in the education of students and teachers. We regularly offer training courses for teachers and have our own student laboratory called PhotonLab, where high school kids can do their own experiments and experience quantum science. It is very rewarding to meet twelve-year-old kids who are fascinated by quantum physics. Working with children is especially important to us. They will be the researchers of tomorrow. It is only by investing in the next generation that we can reach the number of students and educated scientific staff that will guarantee a continuous progress in science.

A permanent exhibition is to be created in the Deutsches Museum. Can you say anything specific about this?

The Deutsches Museum is the best location to make the public aware of quantum science and technology. We are planning a permanent exhibition on this topic starting in 2025. The Deutsches Museum has set up a scientific advisory board to support this project. Nobel laureates, among other renowned scientists, are involved in this. So far, we have a basic concept and a collection of ideas, but it centers around the problem: How do you present quantum physics to the layman? Besides, we already secured historical exhibits like the first laser. Other historical pieces of equipment, which have been groundbreaking for the development of quantum physics, will be added to the collection. Perhaps we will also be able to get Google's first quantum computer?

"In our cluster we presently establish a communication platform to stimulate exchange between research institutions and industry."

From a researcher's perspective: What impact can the quantum computer have in the near future?

Recently, a Google quantum computer outperformed a classical supercomputer on a specific task, which unfortunately does not have any practical meaning. The key problem is that quantum computers are not error-free today. We are in the so-called NISQ era, with NISQ meaning "noisy intermediate scale quantum". Noisy, because the computers make errors in their gate operations – the gates have a "fidelity" of less than 100%, representing the ideal case. Although today's quantum computers reach fidelities well above 99%, this is not sufficient. If an algorithm with about 1000 gate operations has to be performed, then the error quickly becomes very large. Therefore, the NISQ era computers can solve only quite simple problems such as the simulation of small molecules. IBM, for example, is already doing this. The caffeine molecule is a popular example of this. However, potential industrial users of quantum computers are already making use of NISQ machines, although there are still no significant benefits. They speculate on rapid progress in hardware developments and work with state-of-the-art technology today in order to have a head start tomorrow, when the improved quantum computer can solve actual complex problems. Although it is always dangerous to make predictions for the future, I believe that it will take another 8 to 10 years to develop fault-tolerant quantum computers. These computers then can be scaled up as desired and the enormous power of a quantum computer will find broad applications.

Mr. Gross, what exactly connects you to the project?

I am one of the three spokespersons of the cluster and coordinate one of the seven research units, the one on Quantum Computing. Personally, I do basic research and technology developments for superconducting quantum computers. This is precisely the technology Google and IBM want to translate into products. Actually, we started our research efforts in this technology at the start of the millennium. In the beginning, individual qubits had to be manufactured, tested and optimized. Quantum states decay very quickly when they interact with the environment. Within about fifteen years, the lifetime of superconducting qubits has been improved from the nanosecond to the millisecond regime, that is, by about six orders of magnitude. This is a huge improvement and makes me optimistic regarding the realization of fault-tolerant quantum computers.

There are many basic question keeping us busy: How can we further improve quantum bits? How can we realize useful quantum memories? How can we scale up systems? How can we realize quantum communication between remote quantum processors? We are attacking these questions on the basic research level and, of course, important improvements will then be taken over by the players in industry. Research institutions and industry both work hard to make the quantum computer a reality. Accordingly, there is a great interest in keeping in touch. At the moment we are developing the world's first Quantum LAN in my lab. Like in supercomputers, where a large number of processors communicates via fiber optics, we need something equivalent for distributed Quantum Computing sooner or later. But how to realize this? Since superconducting quantum computers operate at microwave frequencies, we develop quantum communication in the microwave regime – a so-called "quantum LAN". We already implemented this on a centimeter scale and now extend the distance to several meters by connecting two superconducting processors in separate rooms. Fascinating times!

Interview: Hannes Mittermaier

Prof. Rudolf Gross

Professor Gross conducts research in the field of low-temperature solid-state physics. He is particularly interested in quantum phenomena in solid-state nanostructures and their application in quantum technology. He received his doctorate from the University of Tübingen in 1987. After postdoc stays at the Electrotechnical Laboratory in Tsukuba and IBM's T.J. Watson Research Center, he became full professor at the University of Cologne in 1995. In 2000, he became director of the Walther-Meißner-Institute of the Bavarian Academy of Sciences and Humanities, which is combined with a Chair position at TUM. He was the spokesperson of the Collaborative Research Center 631 (2003-2015), served on the executive committee of the cluster of excellence "Nanosystems Initiative Munich" (2006–2019) and is spokesperson of the cluster of excellence "Munich Center for Quantum Science and Technology" (since 2019).

Photo: WMI/MCST, Astrid Eckert

Wie Quantenalgorithmen die **Informationstechnologie revolutionieren**

Roman Uminski

Eine Herausforderung moderner Computersysteme ist es, komplexe Abläufe, wie sie in der Natur vorkommen, möglichst originalgetreu zu modellieren. Wenn man versucht, dieses Problem mit Hilfe von konventionellen Computern zu lösen, kann man die Einschränkungen der Hardware und der klassischen Algorithmen nicht überwinden. Die Hauptschwierigkeit beim Modellieren von komplexen Systemen bestehen darin, dass klassische Algorithmen und Hardware-Architekturen für korrekte Abbildung und Simulation von komplexen Naturprozessen wenig geeignet sind. Lösungsansätze mit klassischen Algorithmen sind zu eingeschränkt, funktionieren zu langsam und führen häufig zu falschen Ergebnissen.

Um Durchbruch in der Forschung und Entwicklung erneuerbarer Energien, künstlicher Intelligenz (KI), in der Molekularphysik, Quantenmechanik und Chemie zu erzielen, ist ein Paradigmenwechsel unausweichlich. Die technologischen Veränderungen betreffen nicht nur herkömmliche Computersysteme, sondern auch Algorithmen, Anwendungsprogramme, Betriebssysteme und Prozessoren für Quantencomputer.

Fortschritt von Quantentechnologien

Versucht man Quantenprozesse in einem klassischen Computer zu modellieren, steigt der Rechenaufwand mit jedem Arbeitszyklus exponentiell. Ein Quantencomputer löst eine komplexe Aufgabe in wenigen Sekunden, während ein moderner klassischer Superrechner Tausende Jahre für die Lösung desselben Problems benötigen würde. Die Prozessorleistung eines Quantencomputers ist extrem hoch, um jede komplexe Aufgabe zu bewältigen. Die ersten wissenschaftlichen Erfolge zeichneten sich, nachdem die ersten Quantencomputer realisiert wurden und praktische Anwendungen von Quantenalgorithmen möglich waren. Ein programmierbarer supraleitender Prozessor zur Erzeugung von Quantenzuständen (53 Qubits) wurde von Google entwickelt und in einem funktionsfähigen Quantencomputer „Sycamore“ verwendet.

In den letzten zwanzig Jahren haben die Quantentechnologien (QT) enorme Fortschritte erzielt und sich zu einem hochpriorisierten interdisziplinären Forschungsgebiet etabliert. Das öffentliche Interesse verlagert sich von der faszinierenden Welt der Quantenphysik immer mehr auf praktische und nützliche Quantenalgorithmen und Quantenanwendungen, deren Problemfelder bislang, ohne Quantencomputer unerschlossen waren.

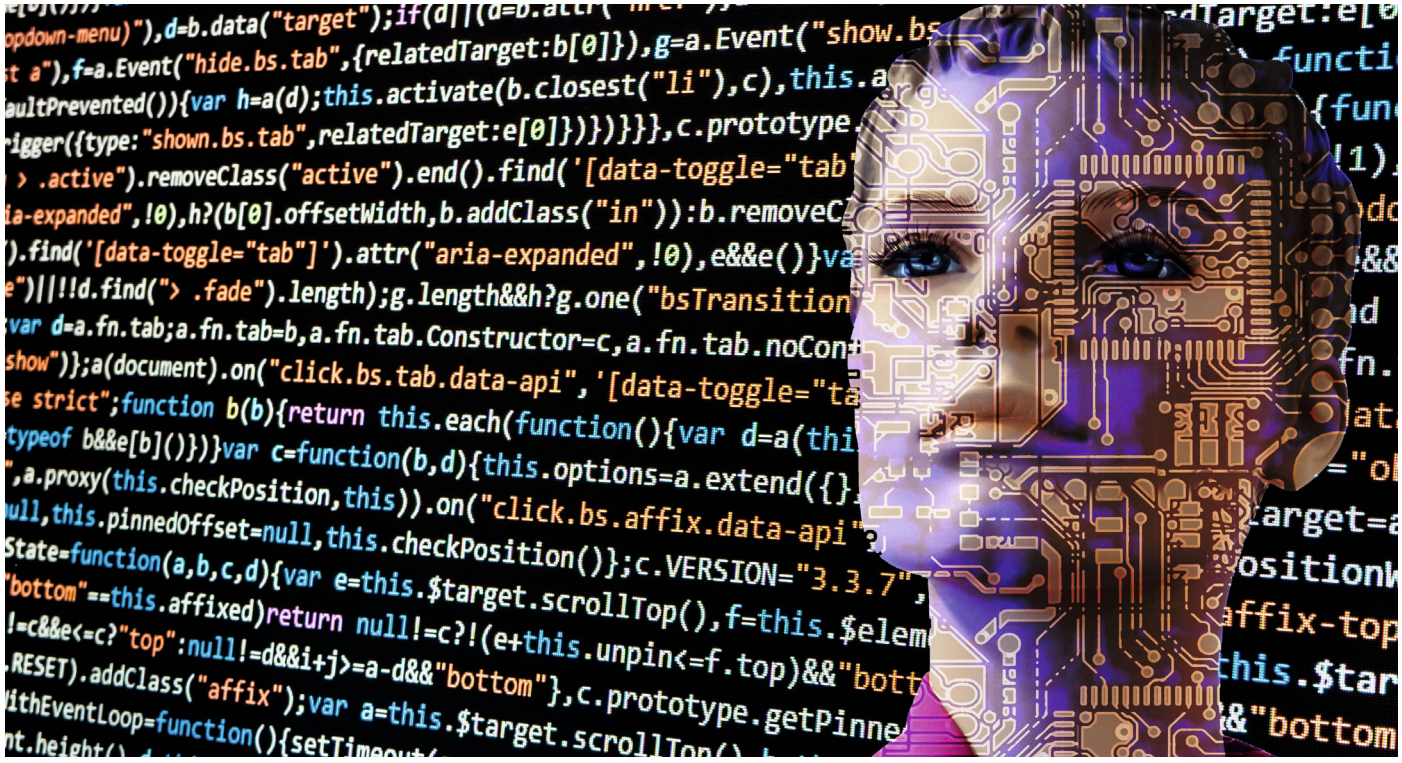
Besonderheiten von Quantenalgorithmen

Quantencomputer arbeiten auf Basis quantenmechanischer Zustände der Quantenphysik und verarbeiten diese Zustände. Auf denselben Grundprinzipien werden auch Quantenalgorithmen realisiert. Ein Quantencompiler übersetzt die Rechenoperationen in entsprechende physikalische Manipulationen der Qubits. Die Ausführung von Prozessorbefehlen unterscheidet sich für Photonen, Atome, Ionen oder Supraleiter und hängt von der im Prozessor realisierten Quantentechnologie ab.

Im Gegensatz zu herkömmlichen Computern, in denen ein Bit nur einen Wert „0“ oder „1“ annimmt, kann ein Quantenbit (Qubit, gesprochen „kju-bit“) nach den Regeln der Quantenphysik in einer Superposition gleichzeitig sowohl „0“ als auch „1“ sein. Ein Ion kann ein Qubit speichern, Qubits können sich auch in einem verschränkten Zustand befinden. Durch Superposition und Verschränkung erreicht ein Quantencomputer einen höheren Grad seiner Rechenleistung und kann Probleme lösen, die sich mit konventionellen Computern nicht bewältigen lassen.

Ein Quantenalgorithmus besteht aus einem Quantenschaltkreis und einer genauen Auswahl der zu manipulierenden und zu messenden Qubits. Quantenprozessoren werden modular aufgebaut. Jeder Einzelprozessor speichert und verarbeitet eine begrenzte Zahl von Qubits, kann aber quantenmechanisch mit anderen Prozessoren logisch zusammengeschaltet werden. Das kann durch Photonen oder mechanische Schwingungen erfolgen. Die einzelnen Prozessoren sind etwa Miniquantencomputer und lassen sich wie Computer programmieren.

Obwohl man einen Quantencomputer auch mit klassischen Algorithmen programmieren kann, bringt das jedoch keine Vorteile, weil die besonderen Eigenschaften des Quantenprozessors wie Superposition und Verschränkung ungenutzt bleiben. Algorithmen für Quantencomputer sollten komplett neu entwickelt werden und die Besonderheiten der Quantenarchitektur berücksichtigen, damit diese Algorithmen effizient funktionieren.



Bekannte Klassen von Quantenalgorithmen
Abhängig von den verwendeten Methoden werden bekannte Quantenalgorithmen in die folgenden vier Gruppen eingeteilt:

1. Algorithmen, die eine globale Eigenschaft aller Funktionswerte einer Funktion bestimmen (Deutsch-Jozsa-Algorithmus, Shor-Algorithmus zur Faktorisierung großer Zahlen u.a.)
2. Algorithmen, die durch Transformation des Status der Qubits die Wahrscheinlichkeit erhöhen, dass das Ergebnis gemessen werden kann (Quanten-Suchalgorithmen wie Grover-Suchalgorithmus, z.B. für BigData-Datenbanken)
3. Algorithmen für Quanten-Simulation (Quantenphysik, Quantenchemie, Photosynthese, Quantenverhalten von lebenden Organismen)
4. Algorithmen, die Methoden aus den ersten drei Gruppen kombinieren (z.B. „Approximate Counting Algorithm“ von Brassard-Hoyer-Tapp)

Vorteile von Quantenalgorithmen auf Quantencomputern
Es gibt Problemklassen, die mit Quantenalgorithmen auf Quantencomputern effizienter gelöst werden als mit herkömmlichen Algorithmen auf modernen klassischen Rechnern. Rechenaufgaben werden in einem Quantenprozessor exponentiell schneller ausgeführt als in einem klassischen superschnellen Prozessor. Der dramatische Geschwindigkeitszuwachs im Vergleich zu allen bekannten Algorithmen ermöglicht auch besonders komplexe Probleme mit Quantenalgorithmen zu lösen, die bisher als hoffnungslos und unlösbar galten.

Quantenalgorithmen nutzen die Eigenschaften der Superposition und die Möglichkeit der Überlagerung von Qubits. Das ermöglicht eine native Parallelität der Rechenprozesse. Die Quantenparallelität ist eine wichtige Eigenschaft eines Quantenprozessors. Erst mit Quantenalgorithmen können die auf Qubits basierten Daten effizient bearbeitet (ausgelesen, gespeichert und manipuliert) werden. Dafür sind Quantenalgorithmen für die Zusammenarbeit mit Quantenprozessoren am besten geeignet. Quantenalgorithmen sind klassischen bit-orientierten Algorithmen weit überlegen, weil nur Quantenalgorithmen die spezifischen Eigenschaften eines Quantencomputers optimal nutzen können.

Konventionelle Computer können zur Verifizierung von Quantenalgorithmen und als Referenzsysteme zur Validierung der Ergebnisse verwendet werden. Die Quantenprozessoren werden weiterentwickelt, so dass sie noch leistungsfähiger werden und stabile Ergebnisse liefern können.

Probleme von Quantencomputern
Derzeit gibt es nur Laborprototypen mit begrenzter Leistung, jedoch keine Quantencomputer auf dem Markt. Man versucht Quantenalgorithmen mit Quantencomputing-Simulatoren auf herkömmlichen Rechnern zu entwickeln und zu testen, bevor diese auf einem echten Quantencomputer laufen zu lassen. Ansätze mit hybriden Computern – einem Quantencomputer und einem oder mehreren konventionellen Computern bzw. Supercomputern in einem gemeinsamen System – sind auch populär und ermöglichen, viele aktuelle Probleme und Schwachstellen von Quantencomputern zu umgehen.

Enorme Datenmengen erfordern auch eine extrem große Speicherkapazität. Aktuell gibt es nicht genügend Direktzugriffsspeicher (RAM), um alle Quantenzustände und Zwischenergebnisse operativ zu speichern. Deshalb wird nach neuen Speichertechnologien für Quantencomputer intensiv geforscht.

Effektive Quantenfehlerkorrektur
Fehlerbehaftete Ergebnisse und eine relativ hohe Fehlerrate beim Auslesen und Manipulieren von Qubits sind zwei

kritische Probleme, die den Fortschritt von Quantencomputern ausbremsen. Um die Fehlerkorrektur zu verbessern, sind fehlertolerante logische Qubits erforderlich, die verlässliche und korrekte Ergebnisse nach Ausführung eines Quantenalgorithmus liefern. Das Engineering der Quantenfehlerkorrektur wird deshalb in den Mittelpunkt der Aufmerksamkeit der Wissenschaftler gerückt.

Quantenalgorithmen basieren auf den grundlegenden Eigenschaften eines Quantencomputers und können Ergebnisse nur mit einer gewissen Genauigkeit erzeugen. Man spricht von einem probabilistischen Algorithmus, der sich von einem deterministischen Algorithmus eines klassischen Computers prinzipiell unterscheidet.

Mit Quantencomputern kann man das Ergebnis mit einer hohen Messwahrscheinlichkeit erlangen, die Fehlerwahrscheinlichkeit liegt aber nicht bei Null. Durch wiederholtes, zyklisches Ausführen und Iterationen des Quantenalgorithmus wird die Fehlerwahrscheinlichkeit effektiv reduziert. Auch wenn die anfängliche Fehlerrate groß genug ist, reichen nur wenige Sekunden andauernde Wiederholungen aus, um ein verlässliches und akzeptables Ergebnis zu erreichen, in dem die Fehlerquote unter dem festgelegten Grenzwert liegt.

Die charakteristische Eigenschaft von Quantenalgorithmen ist es, dass solche Algorithmen:

A. parallele Datenverarbeitung nativ unterstützen;
B. Fehler in Ergebnissen des Quantencomputers berücksichtigen;
C. ein fehlerbehaftetes Ergebnis durch viele Wiederholungen/Iterationszyklen effektiv und in akzeptabler Zeit korrigieren können.

Quantentechnologien und Quantenalgorithmen

Quantentechnologien (QT) im Bereich Computing, Prozessoren und Algorithmen stecken noch in den Kinderschuhen, haben aber ein enormes Entwicklungspotential. Sie werden rasant von den führenden Industrieländern (wie Deutschland), IT-Konzernen (Google, IBM u.a.) und internationalen Forschungszentren (Jülich Supercomputing Centre u.a.) weiterentwickelt. Quantencomputer erschließen einen vielversprechenden innovativen Weg zu neuen Anwendungstechnologien und basieren selbst auf neuen Quantentechnologien.

Man braucht unterschiedliche Werkzeuge und Maschinen, um Aufgaben beliebiger Komplexität effizient lösen zu können. Genauso braucht man auch leistungsunterschiedliche Computer – sowohl klassische Rechner wie PCs, spezielle Server und Mainframes als auch Supercomputer und Quantencomputer. Spezielle für Quantencomputer zugeschnittene neue Programmiersprachen sind erforderlich, um das enorme Rechenpotential der neuen Computer vollständig ausnutzen zu können.

Quantencomputer vs. klassische Computer

Jede Computerklasse hat seine Vorteile und Nachteile. Der Hauptvorteil eines Quantencomputers gegenüber einem klassischen Computer ist seine extrem hohe Rechenleistung (dank supraleitenden Qubit-Prozessoren) und die Fähigkeit Quantenalgorithmen auszuführen, die man bisher mit klassischen Rechnern oder Superrechnern nicht bewältigen konnte.

Auf Quantenalgorithmen basierte Anwendungen für neue Energien, Chemie, Materialwissenschaften, Genomforschung, Biotechnologien, KI und Optimierung sind von großer praktischer Bedeutung und haben die besten Chancen, die Innovation in diesen zukunftsorientierten Technologien erfolgreich voranzutreiben. Auch der Quantencomputer selbst wechselt die Rolle – von einem akademischen Forschungsthema zu einer realen innovativen Technologie.

Fazit

In absehbarer Zukunft werden Quantencomputer klassische Computer nicht verdrängen und nicht ersetzen, sondern werden diese ergänzen. Genauso wie Supercomputer einen herkömmlichen PC nicht ablösen können, werden auch Quantencomputer und Quantenalgorithmen für spezielle komplexe Anwendungs- und Forschungsaufgaben eingesetzt. Nachdem Quantencomputer ihre Kinderkrankheiten und Schwächen überwinden und den Markt erobern, erzeugen Quantenalgorithmen den erwarteten wirtschaftlichen und technologischen Durchbruch, revolutionieren die Industrie und lösen die schwierigsten komplexen Probleme, die bisher auch moderne Supercomputer nicht lösen konnten.

Ein Programmierer von Quantenalgorithmen soll sich auf das eigentliche Problem konzentrieren und sich nicht unbedingt mit den Gesetzen der Quantenmechanik auseinandersetzen. In Informationstechnologien und deren Weiterentwicklung spielt die Quantenphysik eine wichtige, jedoch untergeordnete Rolle. Trotz des quantenphysikalischen Hypes in Medien bleibt der Quantencomputer nur ein notwendiges technologisches Werkzeug zur Lösung von besonders komplexen Problemen. Eine enorme Komplexität eines Quantenprozessors ist nur ein aktuelles technologisches Merkmal, jedoch kein Selbstzweck der IT-Technologie.

Um innovative Anwendungen schnell und effizient entwickeln zu können, müssen Quantenprogrammierer die Komplexität der Quantenwelt überwinden. Es ist zu erwarten, dass Quantencomputer in Zukunft nicht nur zuverlässiger, schneller, effizienter und leistungsstärker werden, sondern auch einfach zu handhaben und zu bedienen sind wie herkömmliche PCs. Erst dann können „Quantenprogrammierer“ – d.h. Programmierer von Quantenalgorithmen für Quantencomputer – ihre Kreativität entfalten, sich auf eigentlichen Anwendungsproblemen konzentrieren und qualitative einsatzfähige Quantenanwendungen entwickeln, die die Vorteile von Quantentechnologien ausgiebig und effizient nutzen.

Roman Uminski

Roman Uminski unterstützt seit 2017 das international tätige digitale Verbrauchermagazin Kaufbater.io als Key Account Manager und SEO-Spezialist. Durch seine langjährige Erfahrung ist er der erste Ansprechpartner für die digitalen Kooperationen im deutschsprachigen Raum.

Foto: geralt / Pixabay.com, Privat

Welche Auswirkungen hat das Quantum Computing auf die **Informationssicherheit?**

Roman Uminski

Quantencomputer werden unsere Welt in nicht allzu ferner Zukunft revolutionieren. Obwohl vor der alltäglichen Anwendung noch zahlreiche Stolpersteine entfernt werden müssen, bedeuten diese neuartigen Computer einen großen Schritt für die Technologie und unsere Gesellschaft. Das betrifft besonders die Bereiche Kryptografie und Cybersicherheit. Die neuen Techniken des Quantencomputers können die kryptografische Welt auf den Kopf stellen und schwerwiegende Auswirkungen auf die Informationssicherheit und die Welt insgesamt haben.

Was können Quantencomputer?
Im Wesentlichen nutzen Quantencomputer die Eigenschaften der Quantenmechanik, um Berechnungen durchzuführen. Dies steht im Gegensatz zu den herkömmlichen (digitalen) Computern, die den Eigenschaften der klassischen Physik entsprechen.

Quantencomputer stützen sich auf Informationseinheiten, die als Qubits bekannt sind. Diese können in Zuständen von Null und Eins sowie Überlagerungen von Null und Eins existieren. Im Vergleich dazu verwenden klassische Computer nur Einsen und Nullen, um Informationen zu speichern.

Da Quantencomputer nach völlig anderen Prinzipien arbeiten als die Computer, die wir in unserem täglichen Leben verwenden, verfügen sie auch über andere Fähigkeiten. Viele Experten erwarten, dass sie in der Lage sein werden, Dinge zu berechnen und mathematische Probleme zu lösen, die klassische Computer heute nicht können. Fachleute bezeichnen diese Errungenschaft als Quantenüberlegenheit, obwohl sie bisher noch nicht erreicht wurde.

Einige der möglichen Anwendungen des Quantencomputers umfassen:
- Ausführen komplexerer KI-Programme
- Fortgeschrittene Berechnungen in der Physik
- Berechnung und Modellierung von komplexen Finanz-Modellen und eigenständig optimierte Investmentportfolios durch einen Robo Advisor
- Modellierung diffiziler chemischer Reaktionen, die zu Innovationen und Fortschritten in der Chemie führen können.
- Genaue Berechnung und Vorhersage von Wetter- und Klimaschwankungen
- Entschlüsseln derzeit sichere kryptografische Algorithmen sowie Einführung neuer Kryptosysteme

Quantencomputer existieren bereits, momentan sind es aber sehr schwache und instabile Maschinen, die für ernsthafte Berechnungen nicht infrage kommen. Zu den führenden Unternehmen zählen Google, Intel, IBM und D-Wave.

IBM testet derzeit einen 53-Qubit Quantencomputer, während Google an einen 72-Qubit-Computer arbeitet. Trotz dieser Bemühungen gibt es für Quantencomputer derzeit nicht viele praktische Anwendungen. Das wird sich erst ändern, wenn die Wissenschaftler die Quanten-Dekohärenz (Wechselwirkung und Verlust von Informationen an die Umgebung) verringern und die Anzahl der Qubits signifikant erhöhen können. Nach Meinung vieler Experten wird es noch mindestens zehn Jahre dauern, bis dieser neue Computer-Typ kommerziell einsetzbar ist. Manche Wissenschaftler halten fünfzehn Jahre für realistischer.

Quantencomputer und Kryptografie mit öffentlichen Schlüsseln
Bei der Kryptografie mit öffentlichen Schlüsseln werden separate Schlüssel für die Ver- und Entschlüsselung verwendet, von denen einer öffentlich und einer privat ist. Diese kryptografischen Systeme sind ein wesentlicher Bestandteil vieler Datenschutz-Mechanismen, die die Sicherheit unserer Online-Welt gewährleisten.

Die Kryptografie mit öffentlichem Schlüssel wird verwendet für:
Authentifizierung und Autorisierung eines anderen Teilnehmers an einer Verbindung
Die Verschlüsselung mit öffentlichem Schlüssel wird im Allgemeinen mit digitalen Zertifikaten kombiniert, um zu überprüfen, ob der andere Teilnehmer an einer Verbindung derjenige ist, für den er sich ausgibt, und kein Betrüger.
Gemeinsame Schlüssel entwickeln
Diese können zum Sichern der Daten in einer Verbindung verwendet werden.
Digitale Signaturen
Diese werden verwendet, um andere Parteien zu autorisieren, die Integrität von Daten zu überprüfen und die Qualität der Nicht-Ablehnung zu gewährleisten.
Verschlüsselung
In der Praxis wird die Verschlüsselung mit öffentlichen Schlüsseln nicht zum Verschlüsseln der meisten Daten verwendet. Stattdessen wird ein symmetrischer Schlüssel verschlüsselt, der die Daten effizienter verschlüsselt.

Die oben genannten Aspekte sind von entscheidender Bedeutung für viele Tätigkeiten, vom normalen Surfen im Internet bis zur Überweisung großer Geldsummen. Quantencomputer wären in der Lage, die allgemein verwendeten Verschlüsselungssysteme mit öffentlichem Schlüssel wie RSA, den Diffie-Hellman-Schlüsselaustausch und deren Varianten vollständig zu entschlüsseln.

Warum sind Quantencomputer eine Bedrohung für die Cybersicherheit?

Zu den einzigartigen Eigenschaften von Quantencomputern gehört es, Berechnungen durchzuführen, die derzeit mit klassischen Computern unmöglich sind. Dies könnte erhebliche Auswirkungen auf die Cybersicherheitslandschaft haben. Wesentliche Teile unserer digitalen Sicherheit basieren auf kryptografischen Berechnungen, die in eine Richtung einfach, in umgekehrter Richtung jedoch fast unmöglich durchzuführen sind. Selbst gängige Verschlüsselungsalgorithmen, mit denen wir heute Daten sichern, können ohne viel Zeit und Rechenaufwand nicht brutal erzwungen werden.

Dies ist mit einer Einschränkung verbunden: Diese Berechnungen können mit der aktuellen Technologie und den aktuellen Techniken nicht rückgängig gemacht werden. Quantencomputer sind eine neue Art Computer, die mit einer Vielzahl unterschiedlicher Technologien einhergehen. Einige davon sind bereits dafür bekannt, verschiedene Kryptosysteme zu entschlüsseln, auf die wir uns verlassen, um unsere tägliche Kommunikation sicher zu halten.

Wenn Quantencomputer in die Hände von Angreifern gelangen, können sie theoretisch Systeme aufbrechen, die als sicher gegen klassische Computerangriffe gelten, und so den Angreifern den Zugriff auf Daten ermöglichen, die zuvor sicher waren.

Gegenwärtig stellen Quantencomputer die größte Bedrohung für unsere am häufigsten verwendeten Public-Key-Verschlüsselungsverfahren dar. Einige Algorithmen mit symmetrischen Schlüsseln sind ebenfalls betroffen, jedoch nicht in gleichem Maße.

Natürlich steckt die Entwicklung des Quantencomputers immer noch voller Überraschungen, sodass es nicht ausgeschlossen ist, dass in einem bestimmten Stadium andere wichtige Schwachstellen in verschiedenen kryptographischen Systemen gefunden werden.

Quantencomputer: Mehr als nur eine Sicherheitsbedrohung

Quantencomputer sind eine Bedrohung, wenn es um Internetsicherheit und Kryptographie geht. Trotz der Gefahren, die Quantencomputer auf diesem Gebiet mit sich bringen kann, könnte es auch Vorteile geben.

Die einzigartigen Eigenschaften der Quantenmechanik eröffnen eine Welt neuer Möglichkeiten, wenn es um sichere Kommunikation geht. Mögliche Anwendungen sind die Quantenverschlüsselung und digitale Quantensignaturen. Einige davon, wie die Quantenschlüsselverteilung, werden bereits verwendet.

Die Quantenschlüsselverteilung ist mit jedem anderen Schlüsselaustauschprotokoll vergleichbar. Damit können zwei Parteien sicher einen symmetrischen Schlüssel einrichten, mit dem sie ihre zukünftige Kommunikation verschlüsseln können. Der Hauptunterschied besteht darin, dass die einzigartigen Eigenschaften der Quantenmechanik genutzt werden, sodass die beiden Parteien erkennen können, ob ein Angreifer die Nachrichten abhört.

Möglich wird dies durch eines der Grundprinzipien der Quantenmechanik: Jeder Versuch, ein Quantensystem zu messen, wird es verändern. Da das Abfangen von Daten im Wesentlichen eine Form der Messung ist, erkennt ein Quantenschlüsselverteilungsschema alle Anomalien, die von einem abhörenden Angreifer stammen, und bricht die Verbindung ab.

Wenn das System kein Abhören erkennt, wird die Verbindung hergestellt. Die Teilnehmer können dann sicher sein, dass der von ihnen entwickelte Schlüssel sicher ist, solange eine angemessene Authentifizierung stattgefunden hat.

Die Verteilung von Quantenschlüsseln wird derzeit in bestimmten Situationen verwendet, in denen ein hohes Sicherheitsbedürfnis besteht, zum Beispiel bei Bankgeschäften und Abstimmungen. Es ist immer noch relativ teuer und kann nicht über große Entfernungen verwendet werden, was eine weite Verbreitung bisher verhindert hat.

Quantencomputer bedrohen außerdem unsere häufig verwendeten digitalen Signatur-Schemata. Diese basieren auf Public-Key-Chiffren, die für bestimmte Entschlüsselungs-Algorithmen anfällig sind. Die neue Technologie öffnet aber auch die Tür für digitale Quantensignaturen, die diesen Angriffen widerstehen würden.

Quanten-Digitalsignaturen funktionieren genauso wie normale Digitalsignaturen und können Daten authentifizieren, ihre Integrität überprüfen und nicht widerlegen. Der Unterschied besteht darin, dass sie sich auf die Eigenschaften der Quantenmechanik stützen und nicht auf mathematische Probleme, die sich nur schwer umkehren lassen.

Quantencomputer und Informationssicherheit – Müssen wir uns Sorgen machen?

In der Praxis arbeitende Quantencomputer sind noch in weiter Ferne und es gibt eine Menge, die noch zu lösen sind. Zurzeit stehen die Wissenschaftler vor großen Herausforderungen. Aktuelle Maschinen sind nicht leistungsfähig genug und die Probleme im Zusammenhang mit der Quanten-Dekohärenz (siehe oben) müssen gelöst werden.

Obwohl unsere aktuellen kryptographischen Systeme derzeit sicher zu sein scheinen, besteht immer noch das Risiko, dass neue Algorithmen, Techniken und Angriffe entdeckt werden. Wenn die Quantencomputer marktreif sind, können diese Risiken weitaus größer sein als erwartet.

Auch wenn ein Quantencomputer noch Jahre entfernt ist, könnte ein Worst-Case-Szenario dazu führen, dass diese Computer in die Hände von Angreifern fallen, bevor die geeigneten Abwehrmechanismen vorhanden sind. Dies wäre für alle unsere digitalen Kommunikationen katastrophal. Deshalb sollten wir jetzt mit Vorsichtsmaßnahmen beginnen. Solange wir unseren derzeitigen Weg fortsetzen und keine plötzlichen Überraschungen auftauchen, sollte das mögliche Eintreffen des praktischen Quantencomputers keine größeren Störungen oder Umwälzungen verursachen.

Künstliche Intelligenz und Quantencomputing: Eine natürliche Trendwende?

Quantencomputing ist neben künstlicher Intelligenz (KI) ein weiterer Technologiefortschritt, der einst unmöglich schien, aber heute bereits Teil unserer Realität ist. Viele Menschen begegnen diesen Technologien mit Skepsis oder gar Vorurteilen, was nicht selten an einem Mangel an Informationen liegt. Infolgedessen werden diese Technologien oft als unnatürlich und unheimlich wahrgenommen und stoßen auf Ablehnung. Aber die nächste Welle der digitalen Transformation sollte nicht als feindliche Übernahme durch futuristische Konzepte wahrgenommen werden.

Quantencomputer funktionieren nach den Gesetzen der Physik, indem sie sich Quantenobjekte zunutze machen, die in der natürlichen Welt allem aktiv sind. Daher zerstören Quantencomputer nicht die Art und Weise, wie wir die Welt um uns herum berechnen und baut sie neu auf, sondern sie ermöglichen es uns, die physikalischen Gesetze als Modell für die Datenverarbeitung zu nutzen. Folglich vergrößert sich durch Quantencomputing nicht die Distanz von der digitalen zur physischen Welt, sondern wir entwickeln Geräte, die dabei helfen, die beiden Welten in Einklang zu bringen.

Mit Quantencomputern können Berechnungen in Sekunden verarbeitet werden, die einen klassischen Computer mehrere Hunderte Jahre beanspruchen würden. Höhere Rechenleistung ist hierbei natürlich eine messbare Bereicherung, aber sie ist bei weitem nicht die revolutionärste Eigenschaft des Quantencomputings. Die Revolution liegt vielmehr darin, dass wir durch Quantencomputing die Gesetze der Physik auf die digitale Welt anwenden können und diese so ebenso vielfältig wie das Leben selbst werden kann.

Das binäre Spiel

Da das Leben unser Vergleichsmaßstab ist, wollen wir die Art des Lebens vergleichen, die uns am vertrautesten ist. Als Mensch ist es überraschend schwer, eine Frage mit einem einfachen Ja oder Nein zu beantworten. Oft suchen wir nach einem Vielleicht, das unserer Antwort einen Kontext gibt. Würdest du den letzten Keks vom Teller nehmen? Ja, aber nur, wenn ich die einzige Person im Raum wäre. Dies ist ein vereinfachtes Beispiel für die Komplexität von Entscheidungen, aber eines, das noch kein zufriedenstellendes Modell bietet. Es gibt einfach zu viele Möglichkeiten, um sie alle zu berücksichtigen, wodurch wir niemals zu dem sagenumwobenen „rationalen Wesen“ werden, das wir gerne wären.

Klassische Computer arbeiten binär, was bedeutet, dass sie Informationen als Ja oder Nein beziehungsweise als Nullen und Einsen verarbeiten. Da wundert es nicht, dass klassische Computer nur mangelhaft Szenarien im Voraus berechnen können. Eine starre Antwort wie Ja oder Nein, An oder Aus, 1 oder 0 ist zu endgültig, um Raum für die Varianz und Zufälligkeit zu lassen, durch welche sich die physikalische Welt auszeichnet.

Ja, Nein, Vielleicht

Quantencomputer haben die Fähigkeit, Vielleicht zu sagen. Auch hier vereinfachen wir der Anschaulichkeit halber wieder. Ein Qubit hat eine gewissen Wahrscheinlichkeit 0 oder 1 zu sein. Diese sogenannte Superposition der Qubits kann zwei der unendlichen Abstufungen zwischen 1 und 0 gleichzeitig annehmen und wird erst offenbart, wenn sie gemessen wird. Den Implikationen hieraus widmen wir uns später genauer. Für den jetzigen Moment stellen wir uns lediglich vor, wie viel mehr es dem echten Leben entspricht, die Unsicherheit zu akzeptieren, bis ein Ereignis eintritt. Das Ergebnis könnte dieses oder jenes sein, 0 oder 1, aber wir wissen es erst, wenn es passiert.

Quantencomputing bringt uns an eine neue Grenze. Bis vor wenigen Monaten war die höchste Rechenleistung ein Digital Native, geboren und aufgewachsen in einer Zeit, in der das binäre Modell regierte. Es fußt auf anderen Prinzipien als die natürliche Welt, was einige Vorteil mit sich bringt, aber eine grundlegende Trennung von physikalischer und digitaler Welt voraussetzt. Jetzt, da erste Quantencomputer öffentlichkeitswirksamen Tests unterzogen werden, übertreten wir eine neue Schwelle: Quantencomputer, die physikalischen Gesetzen unterworfen sind.

Das Spiel der Natur

Es gibt weitere Eigenschaften von Quantencomputern, die an dieselben Gesetze gebunden sind wie die Quantenphysik und somit an die Gesetze der Naturwissenschaft. Die sogenannte Verschränkung (engl. Entanglement) ist eines davon. Verschränkung beschreibt das Phänomen, dass Qubits immer in Kombination verarbeitet werden und nicht unabhängig voneinander beschrieben werden können. Ihre Kräfte wirken so stark auf einander ein, dass die Entfernung keinen Effekt darauf hat. Forscher arbeiten immer noch an einem besseren

Annie Bailey, Analyst, KuppingerCole Analysts AG

Verständnis des mysteriösen Phänomens der Verschränkung.

Aber sinnbildliche Verschränkung betrifft auch uns als Menschen: Unsere Interaktionen benötigen Kontext, bevor so tun können, als würden Situationen in ihrer Gänze verstehen. Wie fühlst du dich heute? Besser als gestern. Ein Bezugspunkt ist immer direkt mit unseren Messungen oder Vergleichen verbunden, und zwar unabhängig von Zeit oder Entfernung. Die Kraft einer Kindheitserinnerung kann uns heute noch genauso stark beeinflussen, wie vor 20 Jahren, oder ein Wort kann eine komplett andere Konnotation haben als in dem Kontext, in dem es benutzt wurde. In der Natur beobachten wir das Prinzip von Ursache und Wirkung aber im Quantencomputing kann dieses Konzept in seiner komplexesten Ausprägung genutzt werden, um zu verstehen, wie Quantenobjekte sich gegenseitig beeinflussen.

Viele Forschungsgruppen haben auf erstaunliche Weise dazu beigetragen, die Gesetze der Natur im Sinne der Rechenleistung zu nutzen. In den vergangenen Monaten haben wir die Enthüllung erster Quantencomputer beobachten können und dürfen auf die darauffolgende Entwicklung und Verbesserung gespannt sein. Noch nie zu vor waren wir so nah dran, Rechner zu besitzen, die auf Basis der Naturgesetze funktionieren und diese nicht bloß nachahmen. Aber was ist mit dieser anderen Technologie, die den Naturgesetzen folgen sollte?

Was ist mit künstlicher Intelligenz?

Seit ihrer Gründung war das Ziel der künstlichen Intelligenz (KI) die Schaffung einer digitalen oder robotischen Kraft, die mit einer ihr innewohnenden Intelligenz agiert. Aber die KI ist seit ihrer Gründung „engen“ Funktionsmustern unterworfen. Diese Muster ermöglichen es KI-basierten Tools nur, die menschliche Logik nachzuahmen, anstatt von Natur aus auf eine menschliche Art der Datenverarbeitung zuzugreifen. KI-Tools verbessern sich zwar, aber sie sind in einer Schleife gefangen, innerhalb derer sie die Nachahmung eines Algorithmus zur Intelligenz verbessern. Trotz zunehmender Investitionen und Forschung sind KI-Instrumente nach wie vor nicht in der Lage, intuitiv, intelligent und wirklich unabhängig zu handeln, und so bedeutende Fortschritte auf dem Weg zur Artificial General Intelligence (AGI) zu machen.

Die sogenannte Narrow AI entwickelt sich nicht hin zu einer AGI, weil sie nicht nach den Gesetzen der Natur, sondern denen der digitalen Welt programmiert ist. Mit dieser grundlegenden Einschränkung wird kein AI-Tool jemals den Konstruktionsfehler überwinden, künstlich zu sein. Trotz der erstaunlichen Fortschritte, die Forscher im Bereich der KI erwirken konnten, imitieren KI-Anwendungen lediglich die Eigenschaften menschlicher Intelligenz, sind aber nicht durch eine solche gesteuert. Auch wenn Quantencomputing noch im Anfangsstadium ist, birgt es das Potenzial, künstlicher Intelligenz den Sprung von Narrow zu AGI zu ermöglichen. Indem wir Algorithmen auf einer Maschine ausführen und trainieren, die nicht grundlegend künstlich ist, können wir vielleicht mehr Aspekte der natürlichen Welt in die von uns entwickelten KI-Akteure integrieren. Ein Teil des Wettlaufs um die Entwicklung von Quantencomputern wird die Entwicklung komplementärer Lösungen für Quantencomputer, maschinelles Lernen und andere Optimierungsanwendungen sein.

Was Quantencomputing für KI tun kann

Quantenbetriebene neuronale Netze sind vielleicht der stärkste Anwendungsfall, um die Lücke zwischen Narrow und AGI zu schließen, indem man die natürlichen physikalischen Eigenschaften nutzt. Quantenneuronale Netze nutzen Quantenzustände sowohl im Eingang als auch im Ausgang einzelner Neuronen, wobei ein Qubit wie ein Neuron wirkt. Die frühen Phasen solcher Untersuchungen haben zu Ergebnissen geführt, wie

- der Definition von Ähnlichkeiten zwischen quantenneuronalen Netzen und der Schwerkraft als negativer interaktiver Energie.[1]
- der Definition des Potenzials, die Renormierung in faltungsneuronalen Netzen für eine kompakte Quantenschaltung zu nutzen.[2]
- eine direkte Übertragung klassischer Bildklassifikationsaufgaben an Quantencomputer übertragen werden könnte.[3]

Die Schaffung einer künstlichen allgemeinen Intelligenz auf der Basis natürlicher Prinzipien kann anders aussehen, als wir es erwarten. Menschliche „Schöpfer“ oder Entwickler werden den AGI-Tools womöglich Fähigkeiten einverleiben, die unseren ähneln. Aber diese Denkweise beschränkt die Werkzeuge, die wir entwickeln, darauf, dass sie in menschlicher Gestalt geschaffen werden. Quantencomputing könnte maschinelle Lerntechniken von der menschlichen Aufsicht und Einschränkung befreien, um unbeaufsichtigte Lerntechniken zu verbessern.

Was KI und Weizen gemeinsam haben

Ein faszinierendes Experiment mit klassischen Computern und Narrow-KI-Algorithmen führte zu einem überraschend natürlichen Ergebnis: Als ein simulierter Roboter damit beauftragt wurde, die schnellste Art und Weise zu lernen, eine definierte kurze Strecke zu überwinden, wurde er einfach sehr groß und fiel dann um. So erfüllte er seine Aufgabe nicht durch Gehen, Springen, Rollen oder Fliegen – vielleicht das, woran Menschen denken würden – sondern durch etwas scheinbar Unbrauchbares. Die Forscher waren amüsiert, aber verblüfft, bis ein Biologe Wind von den Versuchen bekam und ein faszinierendes Feedback gab: Dass sich der simulierte Roboter genauso verhielt wie Weizen zur Vermehrung, perfektioniert über Jahrtausende hinweg. Der Zugang zu diesen nicht-menschlichen, aber natürlichen Lösungen ist ein Aspekt, den Quantencomputer verbessern könnten, außer dass Quantencomputer nicht nach der Biologie funktionieren, sondern nach den Wechselwirkungen von Quantenobjekten.

Die Simulation von Naturphänomenen hat mit Quantencomputern ein enormes Potenzial, insbesondere was chemische Strukturen und Moleküle betrifft. Die physikalischen Eigenschaften der Moleküle machen sie für klassische Computer unpraktisch, z.B. die Tendenz eines einzelnen Elektrons, sich durch Überlagerung in mehrere Richtungen zu drehen. Dies bietet massive Vorteile für die Quantenchemie, den Gesundheitssektor, die Pharmazie sowie die landwirtschaftliche und geologische Forschung. Bereits jetzt kommen neue Geschäftsmodelle auf den Markt, die individuelle Gesundheitslösungen auf der Grundlage des Genoms und der Phänomene eines Patienten anbieten, die in ein 2-Qubit-System eingegeben wurden, um maßgeschneiderte Behandlungen zu entwickeln.

Der Sprung zur künstlichen allgemeinen Intelligenz

Das sogenannte Quantenglühen und universelles Gate-Quantencomputing sind ergänzende Werkzeuge für Narrow KI, schaffen aber auch die Voraussetzungen für die Überarbeitung von Kernstrukturen von KI-Algorithmen, um die Transformation in AGI zu ermöglichen. Das Glühen nutzt die wachsenden Fähigkeiten eines Quantencomputers, um Optimierungsprobleme in einem Bruchteil der Zeit zu lösen, die klassische Computer benötigen würden. Dies öffnet die Tür für die Verarbeitung größerer Mengen an komplexeren Datenpunkten zur Bearbeitung präziserer Fragen.

Universal Gate Computing konzentriert sich auf die Manipulation verschiedener Quantenzustände, um kundenspezifische Sequenzen zu erstellen, die sich besser für die Simulation und Durchführung von Vorhersageaufgaben eignen. Obwohl diese getrennten Zweige im Quantencomputer große Erfolge erzielt haben, tragen ihre direkten Anwendungen zu engen KI-Aufgaben bei.

Die Entwicklung von quantenneuronalen Netzwerken wird bei der Schaffung einer neuen Logik nützlich sein, die ursprünglich in der physikalischen Welt für AI-Anwendungen fußt. Durch das Vorantreiben dieser Entwicklung, könnte eine neue Welle der künstlichen Intelligenz entstehen, die uns einen Schritt näher an die AGI bringt.

Fazit

Die meisten Quantencomputer-Forschungsprojekte konzentrieren sich auf die Nutzung der Geschwindigkeit, die das Quantencomputing bringt. Aber der Wandel von einer digitalen Gesetzgebung hin zu einer natürlichen könnte die grundlegende Transformation sein, die notwendig ist, um von der Narrow zur allgemeinen KI zu gelangen.

Annie Bailey

Referenzen: **[1]** https://arxiv.org/pdf/1801.03918.pdf **[2]** https://phys.org/news/2019-09-quantum-convolutional-neural-networks.html **[3]** https://arxiv.org/pdf/1802.06002.pdf

Kann Quantum Computing den Klimawandel stoppen?

Das volle Ausmaß des Klimawandels und all seine Auswirkungen zu verstehen, ist eine komplexe Angelegenheit. Das Problem, das den Klimawandel verursacht, ist jedoch relativ einfach zu verstehen: In unserer Atmosphäre befindet sich zu viel Kohlendioxid. Um dieses Problem zu lösen, konzentrieren wir uns hauptsächlich darauf, wie wir die Menge an emittierten Kohlenstoff reduzieren.

Es gibt jedoch auch einen anderen Ansatz: das Entfernen des Kohlenstoffs, der sich bereits in der Atmosphäre befindet. Die Lösung dieser Aufgabe ist zurzeit kostspielig und eher theoretisch als praktisch. Durchbrüche im Bereich des Quantencomputers sind jedoch möglicherweise der Schlüssel, um Verschmutzungen schnell, effizient und effektiv aus der Atmosphäre zu entfernen.

Warum kann ein Quantencomputer die Klimaprobleme lösen?

Das Konzept des Quantencomputers ist für viele Branchen vielversprechend, von der medizinischen Forschung bis zur Wettermodellierung. Einer der

Bereiche, in denen dies die positivsten Auswirkungen haben könnte, ist die Bekämpfung des Klimawandels. Das neue Computermodell würde eine Rechenleistung erzielen, die derzeit von herkömmlichen Computern nicht erreicht werden kann.

Dies eröffnet die Möglichkeit neuer Modelle und Simulationen. Damit erhalten wir neue Einblicke in eine Welt, die wir nicht sehen können. Mit Hilfe eines Quantencomputers kann es gelingen, neue Methoden zur Eindämmung und Beseitigung der Emissionen zu entwickeln, die wir mehr als ein Jahrhundert lang in die Atmosphäre geschickt haben.

Wie funktioniert ein Quantencomputer?

Um das Potenzial des Quantencomputers zu erfassen, ist es wichtig zu verstehen, was genau ein Quantencomputer ist. Herkömmliche Computer verwenden Bits zum Speichern von Daten, die als eine Folge von Nullen und Einsen dargestellt werden. Ein Quantencomputer benutzt Quantenbits oder Qubits, um Informationen zu speichern.

Roman Uminski, Senior Key Account Manager, Kaufberater.io

Qubits unterliegen nicht den gleichen Beschränkungen wie ihre binären Gegenstücke. Anstatt den Wert 0 oder 1 anzunehmen kann ein Qubit gleichzeitig eine 0, eine 1 oder beides sein. Diese technische Leistung wird durch Elektronen und Photonen ermöglicht, die gleichzeitig unterschiedliche Zustände einnehmen können, solange sie nicht beobachtet werden.

In den letzten Jahren haben sich Quantencomputer aus dem Bereich der Theorie gelöst und sind immer mehr zur Realität geworden. Mitte 2019 baute Google einen Quantencomputer, dessen Prozessor nach Angaben des Unternehmens in nur 200 Sekunden eine Aufgabe erledigt hat, für die ein herkömmlicher Computer etwa 10000 Jahre gebraucht hätte. Auch wenn diese Angaben bisher nicht verifiziert wurden, hat sich damit eine Tür für Computer mit gigantischer Rechenleistung geöffnet.

Eine unmittelbare Auswirkung von Quantencomputern könnte darin bestehen, den Energieverbrauch von Hochleistungsrechnern zu senken. Es liegt auf der Hand, dass 40000 Prozessoren und 250 Million GB Speicher für eine Simulation mehr Energie verbrauchen, als 53 Qubits eines Quantencomputers, die die Aufgabe in 3 Minuten erledigen.

Quantenkompetenz braucht jedoch Zeit, um sich zu entwickeln. Oft fehlen Mitarbeiter, um wirkungsvolle Technik entwickeln zu können. Studiengänge wie der Masterstudiengang Quantum Engineering der ETH Zürich sollten auch an anderen Universitäten und Fachhochschulen eingeführt werden. Airbus hat beispielsweise eine Quantum Computing Challenge gesponsert, um enge Beziehungen innerhalb der Quantengemeinschaft aufzubauen und Unterstützung bei der Beantwortung der wichtigsten Fragen der Luft- und Raumfahrtindustrie zu ermutigen.

Die Unsicherheiten des Klimawandels

Wir wissen, dass sich unser Planet erwärmt. Nach Angaben der National Oceanic and Atmospheric Administration ist die durchschnittliche Oberflächentemperatur der Erde seit dem späten 19. Jahrhundert um etwa 0,9 Grad Celsius gestiegen. Es ist auch bekannt, dass die Menschen und die Industrie in diesem Zeitraum mehr Kohlendioxid und andere Emissionen in die Atmosphäre entlassen haben als zu irgendeinem anderen Zeitpunkt in der Geschichte. Es gibt eine Fülle von Daten, die diese Veränderungen dokumentieren. Genug Daten, um einen wissenschaftlichen Konsens darüber zu erzielen, dass der vom Menschen verursachte Klimawandel real ist.

Was wir derzeit nicht haben, ist eine zuverlässige Methode, um die Auswirkungen dieser Änderungen zu verstehen oder zukünftige Ergebnisse vorherzusagen. Wissenschaftler verfügen zwar über Computer, mit denen sie die potenziellen Veränderungen projizieren können, die der Planet aufgrund des Klimawandels erleiden könnte, diese Modelle sind jedoch weitgehend durch die traditionelle Rechenleistung begrenzt.

Viele der heutigen Wettermodelle führen häufig zu falschen Vorhersagen. Das ist meistens auf die Mängel der aktuellen Modellierungssysteme zurückzuführen. Meteorologen und Wissenschaftler haben mit den vorhandenen Instrumenten keine wirklich sichere Möglichkeit, zu prognostizieren, wie sich unsere Emissionen auf die Atmosphäre auswirken und welche langfristigen Auswirkungen sich daraus ergeben könnten.

Der Quantencomputer befindet sich heute noch im Äquivalent des Röhrenzeitalters und hat sein Transistor-Äquivalent noch nicht erreicht. Viele der zahlreichen neuen Technologien (darunter supraleitende, Ionenfallen-, Photonen- oder Silizium-basierte und topologische Technologien) erfordern noch mehr Forschung und eine gesicherte Finanzierung.

Wie Quantencomputer zur Bekämpfung des Klimawandels beitragen können

Ein Quantencomputer kann die Lücke der heutigen Wettermodelle schließen. Darüber hinaus könnte er einen Schlüssel zur Lösung unseres Emissionsproblems enthalten. Da die Rechenleistung von Quantenprozessoren um ein Vielfaches höher ist als bei herkömmlichen Alternativen, können Computermodelle in Zukunft sehr viel genauer werden. Indem wir größere Datenmengen verwenden und diese Informationen sich schneller und effizienter als je zuvor verarbeiten lassen, können wir einen klareren Überblick darüber bekommen, was genau der Klimawandel auf dem Planeten bewirkt und was sich für uns am Horizont abzeichnet.

Computer mit dieser Rechenleistung können den Wissenschaftlern auch bei anderen Problemen helfen

und zum Beispiel den Aufbau und die Wirkung großer komplexer Moleküle berechnen. Dieses können binäre Computer nicht effektiv leisten. Der Versuch, das Verhalten eines Moleküls mit 70 Atomen zu berechnen, würde mit herkömmlichen Computern viele Jahre benötigen.

Mit dem Quantencomputer könnten Wissenschaftler das Verhalten komplexer Moleküle genau simulieren. Das würde zum Beispiel die Möglichkeit eröffnen, genau zu verstehen, wie Kohlendioxid auf verschiedene chemische Methoden zur Reduktion reagiert. Dadurch könnten Wissenschaftler außerdem die besten Wege finden, um Kohlenstoff aus der Atmosphäre zu entfernen. Sicher würden dabei auch neue Methoden entwickelt, um vorhandenen Kohlenstoff zu recyceln und wiederzuverwenden, anstatt ihn in die Atmosphäre zu entlassen.

Wenn Ingenieure und Wissenschaftler mit hinreichender Genauigkeit wissen, wie Kohlenstoff auf verschiedene Arten der Interaktion mit ihm durch Simulationen reagiert, können wir endlich Maßnahmen ergreifen, um das schädliche Gas aus unserer Atmosphäre zu entfernen. Die Abscheidung von Kohlenstoff ist seit Jahrzehnten ein Thema für Wissenschaftler. Am Horizont stehen neue Tools, mit deren Hilfe Emissionen aus der Atmosphäre genommen und als Rohstoffe wiederverwendet werden. Jüngste Durchbrüche deuten darauf hin, dass es möglich ist, Treibhausgasemissionen in eine Brennstoffquelle umzuwandeln, die Energie liefern kann.

Diese Art von technischen Entwicklungen sind kein geeigneter Ersatz für die Senkung der Emissionen und den Verzicht auf das wahllose Ablassen von Kohlendioxid und anderen schädlichen Treibhausgasen in die Atmosphäre. Sie bieten jedoch einen brauchbaren Mittelweg, um unseren derzeitigen Weg fortzusetzen. Letztlich geht es darum, die Realität des Klimawandels anzuerkennen und die drastischen Maßnahmen zu ergreifen, die erforderlich sind, um die verheerendsten Auswirkungen, die sich in Zukunft abzeichnen, zu verhindern. Quantencomputer könnten endlich die Technologie ermöglichen, die wir benötigen, um so viel Kohlenstoff wie möglich aus der Atmosphäre zu entfernen und ihn sinnvoll zu nutzen.

Fazit

Bis die Menschheit endlich eine Netto-Null-CO2-Emission erreicht, müssen wir die Auswirkungen des Klimawandels begrenzen und einen sinnvollen Weg finden, den überschüssigen Kohlenstoff aus der Atmosphäre zu entfernen. Überschüssiges CO2 kann für viele andere Zwecke sinnvoll verwendet werden.

Regierung und Industrie müssen ihre Anstrengungen beschleunigen, indem sie in Software, Hardware und Köpfe investieren, zu ihrem eigenen Nutzen und zum Nutzen des Planeten. Quantum Computing könnte die bestimmende Technologie der Zukunft sein. Der Klimawandel ist die entscheidende Herausforderung unserer Zeit. Es geht um nichts Geringeres als unsere Zukunft. Wir müssen alle verfügbaren (und bald verfügbaren) Tools nutzen, um diese Herausforderung zu gewinnen.

Roman Uminski

2. CYBER SECURITY

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

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

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

Ebenso facettenreich wie das Thema Cyber Sicherheit sind die einzelnen Beiträge dieser Ausgabe selbst. Sie reichen von prozessorientiertem Datenschutz sowie Governance zu den vielfältig eingesetzten digitalen Identitäten und konkrete Ausprägungen angewandter Sicherheit.

MEIST GEKLICKT – Unsere erfolgreichsten Blog-Beiträge

Unsere Beiträge wurden insgesamt über **1.000.000 Mal** geklickt*

Beiträge zum Thema **CYBER SECURITY** erhielten **222.000** Klicks.

	Autor | Thema
#1	**Dietmar Schnabel |** Cyberangriffe 2019: Warum sind Unternehmen und Privatpersonen immer noch so verwundbar? **Seite 70**
#2	**Thomas Jakubiak |** Awareness-Bildung durch Live-Hacking: Cyberrisiken erfahrbar machen **Seite 82**
#3	**Pascal Cronauer |** LockerGoga CottleAkela und Gorgon – Ransomware ist zurück **Seite 66**
#4	**Arved Graf von Stackelberg |** Richtiges Nutzerverhalten in Zeiten von Hackerangriffen **Seite 73**
#5	**Roman Hugelshofer |** Sicherheitsansätze für Digitalisierungsprojekte: Das richtige Werkzeug ist Waffe und Segen zugleich **Seite 79**

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 27. Januar 2020.**

INHALT

2.1 IT INFRA-STRUCTURE

Sicher in die Cloud

Wer in die Cloud geht, muss auch seine IT-Sicherheit neu ausrichten. Rolf Haas, Senior Enterprise Technology Specialist bei McAfee erklärt, worauf es ankommt.

Rolf Haas, Senior Enterprise Technology Specialist, McAfee

Die Zeit, in der die Cloud in deutschen Unternehmen als unberechenbares Sicherheitsrisiko galt, ist vorbei. Im aktuellen Cloud Security-Report von McAfee geben 96 Prozent der Unternehmen an, bereits auf Cloud-Angebote zu setzen. 85 Prozent sagen außerdem, dass in ihrem Unternehmen inzwischen ein größeres Vertrauen in die Cloud herrsche als noch vor zwölf Monaten. Die Stoßrichtung stimmt: Cloud-Lösungen bergen viele Vorteile für Endnutzer, darüber hinaus sind sie oftmals wirtschaftlicher, da insbesondere im Vergleich zu On-Premise-Alternativen ein Großteil des Administrationsaufwands entfällt. Auch hohe Anschaffungskosten für neue Hardware entfallen.

Trotz aller Vorteile dürfen Unternehmen aber nicht vergessen, ihre Infrastruktur adäquat abzusichern. Denn je mehr Daten vom eigenen Rechenzentrum in die Cloud wandern, desto höher das Risiko von Datenverlusten und teuren Verstößen gegen die europäische Datenschutzgrundverordnung (DSGVO). Um Cyber-Kriminellen das Leben möglichst schwer zu machen und auch in der Cloud ein Höchstmaß an Sicherheit und Datenschutz zu gewährleisten, müssen Unternehmen ihre IT-Sicherheit gezielt auf die neuen Herausforderungen einstellen.

Sicherheit auch außerhalb des Perimeters

Als die IT-Landschaften von Unternehmen noch ausschließlich aus On-Premise-Lösungen bestanden, waren die Daten auf den Servern so sicher wie das Gold in einer Schatzkammer. Es musste lediglich sichergestellt sein, dass niemand die Burgmauer überwand – beziehungsweise den Perimeter, wie das IT-Äquivalent heißt. Im Cloud-Zeitalter bewegen sich Daten hingegen mobil zwischen Cloud-Anwendungen und dem eigenen Rechenzentrum, die Verteidigung des Perimeters alleine reicht nicht mehr aus. Egal wie gut die On-Premise-Sicherheit auch sein mag, sie verhindert nicht, dass eine Cloud-Anwendung zum Einfallstor für Datendiebe werden kann.

Um sich gegen Datendiebstähle abzusichern, haben Unternehmen üblicherweise eine Data Loss Prevention (DLP)-Lösung im Einsatz. Diese kontrolliert den Zugriff auf Daten und spürt anhand von vordefinierten Sicherheitsrichtlinien illegitime Zugriffsversuche auf. Dabei kann es sich einerseits um Zugriffe von Cyber-Kriminellen handeln, die kompromittierte Accounts nutzen, oder um leichtsinniges Verhalten der eigenen Mitarbeiter. Wenn die Cloud ins Spiel kommt, verlieren DLP-Lösungen aber oft an Effektivität. Ein Beispiel: E-Mail-Richtlinien verhindern den Versand von sensiblen Dokumenten per E-Mail, sämtliche Versuche werden blockiert und dem Sicherheitsteam gemeldet. Dieser Mechanismus greift jedoch nur auf lokalen Geräten. Wenn sich ein Cyber-Krimineller stattdessen über den Browser bei Office365 oder einem anderen Anbieter einloggt, funktioniert der Versand sensibler Dokumente ohne Probleme. Um Daten auch außerhalb des eigenen Perimeters zu schützen, benötigen Unternehmen also einen neuen Ansatz.

CASB-Lösungen schaffen Abhilfe

Cloud-Ressourcen sollen ihrer Bestimmung nach unkompliziert und flexibel zu erreichen sein – standortunabhängig und von jedem Endgerät. Gerade diese Einfachheit öffnet aber auch Cyber-Kriminellen Tür und Tor. Um sich vor Angriffen zu schützen, müssen Unternehmen den Cloud-Zugang deshalb besser absichern. Am besten gelingt dies mit einem Cloud Access Security Broker (CASB). Ein CASB ist eine Appliance, die zwischen die Nutzer von Cloud-Services und die Angebote der Cloud-Service-Provider geschaltet wird, um sämtliche Interaktionen zu überwachen, Sicherheits- und Datenschutzrichtlinien durchzusetzen sowie Bedrohungen zu erkennen und zu bekämpfen. Auch ein CASB folgt dabei vordefinierten Sicherheitsrichtlinien und blockiert sowie meldet sämtliche Verstöße. Die Branchenanalysten von Gartner prognostizieren, dass im Jahr 2020 85 Prozent der Großunternehmen einen CASB im Einsatz haben werden.

Bedeutet eine zusätzliche Lösung auch zusätzliche Arbeit? Wenn der Umstieg in die Cloud eine Vervielfachung des Aufwands für IT-Sicherheit bedeutet, dann könnte das die oben beschriebenen Effizienzgewinne auffressen. Deshalb ist entscheidend, den CASB mit der eingesetzten DLP-Lösung zu integrieren. So wird es möglich, einen einzelnen Katalog an Sicherheitsrichtlinien anzulegen, der dann sowohl für die durch eine DLP-Lösung abgesicherten On-Premise-Ressourcen als auch für die durch einen CASB geschützten Cloud-Anwendungen gilt. Über eine zentrale Verwaltung wird es außerdem möglich, Sicherheitsvorfälle in beiden Umgebungen zentral abzubilden. Das erleichtert den Mitarbeitern das

Incident Management und verringert den Administrationsaufwand.

Verdächtige Nutzer immer im Blick

Einem Datendiebstahl gehen fast immer auffällige Verhaltensweisen voraus, unabhängig vom Hintergrund des Angriffs und der Professionalität des Vorgehens. Kommt es bei einem bestimmten Account etwa zu einer außergewöhnlich hohen Zahl an fehlerhaften Login-Versuchen, kann das ein Hinweis auf einen Bruteforce-Angriff sein. Probiert es ein einzelner Nutzer hingegen mit einer großen Zahl an Nutzername-Passwort-Kombinationen, handelt es sich möglicherweise um einen Fall von „Credential Stuffing". Auch wenn ein Zugriff verschlüsselt über das Tor-Netzwerk erfolgt, deutet dies auf einen Angriff hin. All diese punktuellen Hinweise muss eine Sicherheitslösung routinemäßig auswerten. Erkennt sie einen Verstoß gegen die Richtlinien, muss sie den entsprechenden Account oder Nutzer blockieren, bis der Vorfall hinreichend untersucht wurde.

Gleichzeitig sind viele Risikobeurteilungen jedoch stark kontextrelevant. Wenn es zu Verhaltensweisen kommt, die zwar kein klarer Beweis für einen Angriff sind, aber zumindest verdächtig erscheinen, sollten alle weiteren Aktionen dieses Nutzers besonders kritisch beäugt werden. Verzeichnet etwa ein Account bislang ausschließlich Zugriffe aus Deutschland und dann plötzlich einen Login-Versuch über eine russische IP-Adresse, dann kann das bedeuten, dass der betroffene Mitarbeiter lediglich dort auf Geschäftsreise ist. Versucht der aus Russland eingeloggte Nutzer dann jedoch sofort, auf sensible Daten zuzugreifen, erscheint eine vorübergehende Sperrung des Accounts und eine nähere Überprüfung des Vorgangs unbedingt sinnvoll. Diese kontextabhängige Beurteilung fällt umso leichter, je einheitlicher die Sicherheitslandschaft ist. Fragmentierte Lösungen erfassen immer nur einen kleinen Teilbereich und sind bei solchen Vorgängen weitgehend nutzlos – auch das ist ein wichtiges Argument für die Integration von CASB und DLP-Lösung.

Sicherheit im Cloud-Zeitalter

Die Cloud steht On-Premise-Systemen heute nicht nur gleichberechtigt gegenüber, sondern wird in absehbarer Zeit das dominierende Bereitstellungsmodell werden – mancherorts ist sie das schon. Auf diesen Wandel müssen sich die IT-Sicherheitsteams in Unternehmen einstellen. Wo sie vormals jede Migration in die Cloud kritisch beäugten, wird in Zukunft eine „Cloud first"-Strategie Einzug erhalten. Konkret bedeutet das, nicht etwa vorhandene, lokale Sicherheitslösungen in die Cloud zu verlängern, sondern völlig neue Wege einzuschlagen. Vorhandene Modelle und Lösungen alleine schaffen keine Abhilfe, logische Erweiterungen wie SSL-Proxying oder DLP-Browser-Plugins mögen zwar punktuell sinnvoll sein, lösen aber nur einen kleinen Teil der Herausforderungen. Darüber hinaus lassen sich die Vorteile der Cloud nur dann mit den Sicherheitsanforderungen moderner Unternehmen ausbalancieren, wenn passgenaue Lösungen zum Einsatz kommen. Ein Umstieg auf Endnutzer-Anwendungen aus der Cloud und ein gleichzeitiges Festhalten an Sicherheitslösungen aus dem On-Premise-Zeitalter stellt vor diesem Hintergrund schlicht ein Versäumnis dar, das enorme Risiken mit sich bringt. Wer in die Cloud geht, muss auch seine IT-Sicherheit neu ausrichten.

Rolf Haas

Keine IT-Umgebung ist unantastbar

Unternehmen müssen sich die Bedeutung von durchdachter IT-Sicherheit stärker ins Bewusstsein rufen und aktuelle Malware-Trends beobachten

Wer als Verantwortlicher in einem Unternehmen glaubt, dass ihn nur ein Teil der Bedrohungen interessieren muss, die im Internet unterwegs sind, der irrt sich gewaltig. Es gibt keinen Zweig der IT-Sicherheit, der für sich alleine dasteht und isoliert betrachtet, sowie behandelt werden kann. Ebenso wenig reicht es aus, ein Schutzprogramm alleine hochzufahren, um einen Bereich abzudecken, der besonders empfindlich erscheint und die restlichen zu vernachlässigen, als wären sie unantastbar. Keine IT-Umgebung ist immun gegen Angriffe von kriminellen Kräften. Kein Angriffsweg ist der einzige gefährliche und keine Methode die allein bedrohliche. Natürlich kann ein Unternehmen sagen: „Was gehen mich die Cloud-Bedrohungen an? Ich betreibe ja nicht mal eine." Das bedeutet aber nicht, dass die IT-Sicherheit daher vernachlässigt werden darf, nur weil sich derzeit viel in der öffentlichen Debatte auf Angriffe gegen Cloud Computing konzentriert. Malware wird für alle möglichen Varianten von Angriffswegen geschrieben und Angriffswege können sich allen möglichen Gegebenheiten von Netzwerkaufbau und Speicherort der Daten anpassen. Sie schlagen dort zu, wo sie können – egal ob auf dem Server in der Firma, im Rechenzentrum, auf dem Mobiltelefon oder eben in der Cloud.

Der Mid Years Report von Check Point für das erste Halbjahr 2019 belegt deutlich, dass alt-

bekannte Bedrohungen weiterentwickelt werden, während gleichzeitig neue Schadprogramme auf den Markt kommen. Die Kriminellen passen sich der Situation an, sie machen den digitalen Wandel mit und die IT-Sicherheit muss nachlegen, falls die Unternehmen nicht sehr bald den Kürzeren ziehen wollen.

Banken-Trojaner auf dem Vormarsch

Der Bericht deckt besonders auf, dass Banken-Trojaner zunehmend beliebter werden. Im Vergleich zum Vorjahr haben sich Angriffe dieser Art von Schädlingen um 50 Prozent erhöht. Mittlerweile ist Banken-Malware in der Lage, gezielt Zahlungsdaten, Anmeldeinformationen und Gelder zu stehlen. Neue Versionen stehen bereit für eine massive Verbreitung – und zwar durch jeden, der für sie auf dem Schwarzmarkt bezahlt. Interessant dabei ist vor allem, dass die drei häufigsten Banken-Trojaner schon den Großteil der Angriffe abdecken: Ramnit traf 28 Prozent der Unternehmen, Trickbot kam auf 21 Prozent und Ursnif bedrohte noch stattliche 10 Prozent der Firmen weltweit – die Top-3 sind bereits verantwortlich für 59 Prozent aller Angriffe mittels Banken-Trojaner.

Dietmar Schnabel, Regional Director Central Europe, Check Point Software Technologies

Dieses Ergebnis führt uns deutlich vor Augen, wie moderne IT-Sicherheit aussehen muss: Kein Rundumschlag ins Blaue, keine Hoffnung auf die Unantastbarkeit irgendeiner Umgebung, oder der Glaube, dass man zu unwichtig sei, um ins Visier zu geraten; stattdessen eine gezielte Verteidigung, die so viel wie möglich abdeckt, aber besonders die Schadprogramme abwehrt, die am bekanntesten sind. Die Angreifer nämlich gehen sehr überlegt vor: In Italien kam Ramnit gezielt zum Einsatz, als die jährliche Steuerbescheinigung bevorstand und richtete große Schäden an. Die IT-Sicherheit muss darum ebenfalls durchdacht implementiert und ausgebaut werden. Letzten Endes ist nichts ärgerlicher, als das Opfer eines Cyber-Angriffes geworden zu sein und sich dabei eingestehen zu müssen, dass die Attacke über diesen speziellen Angriffsweg eigentlich leicht zu verhindern gewesen wäre: Weil die Malware und ihre Häufigkeit bekannt, sowie die Umstände, warum sie gerade jetzt zuschlug, einladend waren.

Regionale Eigenheiten

Der europäische Raum wurde besonders stark durch Krypto-Miner getroffen – obwohl Coinhive, einer der verbreitetsten Schädlinge, bereits im Frühjahr eingestellt wurde. Sie machten 19 Prozent aller Angriffe aus. Auf den vorderen Plätzen rangieren im Gebiet EMEA (Europe, Middle East, Africa) die Schadprogramme Cryptoloot mit 6,3 Prozent, Coinhive mit 6,0 Prozent und JSEcoin mit 5,3 Prozent. Bei ihnen handelt es sich um Malware, die einen Rechner infiziert und seine Leistung missbraucht, um heimlich Krypto-Währung wie BitCoin und Monero zu generieren. Das mag anfangs noch harmlos klingen, weil es keine Unternehmens-Daten gefährdet. Doch je mehr der Miner arbeitet, desto mehr Leistungs des Rechners nimmt das Schürfen in Anspruch, desto mehr Strom verbraucht der Computer und umso stärker sinkt die Rechenkapazität, die dem Unternehmen noch zur Verfügung steht. Ein Computer mag da verkraftbar sein; wenn sich aber der Miner im Netzwerk verbreitet und ein Bot-Netz von Minern aufbaut, dann lassen sich die Auswirkungen leicht absehen: Der Stromverbrauch und damit die Kosten steigen ins Unermessliche, die Mitarbeiter können ihre Rechner kaum zur Arbeit nutzen – und es liegt wohl eine Hintertür im System offen, denn irgendwie kam der Krypto-Miner hinein.

Dieses Schlupfloch können auch wesentlich gefährlichere Schädlinge ausnutzen – oder aber ein solcher hat sie geschaffen und befindet sich bereits auf den Firmen-Computern. Ein gutes Beispiel ist der Trojaner Emotet, der in Deutschland über viele Monate die Top-Malware-Rangliste von Check Point angeführt hatte, weil er die meisten Unternehmen hierzulande traf. Ursprünglich als Banken-Trojaner programmiert, wurde er nach einiger Zeit modifiziert und ist nun in der Lage – und vor allem dazu gedacht – Hintertüren für andere Malware zu öffnen. Dabei beherrscht die Malware außerdem eine Vielzahl von Ausweichfähigkeiten, um einer Entdeckung oder Entfernung möglichst lange zu entgehen. Emotet selbst prescht also vor, schlägt heimlich eine Bresche in das Sicherheitsnetz und macht den Weg frei für Krypto-Miner, Ransomware, Spionage-Programme und andere Bedrohungen.

Den größten Anteil an Angriffen macht aber in allen Regionen der Welt die Kategorie ‚Mobile' aus. Im Raum EMEA fallen 25 Prozent der Angriffe in diesen Sektor. Der gefährlichste Schädling ist hier Triada mit 38 Prozent. Dabei handelt es sich um eines der fortschrittlichsten Schadprogramme gegen Android-Smartphones. Im Jahr 2018 wurde Triada sogar auf einigen Smartphones als bereits ab Werk installiert entdeckt. Google veröffentlichte einen Bericht dazu, aus dem hervorging, dass Triada während des Produktionsprozesses der Mobilgeräte durch eine dritte Partei eingeschleust wurde.

Malware stirbt nicht aus

Was der Halbjahresbericht besonders hervorhebt: Eine Angriffsmethode taucht nicht auf, schlägt

eine Zeit lang zu und verschwindet für immer von der Bildfläche. Die Bedrohungslandschaft erweitert sich täglich, sie schrumpft nicht. Alte Bekannte, wie DNS-Angriffe, DdoS-Attacken und klassische Remote-Access-Trojaner sind weiterhin im Einsatz und kommen in modifizierten Varianten erneut auf den Schwarzmarkt. Verschiedene Malware-Arten können also eine Zeit lang ruhen und plötzlich wieder auftauchen. Es wäre daher eine gefährliche Fehlannahme, zu glauben, dass eine Bedrohungsart erledigt wäre und in den Sicherheitsplanungen keine Rolle mehr spielen muss. Kein digitaler Schädling verschwindet endgültig. Das beweist unter anderem Emotet oder die neue Ransomware-Welle, die keineswegs nach der großen Attacke durch WannaCry besiegt wurde. Unternehmen müssen also neben aktuellen Patches, Updates und Überprüfungen der Richtlinien auch dafür sorgen, dass sie ein durchdachtes und dichtes Netz aus Sicherheitslösungen um ihre wertvollen Daten ziehen. Sie müssen gegen Angriffe auf Mobilgeräte ebenso gewappnet sein, wie gegen Attacken auf eine Cloud oder ein klassisches Server-Zentrum. Dabei kann keine Malware-Art – ob Ransomware, Spionage, Banken-Trojaner – priorisiert behandelt oder ein IT-Bereich vernachlässigt werden. Denn keine vernetzte Umgebung ist immun gegen kriminelle Attacken.

Dietmar Schnabel

Ein Sicherheits-Hub für alle Applikationen

Web-Applikationen sind im Zuge der Digitalisierung zu einem geschäftskritischen Teil der IT und somit zu einem attraktiven Angriffsziel für Hacker geworden.

Die Bedeutung des Schutzes von Applikationen wird oftmals unterschätzt. Unternehmen wollen rasch ihre Ideen umsetzen, dabei werden nicht selten Security-Grundsätze verletzt oder ignoriert. Sie bringen minimal funktionsfähige Iterationen eines Produkts auf den Markt, um sie möglichst schnell mit Kunden zu testen. Das Produkt steht im Internet und ist mit anderen Datentöpfen verbunden. Schon hat man das Tor geöffnet.

Um dem zu entgegnen, bietet sich eine Komplettlösung an. Dabei geht es darum, verschiedene Komponenten zu kombinieren, die in unterschiedlichen Disziplinen für Sicherheit sorgen. Die Nachfrage nach solchen Komplettlösungen aus einer Hand steigt, da Einzelkomponenten häufig von diversen Herstellern stammen und nicht gut zusammenspielen.

Eine Web Application Firewall muss viele Aufgaben bewältigen

Eine moderne Web Applikation Firewall (WAF) ist ein Multitalent. So sollte sie neben ihren eigentlichen Aufgaben auch APIs schützen können. API steht für Application Programming Interfaces, also Schnittstellen zu anderen Programmen. Eine herkömmliche WAF ist auf HTML-Formulare ausgelegt und kann mit JSON-Strukturen nicht umgehen, die bei APIs üblich sind. API-Sicherheit und Web-Applikation-Security verschmelzen zunehmend, zumal Security-Themen wie Cross-Site-Scripting oder Injection-Angriffe inzwischen auf allen Kanälen relevant sind. Javascript-Applikation, die im Browser laufen und auf APIs im Backend zugreifen, erfahren eine zunehmende Verbreitung.

Die WAF analysiert jeden Request zwischen Anwendern und Web-Applikationen und -Services. So lassen sich Angriffsversuche blockieren, bevor sie in das interne Netzwerk gelangen. Ein Zusammenspiel mit einem Identity and Access Management und einem API-Gateway garantiert, dass nur gefilterte, authentisierte und autorisierte Zugriffe passieren.

Manche WAFs bieten zudem eine Integration von Threat Intelligence, also eine Prüfung gegen Listen von Threats. Praktisch für jede Adresse aus dem IPv4-Bereich lässt sich damit ein Scoring erstellen, ob bösartige Aktivitäten davon ausgehen, etwa Spam, Angriffe gegen Webserver, Phishing, oder Tor-Nodes. Diese Informationen können im Access Management herangezogen werden, um entsprechende Policies zu entwickeln. Beispiel: Wenn ein Zugriff über Tor erfolgt, dann ist zwingend eine Zwei-Faktor-Authentifizierung erforderlich.

Eine weitere Technik nennt sich Virtual Patching: Ein Reverse Proxy schützt dabei interne Dienste vor Zugriffen von außen. Der Zugriff landet auf dem Proxy, wo sich zeitnah und automatisiert Patches gegen Sicherheitslücken einspielen lassen. Das verschafft den Unternehmen mehr Zeit, um die physikalische Hardware abzusichern. Auch verteilte Schlüssel sorgen für ein Plus an Sicherheit. Normalerweise werden Passwörter als Hashwerte abgespeichert. Wenn ein Angreifer an eine solche Passwort-Datenbank gelangt, ist es eine Frage der Zeit, bis die Hash-Verschlüsselung geknackt ist. IBM Research hat ein kryptografisches Protokoll entwickelt, wie sich ein Passwort in verteilte Hashes aufteilen und auf mehreren Servern speichern lässt. Um den Hash eines Passworts zu entschlüsseln, sind dann sämtliche Einzelteile notwendig. Das erschwert die Aufgabe für den Angreifer um ein Vielfaches.

Andreas Dumont, Freier Journalist, Büro Andreas Dumont

API-Gateway für sichere Schnittstellen
Application Programming Interfaces (APIs) sind die tragenden Säulen moderner Anwendungen und Services. Dies Schnittstellen exponieren Daten über Unternehmensgrenzen hinaus in das Internet, wo die Kunden darauf zugreifen. Daher ist ein Schutz notwendig, nicht nur gegen herkömmliche Angriffe über das Web, sondern auch vor API-spezifischen Angriffen. Mit einem API-Gateway lassen sich JSON-Schemas und Open-API-Spezifikationen durchsetzen. Alle API Calls, die dem nicht entsprechen, werden abgewiesen. Dashboards und Reporting sorgen dabei für einen Überblick über sämtliche API-Zugriffe, zeigen Angriffsversuche und Spezifikationsverletzungen, erkennen Performance-Probleme und machen Fehler im Backend sichtbar. Access Logs zu API Calls können an Untersysteme weitergeleitet werden und so beispielsweise als Basis für die Monetarisierung von Zugriffen dienen.

Identity and Access Management
Das Identity and Access Management (IAM) hat die Aufgabe, Benutzer zu authentifizieren und die Informationen an die passende Anwendung zu übermitteln. Um nicht von einer Methode abhängig zu sein, empfiehlt sich dabei eine starke Zwei-Faktor-Authentifizierung. Diese lässt sich sogar bei Applikationen durchsetzen, die das eigentlich gar nicht unterstützen. Ein Beispiel ist Microsoft Sharepoint, das mit Benutzernamen und Passwort arbeitet. Das IAM ermöglicht dennoch eine Zwei-Faktor-Authentifizierung, in dem es einen zweiten Faktor abfragt und die festgestellte Identität an die Applikation übermittelt. Anwender profitieren zudem von einem Single Sign-On: Je nachdem, wo ein Zugriff hingeleitet wird, kann die Identität des authentifizierten Benutzers anders repräsentiert werden. Das IAM dient dabei als eine Art Identitätsweiche. Zudem lässt sich die Situation des Zugriffs – am Arbeitsplatz, von zuhause oder unterwegs – und die Historie eines Benutzers berücksichtigen. Wenn Benutzer ihre Identitäten für den Zugriff von außen mitbringen, spricht man von BYOI (Bring Your Own Identity). Sie verwenden bestehende Accounts aus sozialen Netzwerken wie Facebook, Google oder Twitter für den Zugriff auf Services. Mit einem zweiten Faktor lässt sich ein solcher Social Login zu einem stark authentisierten Login erweitern.

Andreas Dumont

2.2 TRUST

KI in der Cybersecurity: Fluch oder Segen?

KI, Big Data und Analytics werden in der Absicherung von IT-Infrastrukturen zukünftig eine tragende Rolle spielen, da sind sich inzwischen viele Unternehmen sicher . Mehr als ein Viertel will sie in Ergänzung zu bestehenden Systemen einsetzen, 36 Prozent wollen damit eine vollautomatisierte IT-Sicherheitsarchitektur aufbauen. „Für ein wirksames Management von Informationssicherheit brauchen Unternehmen aber mehr als nur Technologie“, sagt Severin Rast, Leiter IT Security Consulting bei der INFODAS GmbH. Er plädiert für einen ganzheitlichen Ansatz: ein wirksames Informationssicherheitsmanagementsystem (ISMS), bei dem menschliche und künstliche Intelligenz durchaus Hand in Hand arbeiten sollten.

KI-Tools in der Cybersecurity werden aktuell hoch gehandelt. Angesichts des Fachkräftemangels in der IT ist das kein Wunder. KI-basierte DLP und Netzwerküberwachung kann in Echtzeit die Sicherheit des Informationsverbundes erhöhen. KI-basierte Sicherheitssoftware entlastet die Cybersecurity-Teams von Routineprozessen und erlaubt die Konzentration auf die Kernaufgaben, sie ermöglicht Echtzeitanalysen und schnelle kontextbasierte Informationsauswertung. Aber noch wenig verbreitet ist das Bewusstsein, dass sich auch KI täuschen lässt, wird sie nicht entsprechend abgesichert und durch menschliche Intelligenz überwacht.

Und damit können neue Bedrohungslagen entstehen. Denn auch Cyber-Kriminelle interessieren sich bei der Entwicklung von leistungsfähiger neuer Malware für diese Form der Effizienzsteigerung: Niemand hindert sie daran, sich diese frei verkäuflichen Systeme zu beschaffen und diese gegen ihre KI-basierten und lernfähigen Schadcodes antreten zu lassen. Dadurch trainieren Cyber-Kriminelle ihre Systeme, die dann beispielsweise typischen Netzwerkverkehr oder das Verhalten eines authentifizierten Nutzers oder seines Endgerätes simulieren. Es ist daher nicht ausgeschlossen, dass präventive Lösungen nur so lange ihre Schutzwirkung behalten, so lange sie besser und schneller lernen als die Angreifer.

Hinzu kommt: Die Arbeitsweise von leistungsfähigem Machine Learning ist selbst für die Programmierer meist nicht vollständig transparent. Sobald Künstliche Neuronale Netze (KNN) mit vielen verborgenen Schichten ge-

nutzt werden, die durch ihr Training, – sei es für Anomalieerkennung im Netzwerkdatenverkehr bei Cyberattacken, Bilder- oder Spracherkennung – Erfahrungen sammeln und ihren Algorithmus dabei selbst optimieren, stehen wir vor einer Black Box. Es ist bereits vorgekommen, dass Entwickler einer KI ab einem bestimmten Punkt nicht mehr nachvollziehen können, wie sich der Algorithmus im KNN weiterentwickelt.

Dies führt dazu, dass sich einerseits nur schwer überprüfen lässt, ob KNN in ihren Lernprozessen manipuliert wurden und andererseits die entstandenen Algorithmen unbekannte Schwachstellen haben. Nachgewiesen wurde dies mit unter anderem mit Adversarial Examples bei Audio- und Bilddateien. Hierbei werden Pixel in einem Bild oder Frequenzen in der Audiospur derart verändert oder überlagert, dass dies für das menschliche Auge oder Ohr nicht wahrnehmbar und auch kaum messbar ist. Die angegriffene KI wird das Bild oder die Audiospur aber durch die Manipulation völlig anders interpretieren und klassifizieren. Solche Adversarial Examples wird es genauso für andere Datentypen und Muster geben, auch in IT-Security-Systemen.

Möglich sind auch Angriffe über Supply-Chains, in dem Fall die Entwicklung der Algorithmen. Gelingt es Angreifern, Trainings- oder Referenzdaten, die zum Teil öffentlich im WWW erhoben werden, zu manipulieren, lernt das System dann bereits unentdeckt mit „falschen“ Daten. Angesichts der Tatsache, dass ein Trainingsdatensatz für eine KI leicht über eine Millionen Einzeldaten enthalten kann, ist nicht ausgeschlossen, dass heute schon versteckte Hintertüren in KI-Systemen existieren, die Angreifer lediglich aktivieren müssen.

Weltweite Schadenszenarien waren bislang glücklicherweise die Ausnahme. Das muss aber nicht so bleiben, solange Entscheider IT-Sicherheit immer noch als Technologie-Frage behandeln – statt sie als Top-Management-Aufgabe und eines der wichtigsten Unternehmensrisiken, die es zu steuern gilt, begreifen. Firmennetzwerke sind noch immer häufig viel zu schlecht abgesichert, die wachsende Vernetzung von Industrie und Gesellschaft sowie die steigende Verwundbarkeit von Legacy-Systemen kritischer Infrastrukturen durch immer mehr Schnittstellen ins Internet sind beste Voraussetzungen dafür, dass uns richtig große Cyberattacken erst noch bevorstehen – und zwar gerade auch und gerade durch KI in den falschen Händen, die durch automatisierte oder gar autonome Prozesse mögliche Auswirkungen noch potenzieren kann.

IT-Sicherheit weder strategisch noch operativ vernachlässigen

Angesichts dieser komplexen Bedrohungslage sollte jedes datenverarbeitende Unternehmen ein ISMS implementieren, konsequent anwenden, regelmäßig fortschreiben und überprüfen, das empfiehlt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI), die nationale Cybersicherheitsbehörde. Ein ISMS steigert die Resilienz gegenüber Cyberangriffen, senkt Kosten und schafft Vertrauen in die eigene Marke. Zeitgemäße Frameworks für IT-Sicherheit sind die 2018 modernisierten BSI-Standards zusammen mit dem IT-Grundschutz-Kompendium. Der IT-Grundschutz ist bereits seit 2006 offiziell zur Erfüllung der ISO/IEC 27001 Norm an¬erkannt. Diese internationale Industrienorm beschreibt sehr detailliert und für ver¬schiedene Branchen, wie Unternehmen ihre IT-Infrastruktur und ihre digitalen Assets besser schützen können, wie die Sicherheitsanforderungen an Nutzung und Einrichtung von IT-Hard- und Software-Systemen, Betriebssteuerung, Wartung und die fortlaufende Verbesserung eines ISMS gestaltet sein sollten. Darüber hinaus fordert die Norm eine lückenlose Dokumentation aller Maßnah¬men und regelmäßige Überprüfungen. Erfasst und beurteilt werden müssen auch Sicherheitsrisiken sowie die angemessenen Maßnahmen, mit denen das Unternehmen diese Risiken zu behandeln gedenkt. Spätestens hier sind menschlicher Sachverstand und Expertise erforderlich, um fortlaufend Risiken zu identifizieren und zu bewerten.

Ein ISMS basiert auf einen ständig sich wiederholenden und damit nie endenden Prozess, bei dem sich Teilaufgaben auf allen Stufen und die Auswertung durch maschinelles Lernen und andere KI-Methoden ergänzen lassen. KI spielt immer dann ihre Potenziale aus, wenn es um die Analyse großer Datenbestände geht und diese segmentiert, gruppiert und bewertet werden müssen. Bei der Analyse von Netzplänen und Dokumentationen kann sie via Bildauswertung, Text und Data Mining die Strukturanalyse beschleunigen und absichern. Bei der Feststellung des Schutzbedarfs kann sie kontextbezogen Vererbungsregeln überprüfen sowie Optimierungsvorschläge durch inkrementelles Vorgehen bei IT-Systemen erarbeiten, die sich ständig verändern. Auch bei der Modellierung, Maßnahmen-Checks und der eigentlichen Risikoanalyse kann sie die Sicherheitsexperten bei zahlreichen Routinen unterstützen.

All diese Vorteile dürfen aber nicht dazu verleiten, sich zurückzulehnen und die IT-Sicherheit strategisch wie operativ zu vernachlässigen. Wichtig ist auch, dass KI-gestützte (Sicherheits-)

Severin Rast, Mitglied der Geschäftsleitung, infodas GmbH

Systeme und -anwendungen im ISMS berücksichtigt werden, um ebenfalls angemessen abgesichert werden zu können. Sinnvoll sind hierbei integrierte Konzepte, die mehrere Schichten von Sicherheit kombinieren und einzelne technologische Lösungen gegenseitig absichern.

ISMS – nicht nur Technik, sondern auch menschliche Intelligenz

Aber: Eine wirksame Cybersecurity-Strategie kann nicht allein auf technischen Lösungen basieren. IT-Sicherheit bleibt eine Managementaufgabe für CIOs und CISOs, die mit einem ISMS eine ganzheitliche Strategie verfolgen sollten. KI-basierte Technologien und menschliche Intelligenz müssen dabei sinnvoll und gegenseitig ergänzend arbeiten. Und dies geht nur mit „Security by Design“: Die Anwendung dieses Prinzips bedeutet einerseits, bei neuen Lösungen immer die Sicherheit mitzudenken und andererseits bestehende IT-Infrastruktur und die eingesetzte Hard- und Software im Zuge jeder Ersatzbeschaffung darauf hin zu analysieren, welche Schwachstellen neue Systeme nicht mehr enthalten sollen. So können auch bestehende operative Architekturen sukzessive erneuert und sicherer gemacht werden. Security by Design muss vor allem bei der Anwendungsentwicklung ein fester Bestandteil des Entwicklungsprozesses sein. Es reicht einfach nicht, die Programmierer im einsamen Kämmerlein coden zu lassen. IT-Sicherheitsexperten müssen in die Teams integriert sein und jeden Sprint auf seine Sicherheitsrelevanz abklopfen. Im Bereich der Anwendungsentwicklung beispielsweise sollten sie Regeln für den OSB-Einsatz aufstellen. Sie müssen deren Einhaltung überwachen und Tests entwickeln, um auch im laufenden Betrieb einer Anwendung neue Schwachstellen (Security by Default) sofort erkennen und abstellen zu können. Gleiches gilt für eine KI, deren Selbstlernprozesse sich nur durch regelmäßige Tests nachvollziehen lassen. Dazu brauchen Unternehmen KI-Experten, die nicht nur den Ausgangscode für eine KI und deren KNN schreiben können, sondern auch in der Lage sind, die Risiken möglicher Black Boxes zu erkennen und zu bewerten.

„Security by Design“ sollte auch im Kontext eines ISMS Anwendung finden und betrifft sowohl die Architektur der IT-Infrastruktur als auch die Anwendungsentwicklung und mündet zwangsläufig in einer kontinuierlichen Überprüfung der gesamten IT.

Natürlich kann kein Unternehmen seine IT von heute auf morgen völlig neu planen.

Grundsätzlich müssen Organisationen ihre Systeme weiterhin auf dem Stand der technischen Entwicklung halten und im Rahmen eines ISMS mit geeigneten Maßnahmen wiederkehrend auf neue Schwachstellen beziehungsweise mögliche Angriffsvektoren überprüfen. Dies gilt insbesondere für neue Technologien wie KI. Die Implementierung von umfassenden, aktuellen Gefährdungen adressierenden Cybersecurity-Maßnahmen muss zur Regel werden. Darüber hinaus sind Anpassungen der einschlägigen Industrienormen und BSI-Standards wünschenswert: Der IT-Grundschutz würde beispielsweise von entsprechenden Bausteinen und Anforderungen mit KI-Bezug profitieren, um den KI-Einsatz sicherer zu managen. Für die ISO 27001 wäre es Zeit zu prüfen, welche Controls sich wie auf KI-Systeme und -Verfahren anwenden lassen oder ob es erforderlich wäre, neue Controls zu erarbeiten. Ähnliches gilt für andere Best Practises und Frameworks.

Heute die Herausforderungen von morgen vor Augen haben

Eine weitere Voraussetzung für die professionelle Steuerung der Informationssicherheit ist das richtige Mindset der Geschäftsfüh¬rung. Nur wenn Cybersecurity eine angemessen hohe oder sogar sehr hohe Priorität eingeräumt wird, lassen sich geschäftskritische IT-Prozesse und Assets im Zuge der fortschreitenden Digitalisierung wirklich schützen. Darüber hinaus liegt der Erfolg einer wirksamen Umsetzung von Cybersecurity und ISMS heute auch in interdisziplinären Teams aus IT-Sicherheitsexperten, die fachlich auf der Höhe der Zeit sind und die Herausforderungen von morgen vor Augen haben. Dafür braucht es

Experten für KI, die programmieren und steuern können und IT-Forensiker, die in der Lage sind, wie Cyber-Kriminelle zu agieren, um offene Flanken zu ermitteln. Ist fachkundiges Personal nicht verfügbar, sollten Unternehmen auf Managed Services, kompetente Dienstleister oder auf interne Weiterbildung setzen – oder am besten gleich auf eine geeignete Kombination. Darüber hinaus bleiben – trotz oder vielleicht gerade wegen innovativer Technologien – „analoge“ Faktoren wie eine Sicherheitskultur, die alle Ebenen der Organisation umfasst, und eine hohe Mitarbeiter-Awareness nach wie vor ein wichtiges Fundament für ein erfolgreiches, nachhaltiges ISMS.

Severin Rast

Referenzen: **[1]** https://www.crisp-research.com/publication/security-design-die-rolle-von-it-sicherheitsstrategien-der-digitalisierung/

Zero Trust macht Schluss mit dem Urvertrauen in den Anwender

Im Security-Bereich hat sich Zero Trust als Buzz-Word etabliert. Bereits vor 10 Jahren als neues Sicherheitskonzept aus der Taufe gehoben, gibt es mittlerweile auch die erforderliche Technologie. Die neuen Lösungsansätze räumen auf mit dem grenzenlosen Vertrauen in den Anwender hinsichtlich des sicheren Zugriffs auf Unternehmensanwendungen in der Cloud oder im Netzwerk. Doch was verbirgt sich hinter Zero Trust?

Ein Zero Trust basierter Ansatz sorgt für die nahtlose und sichere Anbindung eines Anwenders an seine Applikation, unabhängig davon, wo diese vorgehalten wird. Entscheidend dabei ist, dass der Anwender nicht mehr auf das Unternehmensnetz zugreifen muss und die Anwendungen nicht mehr dem Internet ausgesetzt werden. Dieses Sicherheitsmodell verbindet den Nutzer mit seiner benötigten Applikation, ohne dabei auf die IP-Adresse angewiesen zu sein.

IP-Adressen wurden ursprünglich mit der ungebrochenen Konnektivität als Ziel vor Augen entwickelt. Aus Gründen der Sicherheit stellen diese Adressen allerdings das schwächste Glied in der Abwehrkette dar. Die Schwierigkeit rührt daher, dass die Standardeinstellung sofort den Zugriff erlauben, und damit ein Urvertrauen in den Anwender gesetzt wird, das aufgrund der damit einhergehenden Sicherheitsrisiken nicht mehr angebracht ist. In einem ersten Schritt haben Unternehmen mit der Einführung einer Demarkationslinie zwischen dem offenen Internet und dem Unternehmensnetz in Form von Firewalls reagiert. Angetrieben durch die Cloudification und die Mitarbeiter-Mobilität bietet diese Sicherheitsinfrastruktur heute allerdings keinen ausreichenden Schutz mehr.

Netzwerk-Zugriff macht verwundbar

Eine Analogie soll das Bedrohungspotenzial des Netzwerk-zentrierten Modells verdeutlichen. Erhält ein Mitarbeiter Zugang zum Netzwerk, so ist das vergleichbar mit folgendem Bild: der vertrauenswürdige Nutzer steht inmitten einer Straße und kann rund um sich herum Häuser sehen, die sinnbildlich für Anwendungen stehen, also Gebäude (Rechenzentren) und Innenhöfe, sowie andere Straßen (Netzwerke). Der Anwender kann die Straße entlanggehen und dort an Türen klopfen (Ports) und versuchen diese zu öffnen und einzutreten. Dieses Modell geht davon aus, dass jeder Anwender auf der Straße vertrauenswürdig ist und ihm damit die Berechtigung zum Zutritt zu den Häusern eingeräumt wird – also den Anwendungen. Durch ein solches Modell des grenzenlosen Vertrauens entsteht eine große Angriffsfläche innerhalb des Netzwerks und Unternehmen finden sich der Gefahr ausgesetzt, dass auf ihr geistiges Eigentum von jedermann zugegriffen werden kann, der einmal Eingang ins Netzwerk erhalten hat – inklusive Hackern.

Deshalb wurden in diesem Modell die Türen mit Schlössern versehen (Passwörter) und zu deren Schutz zusätzlich ein System an Zäunen, Hecken, Wällen und Eingangstoren rund um die Gebäude errichtet (Firewalls, ACLs, etc.). Wenn die Zäune zu alt und damit morsch waren, wurden sie durch neue, höhere Zäune ersetzt. Somit war es schwieriger, in die Gebäude einzudringen. Allerdings blieb der Einblick durch die Fenster unverwehrt und alle Häuser und Gebäude waren für den Anwender auf der Straße sichtbar.

Nathan Howe, ZPA Principal Architect, Zscaler Germany GmbH

Zero Trust: Was nicht sichtbar ist, das ist nicht angreifbar

In einem idealen, an der Sicherheit orientierten Szenario bleibt nicht nur der Einblick durch das Fenster verwehrt, sondern sogar der Blick auf das gesamte Gebäude. Denn was ein Hacker nicht sehen kann, ist auch nicht durch ihn angreifbar. Somit lässt sich die heutige Anforderung an den Netzwerkzugriff neu definieren: Wenn der Anwender nicht mehr von vorne herein als vertrauenswürdig eingestuft wird und auf die Straße gelangen darf, muss der Netzwerk-zentrierte Ansatz durch einen neuen abgelöst werden.

Hier kommt Zero Trust Network Access (ZTNA) ins Spiel. Der auf Vertrauen basierte Ansatz wird in diesem Modell durch einen Anwender- oder Anwendungs-zentrierten Ansatz ersetzt. Wird der Zugriff von der Netzwerkebene abstrahiert, kann der Besucher die Häuser und Gebäude entlang der Straße nicht mehr einsehen. Der Zutritt wird ihm verwehrt, solange der Anwender nicht autorisiert ist. Erst wenn der Besucher durch Autorisierung die Erlaubnis zum Betreten eines Hauses oder Gebäudes erhält, öffnen sich für ihn auch die Türen zu den erlaubten Anwendungen.

Die Cloud macht Zero Trust-Ansätze möglich

Heute ist der Zero Trust-Ansatz keine Theorie mehr. Die Cloud und das damit verbundene Abwandern von Anwendungen in extern aufgesetzte Umgebungen machen Zero-Trust-Lösungen nicht nur erforderlich, sondern endlich möglich. Denn wenn Anwendungen und Daten in die Cloud umziehen und damit das Firmennetzwerk verlassen, greifen die alten Sicherheitsmodelle nicht mehr. Zero Trust Network Access, auch bekannt als Software-definierter-Perimeter, bietet einen Lösungsansatz, bei dem der Anwender nicht mehr

mit dem Netzwerk, sondern lediglich mit seiner Anwendung verbunden wird.

Die Sicherheitsanforderung wandelt sich damit von einem IP- und Port-definierten Ansatz dahingehend, dass der Anwender und seine Applikation in den Mittelpunkt treten. Dadurch wird dem CARTA-Rahmenwerk von Gartner Rechnung getragen, das einen Kontext-basierten Ansatz fordert. Es gibt Unternehmen die Kontrolle über die Aktivitäten der Anwender zurück. Die Cloud, nicht die herkömmliche Sicherheits-Hardware, ermöglicht das. Ein kontinuierliches Monitoring und Risikoassessment wird mit Hilfe einer Cloud-basierten Sicherheitsplattform eingeführt, die Anwendungen mit autorisierten Nutzern für die Dauer ihrer Sitzung verknüpft.

Wegen eines Zero-Trust-Ansatzes gehört das Urvertrauen beim Netzwerkzugriff der Vergangenheit an. Unternehmen, die auf Multi-Cloud oder hybride IT-Umgebungen setzen, werden nicht um dieses moderne Sicherheitskonzept herumkommen. Denn ihre mobilen Mitarbeiter und Partner haben den klassischen Firmen-Perimeter längst verlassen und greifen von außerhalb auf die Applikationen zu. Diesem Trend muss die IT-Sicherheit folgen.

Nathan Howe

Francois Lasnier, Vice President, Identity & Access Management Products, Thales

Die Gräben zwischen Zero Trust-Frameworks und IAM schließen

Viele Unternehmen stehen in Bezug auf ihre digitalen Sicherheitsstrategien an einem Scheideweg. Auf der einen Seite steigen die Kosten im Zusammenhang mit digitalen Kriminalitäts- und Sicherheitsvorfällen. Cybersecurity Ventures fand in seinem offiziellen jährlichen Cyberkriminalitätsbericht 2017 heraus, dass Schäden durch Cybercrime die Welt bis 2021 sechs Billionen Dollar kosten werden. Ein Jahr später entdeckte das Ponemon Institute in seiner Cost of a Data Breach Study 2018, dass die durchschnittliche Datenschutzverletzung nun 3,86 Millionen Dollar kostet, was einem Anstieg von 6,4 Prozent gegenüber dem Vorjahr entspricht.

Auf der anderen Seite geben Unternehmen mehr Geld denn je für ihre Bemühungen um digitale Sicherheit aus. Gartner schätzte, dass die weltweiten Ausgaben für Informationssicherheit im Jahr 2018 114 Milliarden US-Dollar übersteigen würden – ein Anstieg von 12,4 Prozent gegenüber 2017. Das Forschungs- und Beratungsunternehmen prognostizierte weiterhin, dass diese weltweiten Ausgaben 2019 um 8,7 Prozent auf 124 Milliarden Dollar steigen würden. In seinem jährlichen Aktionärsbrief sagte JPMorgan Chase CEO Jamie Dimon, dass man im vergangenen Jahr 600 Millionen Dollar für Cybersicherheit ausgegeben hat und mehr als 3.000 Mitarbeiter für Sicherheit und den Schutz von Kundendaten einsetzt.

Sicherheitsmodelle dem Stand der Technik anpassen

Was sollen Organisationen tun? Klar ist: Sie können sich nicht auf das klassische Netzwerkperimetermodell verlassen. Wie von Identity Automation erwähnt, haben IT-Teams diesen Ansatz entwickelt, als die Mitarbeiter noch mit den Unternehmenssystemen verbunden waren, während sie an ihrem Schreibtisch in den Firmenbüros saßen. Mit dem Anstieg der Anzahl der Remote-Benutzer ging der Fokus in Richtung Absicherung des Netzwerkverkehrs von Nutzern, die sich mit lokalen Unternehmenssystemen verbinden.

Heutzutage verfügen Unternehmen über hochmobile Mitarbeiter, die sich von überall auf der Welt aus mit dem Netzwerk verbinden. Sie nutzen nun immer mehr Cloud-basierte Assets, Systeme mit sensiblen Kundeninformationen sowie Anbieter und Lieferanten, die einen ebenfalls Netzwerkzugang benötigen. Es gibt einfach zu viele Quellen für den Netzwerkzugriff, als dass das klassische Perimeter-Modell funktionieren könnte.

Einige Organisationen versuchen, diese Herausforderung zu meistern, indem sie einen Perimeter aufrechtzuerhalten und den gesamten Netzwerkverkehr über einen Proxy (WAM oder traditionelle Netzwerksicherheitsgeräte) zu leiten, aber dieses Modell kann nicht einfach skaliert werden, wirkt sich negativ auf die Benutzerfreundlichkeit (Netzwerklatenz) aus und untergräbt die grundlegenden Vorteile der Cloud: Sie sind nicht immer verfügbar.

Warum sollte man also den gesamten Traffic, einschließlich Remote-Benutzer, an einen lokalen Proxy weiterleiten, der abstürzen kann, um Mitarbeiter an der Arbeit zu hindern, wenn es bereits effizientere und sicherere Lösungen gibt?

Aus diesem Grund wenden sich Organisationen zunehmend an die Zero Trust Mentalität „Verify everything, trust nothing“. Diese Perspektive verwirft die Vorstellung, dass interne Benutzer und Geräte automatisch vertrauenswürdig sind. Stattdessen werden alle Devices, Netzwerkinfrastrukturen und Benutzer standardmäßig als nicht vertrauenswürdig behandelt.

Wo IAM eingesetzt wird

Dieses Denkmodell ist ohne Identitäts- und Zugriffsmanagement (IAM) nicht möglich. Denn Zero Trust dreht sich um die verschiedenen Identitätsaspekte eines jeden Users. Laut Microsoft erfordert eine Zero Trust-Denkweise in erster Linie, dass Sicherheitsteams die Identität jedes Benutzers ermitteln; nur dann können sie mit Hilfe von Multi-Faktor-Authentifizierung und anderen zentralen IAM-Komponenten überprüfen, ob jeder Benutzer eine High-Assurance-Sitzung hat, einen gültigen Computer verwendet und auf die entsprechenden Arten von Dateifreigaben zugreift.

Mit Blick auf die Zukunft wird IAM eine noch bedeutendere Säule der Zero Trust-Strategien von Unternehmen werden. Drei aufkommende IAM-Trends zeigen diese Entwicklung auf:

- IAM wird die Zero Trust-Frameworks schrittweise in den Kontext stellen: IAM-Lösungen der Zukunft werden eine stärkere Integration zur Einbettung von Identitätsdaten in Datensicherungs- und netzwerkforensische Systeme nutzen. Auf diese Weise können Sicherheitsteams Datenbestände und Informationspakete mit bestimmten Benutzern im Unternehmensnetzwerk verknüpfen.
- IAM-Architekturen werden zunehmend die Datenidentität nutzen: Im Allgemeinen werden mehr IAM-Produkte es den Sicherheitsteams ermöglichen, Identitätsdaten zu verwalten und mit den Zugriffsrechten der Mitarbeiter zu verknüpfen. Zur Vorbereitung sollten die Sicherheitsteams den Mitarbeitern Datenzugriffsrechte zuweisen und Datenbestände in alle Kampagnen zur Zugangszertifizierung einbeziehen.
- IAM-Suiten werden zu losen, vorintegrierten Angeboten: Klassische IAM-Suiten, bei denen Kunden alles installieren müssen, weichen immer mehr API-basierten Microservices. Von den Zero Trust-Anbietern wird erwartet, dass sie diesen sich weiterentwickelnden Ansatz für IAM übernehmen. Auf diese Weise tragen sie dazu bei, die Last der Implementierung von IAM für viele Unternehmen zu verringern, die sich einer Zero Trust Denkweise anschließen.

In Anerkennung der oben genannten Diskussion ist jetzt der perfekte Zeitpunkt für Unternehmen, um die Einführung einer Zero Trust Denkweise in Betracht zu ziehen. Kernelemente sind dabei Multifaktor-Authentifizierung und Access Management.

Francois Lasnier

Maschinenidentitäten sind im Darknet wichtiger als digitale Identitäten oder Ransomware

Digitale Zertifikate sind unter Cyberkriminellen begehrt, jedoch ist es neu, dass sie sogar größere Umsätze erzielen und im Darknet einfacher zu finden sind als Ransomware-Kampagnen.

Maschinenidentitäten wie digitale Zertifikate und kryptographische Schlüssel sind und werden auch weiterhin die Grundlage für das Vertrauen zwischen Maschinen im Internet sein. In den vergangenen Jahren konnten vermehrt Angriffe mit gefälschten Zertifikaten ausgemacht werden. Der Missbrauch nimmt zu und auch die Möglichkeiten diese zu nutzen. Das Risiko Opfer eines Cyberangriffs zu werden, steigt zum einen mit der Anzahl der im Unternehmen oder der Organisation verwendeten Zertifikate exponentiell, zum anderen aber auch, weil immer mehr Cyberkriminelle hier investieren. Doch auch Fehler schleichen sich immer wieder ein und gefährden Unternehmen. Ein schwerwiegender Betriebsfehler bei GoDaddy, Apple und Google hat erst jüngst zur Ausgabe von mindestens einer Million browsergesicherten digitalen Zertifikaten geführt, die nicht den verbindlichen Branchenvorschriften entsprechen. IT-Sicherheitsverantwortliche müssen nun aufräumen und die zurückgerufenen Zertifikate mühsam manuell ersetzen, wenn sie keine Automatismen implementiert haben. Die Anzahl der nichtkonformen Zertifikate könnte sogar doppelt so hoch sein wie die Anzahl der Zertifikate, und es ist wahrscheinlich, dass auch andere vertrauenswürdige Zertifizierungsstellen betroffen sind.

Im Jahr 2018 wurde über 70 Prozent des Internetverkehrs verschlüsselt. IT-Experten gehen davon aus, dass die Zahl dieses Jahr auf 80 Prozent steigen wird. Zur Verschlüsselung sind die beiden Zertifikate Secure Sockets Layer (SSL, ein älterer Standard) und Transport Layer Security (TLS, ein neuerer Standard) unerlässlich. Sie autorisieren die gesamte verschlüsselte Kommunikation zwischen den Maschinen. SSL/TLS-Zertifikate sind deshalb entscheidend für den Schutz der Privatsphäre und die Verbesserung der IT-Sicherheit, indem sie jeder Maschine eine eindeutige Maschinenidentität geben. Sie steuern den Verkehr sensibler Daten an autorisierte Maschinen und werden in allen Bereichen eingesetzt, von Website-Transaktionen, Cloud-Umgebungen, DevOps und mobilen Geräten bis hin zu Smart City-Initiativen, Robotern, Algorithmen im Bereich der künstlichen Intelligenz und Containern in der Cloud.

In einer gemeinsamen Untersuchung der

Kevin Bocek, VP Security Strategy & Threat Intelligence, Venafi Inc.

Evidence-based Cybersecurity Research Group an der Andrew Young School of Policy Studies der Georgia State University sowie der University of Surrey im Jahr 2019 wurden blühende Marktplätze für TLS-Zertifikate aufgedeckt. Auf den Schwarzmärkten Dream Market, Wall Street Market, BlockBooth, Nightmare Market and Galaxy3 werden einzelne Zertifikate verkauft und mit einer breiten Palette von cyberkriminellen Services angeboten. Zusammen bieten diese Dienste Maschinenidentitäten als Service für Cyberkriminelle, beispielsweise um Websites zu fälschen, in verschlüsselten Datenverkehr zu lauschen, Man-in-the-Middle-Angriffe durchführen und sensible Daten zu stehlen.

TLS-Zertifikate öfter angeboten als Ransomware

Die Recherche über diese fünf Marktplätze ergab 2.943 Erwähnungen für „SSL“ und 75 für „TLS“. Im Vergleich dazu gab es nur 531 Erwähnungen für „Ransomware“ und 161 für „Zero Day“. Es zeigte sich auch, dass sich einige Marktplätze – wie Dream Market – auf den Verkauf von TLS-Zertifikaten zu spezialisieren scheinen und Maschinenidentität-as-a-Service-Produkte anbieten. Darüber hinaus fanden Forscher heraus, dass Zertifikate oft mit anderen Services von Cyberkriminellen, einschließlich Ransomware, kombiniert und angeboten werden.

Die Preise für Zertifikate variieren im Darknet zwischen 260 und 1.600 US-Dollar, je nach Art des angebotenen Zertifikats und dem Umfang der zusätzlichen Dienstleistungen. Die aufgerufenen Preise verdeutlichen, dass die Maschinenidentitäten wichtiger sind, als beispielsweise digitale Identitäten. Die Forscher haben nun auch erstmals erweiterte Validierungszertifikate (Extended-Validation EV-Zertifikate) gefunden, die mit Diensten zur Unterstützung bösartiger Websites wie Google-indexierte „alte“ Domains, After-Sale-Support, Webdesign-Services und die Integration mit einer Reihe von Zahlungsabwicklern – einschließlich Stripe, PayPal und Square – ausgestattet sind. Mindestens ein Anbieter auf BlockBooth verspricht darüber hinaus, Zertifikate von renommierten Zertifizierungsstellen zusammen mit gefälschten Firmenunterlagen – einschließlich Data Universal Numbering System (DUNS)-Nummern – auszustellen. Dieses Paket von Produkten und Dienstleistungen ermöglicht es Angreifern, sich für weniger als 2.000 US-Dollar glaubwürdig als vertrauenswürdiges US- oder britisches Unternehmen zu präsentieren.

SSL- und TLS-Zertifikate, die von vertrauenswürdigen Zertifizierungsstellen ausgestellt werden, dienen als Maschinenidentitäten und gewährleisten eine vertrauliche Kommunikation zwischen Servern und Clients. Vor der Ausstellung dieser Zertifikate, insbesondere vor der Ausstellung von Extended-Validation (EV)-Zertifikaten, sind die Zertifizierungsstellen verpflichtet, einen strengen Satz von Validierungsdaten des Antragstellers zur Überprüfung ihrer Identität zu verwenden. Eingesetzt werden die Zertifikate vor allem, um Webanwendungen mit HTTPS abzusichern. Eingesetzt werden sie zumeist beim Online-Banking, um Phishing-Angriffe zu vermeiden. Obwohl frühere Untersuchungen Möglichkeiten zur Erkennung gefälschter SSL- und TLS-Zertifikate sowie deren Nutzung zur Generierung von Angriffen vorgeschlagen haben, gab es bislang keine wissenschaftlichen Beweise für gefälschte und gestohlene Zertifikatsmärkte im Darknet. Die Ergebnisse der Untersuchung belegen daher die Existenz eines Online-Untergrundmarktes für TLS-Zertifikate. Besonders interessant sind Anbieter auf Online-Untergrundmärkten, die versprechen, EV-Zertifikate für US-amerikanische und britische Unternehmen für weniger als 2.000 US-Dollar auszustellen. Allerdings scheint es einfacher zu sein, solche Zertifikate und verbundene Services für US-amerikanische Firmen, wenn für britische Firmen bereitzustellen.

Forschungsdesign und Methodik

Um die Forschungsziele zu erreichen, tauchten die Forscher in Online-Märkte und Hackerforen ein, die von Oktober 2018 bis Januar 2019 im Tor-Netzwerk, I2P und Freenet aktiv waren, und suchten nach „zum Verkauf stehenden“ Anzeigen von kompromittierten und gefälschten TLS-Zertifikaten. Während dieser Zeit führte das Forschungsteam 16 wöchentliche Recherchen durch und entdeckte fast 60 relevante Online-Markt-Webseiten auf Tor und 17 Webseiten auf I2P. Die Forscher überprüften die Angebote im Detail und führten in einigen Fällen Gespräche mit den Verkäufern, um ein besseres Verständnis der zu verkaufenden Waren und Dienstleistungen zu erlangen.

Fazit

Die Recherche zeigt zweierlei auf, zum einen, dass sich Cyberkriminelle wieder verstärkt versuchen im Verborgenen zu arbeiten und zum anderen, dass es relativ einfach auch für Laien ist, diese Zertifikate zu kaufen und die verbundenen Services zu nutzen. Maschinenidentitäten sind im Darknet eine wichtigere und heißere Ware als digitale Identitäten wie Passwörter und E-Mailadressen oder Ransomware. TLS-Zertifikate und besonders die Validierungszertifikate,

die als vertrauenswürdige Maschinenidentitäten fungieren, sind eindeutig ein wichtiger Bestandteil der Toolkits von Cyberkriminellen – genauso wie Bots, Ransomware und Spyware. In Zukunft gilt es noch viel mehr Forschungsarbeit in diesem Bereich zu leisten. Unternehmen und Organisation sollten sich jedoch schon heute darüber sorgen, dass die Zertifikate, die zur Einrichtung und Aufrechterhaltung von Vertrauen und Privatsphäre im Internet verwendet werden, nun als Darknet-Ware an Cyberkriminelle verkauft werden und das bereits heute ein florierender Markt aufgebaut wurde. Die Forschung wird das ganze Jahr über fortgeführt und die Ergebnisse unter anderem hier veröffentlicht werden.

Kevin Bocek

Maschinelle Identitäten sind die Basis des Vertrauens im Internet

Maschinenidentitäten sind die Grundlage für das Vertrauen zwischen Maschinen und deshalb auch bei Cyberkriminellen sehr begehrt.

Im Internet, in den diversen Clouds und in den Netzwerken von Unternehmen gibt es zwei Arten von Akteuren: auf der einen Seite Menschen, die Benutzernamen, Passwörter oder sogar Biometrie verwenden, um zu beweisen, wer sie sind und welche Berechtigungen sie haben. Auf der anderen Seite stehen Maschinen, die mit anderen Maschinen kommunizieren. Der Begriff der Maschine ist dabei sehr weit gefasst: Gemeint sind nicht nur Hardware und Geräte wie Server und IoT-Devices, sondern auch Applikationen und Cloud-Services bis hin zu Algorithmen und Containern – also vor allem Software.

Schlüssel und Zertifikate sorgen für Vertrauen

Statt Benutzernamen und Passwörtern kommen hier maschinelle Identitäten ins Spiel. Das sind wie beim Menschen bestimmte Merkmale, die sie voneinander unterscheiden. Eine Maschine benötigt eine Identität, um Zugriff auf bestimmte Systeme und Daten zu erhalten, Code auszuführen, Daten zu verschlüsseln oder andere Maschinen zu kontrollieren. Die Basis der maschinellen Identitäten sind digitale Zertifikate und kryptografische Schlüssel, die für jede Maschine einzigartig sind. Die Identitäten bauen das Vertrauen auf, das für eine sichere Kommunikation unerlässlich ist. Hinsichtlich der Investitionen gibt es jedoch eine frappierende Diskrepanz: Unternehmen geben jährlich mehr als 10 Milliarden US-Dollar für den Schutz und die Verwaltung von Passwörtern aus, investieren aber fast nichts in Maschinenidentitäten. Das Bewusstsein für die Bedeutung maschineller Identitäten ist noch wenig verbreitet, ebenso das Wissen, wie damit umzugehen ist.

Maschinelle Identitäten wie TLS-Schlüssel und -Zertifikate, SSH-Schlüssel und API-Schlüssel ermöglichen es, Geräte, Cloud Services und Software sicher zu authentifizieren. Mit Code-signierten Zertifikaten lassen sich zudem auch Updates identifizieren und als vertrauenswürdig einstufen, noch bevor sie bereitgestellt werden. Maschinelle Identitäten finden sich folglich in den verschiedensten Segmenten: Websites, Cloud, mobile Devices bis hin zu künstlicher Intelligenz und Robotern.

Ausfälle durch abgelaufene Zertifikate

Viele Unternehmen haben aufgrund der schieren Masse an Maschinen und Anwendern keinen Überblick darüber, welche Schlüssel und Zertifikate sich aktuell im Umlauf befinden, welche Geräte sie verwenden und wann sie ablaufen. Eine große Bank etwa kommt leicht auf eine Viertel Million maschinelle Identitäten. Anstatt auf Managementlösungen zu setzen, führen die zuständigen Sicherheitsverantwortlichen häufig noch manuelle Listen. In solchen Listen werden bei dem rasanten Zuwachs neuer Maschinen leicht Zertifikate und Schlüssel vergessen oder falsch zugeordnet. Dazu kommt: Die Zertifikate der maschinellen Identitäten haben mehrere Merkmale mit einem Personalausweis gemein: zum Beispiel das Ablaufdatum. Viele Unternehmen, die gar nicht wissen, wo welche maschinellen Identitäten vorhanden sind, werden früher oder später von abgelaufenen Zertifikaten überrascht. In einer Studie von Venafi, ein auf maschinelle Identitäten spezialisiertes Unternehmen, kam es bei fast zwei Dritteln der befragten Unternehmen dadurch zu Ausfällen, die sich auf kritische Geschäftsanwendungen ausgewirkt haben. Zudem sind zertifikatsbedingte Ausfälle sehr schwer zu diagnostizieren und zu beheben. Der Anbieter Venafi hat allein im vergangenen Jahr bei seinen Kunden im Durschnitt 57.000 unbekannte maschinelle Identitäten aufgespürt. Drei Jahre zuvor waren es noch durchschnittlich nur 15.000. Und die Zahl der Maschinen und somit der maschinellen Identitäten wächst weiter exponentiell.

Der Austausch von Zertifikaten bedeutet einen enormen Aufwand

Im Jahr 2018 hat Google sämtlichen Zertifikaten von Symantec und Tochterunternehmen wie VeriSign, Thawte und GeoTrust das Vertrauen entzogen, die folglich alle ausgetauscht werden mussten. Anderes Beispiel: Ob in fünf oder in zehn Jahren ist ungewiss, aber der Tag wird

Andreas Dumont, Freier Journalist, Büro Andreas Dumont

kommen – Quantencomputer machen auf einen Schlag die kryptografischen Schlüssel unbrauchbar, die aktuell für maschinelle Identitäten im Einsatz sind. Sie sind nicht „Quantum ready" und können von einem Quantencomputer in Windeseile geknackt werden. Wenn es soweit ist, müssen sämtliche Zertifikate, die heute existieren, erneuert werden. Eine Herkules-Aufgabe, die manuell nicht zu schaffen ist. Dazu kommen immer wieder Sicherheitslücken und Bugs wie Heartbleed vor ein paar Jahren, die ebenfalls einen Wechsel erforderlich machen. Zusammengefasst: Updates von Zertifikaten und Schlüsseln lassen sich nur mit Hilfe von automatisierten Management-Lösungen bewältigen.

Maschinelle Identitäten sind auch für die Bad Guys interessant

In den vergangenen Jahren nahmen Angriffe mit gefälschten Zertifikaten deutlich zu. Digitale Zertifikate sind inzwischen bei Hackern und Cyberkriminellen sehr begehrt. Im Darknet übertreffen Anzeigen für Maschinenidentitäten die für Ransomware-Kampagnen um den Faktor fünf. Der Hintergrund ist klar: Die Cyberkriminellen wollen mit Hilfe von gekauften Zertifikaten vertrauenswürdig erscheinen, damit angegriffene Rechner ihre Malware akzeptieren. Sogar EV-Zertifikate lassen sich inzwischen im Online-Untergrund erwerben. Diese Extended-Validation-Zertifikate gelten eigentlich als besonders sicher und vertrauenswürdig.

Eine wissenschaftliche Untersuchung hat einen florierenden Schwarzmarkt für TLS-Zertifikate aufgedeckt, die zusammen mit einer breiten Palette von cyberkriminellen Services angeboten werden – eine Art Machine-Identity-as-a-Service, um Webseiten zu fälschen, verschlüsselten Verkehr zu belauschen und sensible Daten zu stehlen. Die Preise für die Zertifikate im Darknet schwanken zwischen 260 und 1.600 US-Dollar, je nach Art des angebotenen Zertifikats und den zusätzlichen Dienstleistungen. Die Preise verdeutlichen, dass Maschinenidentitäten inzwischen wichtiger und lukrativer sind als digitale Identitäten wie E-Mailadressen und Passwörter. Und nicht zuletzt sind auch Nationen und deren Geheimdienste daran interessiert, maschinelle Identitäten zu kontrollieren.

Andreas Dumont

2.3 THREADS

Cryptojacking als ernstzunehmende Warnung

Bitcoin, Monero und Ethereum geben selbst Experten immer wieder Rätsel auf. Der Wert der Kryptowährungen steigt und fällt – es bleibt spannend, auch für Kriminelle, die sich mithilfe von Cryptojacking an dem neuen Zahlungssystem bereichern. Dazu kapern sie mithilfe von Malware Rechenleistung zum Schürfen von Bitcoin & Co. Die Gefahr für Unternehmen liegt jedoch beim Cryptojacking vor allem darin, welche anderen Möglichkeiten sich Hackern eröffnen, wenn sie erst einmal Zugang zum Netzwerk haben. Wie können Unternehmen das illegale Cryptomining in ihren Systemen erkennen und im besten Fall verhindern?

Seitdem der Bitcoin 2018 abstürzte und andere Kryptowährungen wie Monero, Ethereum, Dash, Litecoin oder ZCash an der Börse mit nach unten riss, ist Cryptojacking im Vergleich der häufigsten Cyberbedrohungen abgerutscht. Ransomware hat sich den Spitzenplatz zurückerobert. Diese Einschätzung stützt sich unter anderem auf den Annual Security Report des Cyber-Security-Anbieters SecureLink.

In diese Argumentation passt das im März verkündete Aus von Coinhive. Diese legale Plattform stellte ein Javascript zur Verfügung, das Betreiber von Websites in ihren Internetauftritt einbauen konnten, um die Kryptowährung Monero zu schürfen. Ein Website-Besucher musste dem Mining zustimmen. Hacker implementierten jedoch manipulierte Coinhive-Skripte in fremde Webseiten, welche ohne Wissen und Zustimmung der Website-Besucher im Hintergrund Moneros abbauten. Der Gewinn floss in die Taschen der Kriminellen. Nun ist zu erwarten, dass Kriminelle auf andere Plattformen ausweichen, insbesondere auf CoinImp oder Crypto-Loot. Das browserbasierte Cryptojacking bleibt somit auch ohne Coinhive eine reale Gefahr und ein lukratives Geschäft.

Darauf deutet auch die aktuelle Entwicklung der Kryptowährungen hin. So kostet der Bitcoin aktuell über 11.000 US-Dollar. Zum Vergleich: Die bekannteste Kryptowährung notierte zu Jahresanfang noch bei 3.300 US-Dollar. Auch wenn dies noch weit vom Höchstwert von 20.000 US-Dollar im Dezember 2017 entfernt ist, zeigt sich ein Aufwärtstrend.

Hinzu kommt, dass Cryptomining für Kriminelle selbst bei niedrigen Kursen eine kontinuierliche Einnahmequelle ist, sofern sie genügend Schürfer für sich arbeiten lassen. Daher sind Unternehmen gut beraten, sich mit Cryptojacking und

etwaigen Schutzmaßnahmen zu beschäftigen

Die zweite illegale Mining-Variante
Hacker schleusen nicht nur Mining-Skripte in den Code von Websites ein, sondern installieren über Malware-Attacken auch Software auf den Computern von Betroffenen. Beim ersten Szenario endet das kriminelle Schürfen, wenn ein Browser-Nutzer seine Sitzung schließt. Die eigene Technik nimmt keinen Schaden. Als Prävention empfiehlt es sich, einen Adblocker zu installieren. Dieser verhindert das Einblenden von Anzeigen, die mit einem Mining-Javascript präpariert sein könnten. Zudem lässt sich das Aufrufen gefährlicher Webadressen über die Browser-Einstellung via Blacklisting verhindern.

Für die zweite, gefährlichere Variante nutzen Kriminelle Sicherheitslücken, um das Mining-Skript auf Webservern, Routern oder in Content-Management-Systemen einzupflanzen. In der Folge wird das Skript an alle Webseiten weiterverteilt, die durch diese Systeme fließen. Erschwerend kommt hinzu, dass die Hacker damit in das System eindringen. Sie können zum Beispiel Botnetze aufbauen und für DDoS-Attacken, Spam-Kampagnen oder Klick-Betrug weitervermieten. Ein weiterer Verbreitungsweg für das Skript sind präparierte Apps, sowohl für PCs als auch für mobile Endgeräte. Erst kürzlich beispielsweise hat Microsoft acht Applikationen aus dem Windows Store entfernt, weil sie mit Cryptojacking-Malware infiziert waren.

Ressourcenklau in der Cloud
Richtig teuer kann es werden, wenn Hacker über Cloud-Infrastrukturen auf nahezu unbegrenzte Rechenleistung zugreifen. So war der Autohersteller Tesla Anfang 2018 Ziel eines Cryptojacking-Angriffes, der die AWS-Infrastruktur des Unternehmens mit Mining-Malware infiltrierte. Als Eingangstor nutzten die Kriminellen Kubernetes-Administrationskonsolen, die öffentlich über das Internet ohne Passwortschutz zugänglich waren. Das ergab ein Bericht der Sicherheitsspezialisten von RedLock Cloud Security, die den Vorfall entdeckten.

Befallene Systeme werden langsamer, sind stärker ausgelastet und verbrauchen mehr Strom, was an dem aufwendigen Rechnen für das Schürfen liegt. Beim Erkennen solcher Vorfälle hilft deshalb eine Network-Monitoring-Lösung. Sie zeigt sowohl Auffälligkeiten in der Systemauslastung als auch verdächtige Netzwerkkommunikation auf, etwa weil Cryptojacking-Malware ihre Rechenaufgaben von einer Mining-Plattform erhält und ihre Resultate an diese schickt. Zur Erfassung von Anomalien tragen zudem Intrusion-Detection-Systeme (IDS) oder ein Security Information and Event Management (SIEM) bei.

Wie ein Proxy schützt
Präventiv können sich Unternehmen mit einer Enterprise-Proxy-Lösung wappnen, die gefährliche URLs zentral für alle Rechner im Netzwerk blockiert. Darüber hinaus bietet diese Log-Monitoring, Virenscanning sowie Sandboxing und filtert in machen Ausführungen Javascript heraus. Für den SSL-verschlüsselten (Secure Socket Layer) Webtraffic sollten Unternehmen eine SSL Inspection einrichten. Der Proxy entschlüsselt eingehende Daten, prüft diese und verschlüsselt sie vor der Weitergabe wieder. Sicherheitsverantwortliche sollten zusätzlich über Mobile Device Management (MDM) die Funktionen von Smartphones oder Tablets steuern oder einschränken. Ein zwischengeschalteter Proxy kann den Zugang zu privaten, nicht sicheren E-Mail-Accounts blockieren oder ein Installieren von Apps verhindern, die nicht freigegeben sind.

Neuer Trend: Formjacking
Wer sich nicht vor Mining-Malware schützt, ist auch durch andere Schadsoftware verwundbar. Derzeit zeichnet sich bereits ein neuer Trend ab: das sogenannte Formjacking. Die Kriminellen dringen über Webserver und Content-Management-Systeme ein, also über Server-Strukturen. Sie implantieren ein Javascript in Webseiten, das Daten aus Formularen abgreift. Gibt ein Kunde zum Beispiel seine Zahlungsinformationen ein und klickt auf den „Absenden"-Button, wird eine Kopie seiner Daten an den Hacker übermittelt, der sie dann selbst nutzen oder im Darknet weiterverkaufen kann. Formjacking ist an sich kein neues Phänomen. Im August und September 2018 hat der Sicherheitsspezialist Symantec aber einen erheblichen Anstieg solcher Angriffe verzeichnet.

Den unbemerkten Kontrollverlust vor Augen
Cryptojacking-Malware tarnt sich schlau und hat meist keine gravierenden Folgen, weshalb viele Vorfälle unbemerkt bleiben. Unternehmen sollten die Gefahr jedoch trotzdem ernst nehmen, aufmerksam auf Anzeichen achten und ihre Sicherheitsvorkehrungen überprüfen. Denn selbst wenn es sich um eine „Malware light" handelt, geht es dennoch um eine erfolgreiche Attacke, die auf Sicherheitslücken hindeutet. Auch andere Angreifer können diese Schwachstellen ausnutzen. Wenn es Hackern gelingt, ein System mit einer Cryptojacking-Malware zu infizieren, können sie unbemerkt die Kontrolle übernehmen. Unerwünschtes Cryptomining ist dann vermutlich das kleinste Problem, mit dem die Betroffenen rechnen müssen.

Ben Kröger

Ben Kröger, Technische Leitung, Axians IT Security

LockerGoga, CottleAkela und Gorgon – Ransomware ist zurück

Im letzten Jahr wurde es ruhiger um Ransomware, weniger Nachrichten, weniger betroffene Unternehmen, doch diese Ruhe ist trügerisch. Cyberkriminelle haben viel Geld mit Erpressungstrojanern verdient und die Zeit genutzt. Mit den neuen Cyberbedrohungen wie LockerGoga, CottleAkela und Gorgon sind nun gleich drei neue Programme erfolgreich aktiv. Bekanntheit hat hierbei vor allem LockerGoga erlangt, weil er die IT-Systeme des Aluminiumherstellers Norsk Hydro verschlüsselt hat.

Pascal Cronauer, Regional Director Central EMEA, LogPoint

Der Norsk Hydro-Vorfall
Beim norwegischen Unternehmen sorgte die Ransomware für einen Ausfall der IT-Systeme in den meisten Geschäftsfeldern, deshalb wurde in den betroffenen Bereichen auf den manuellen Betrieb umgestellt, um Mensch und Maschinen zu schützen. Die Angreifer hatten anscheinend im Vorfeld das Unternehmensnetzwerk infiltriert und sich seitwärts durch die Systeme bewegt, bis sie den zentralen Active Directory Server gefunden hatten und über diesen die Ransomware gezielt eingeschleust und verteilt haben. Die Verantwortlichen beim Aluminiumhersteller setzten daraufhin ihren Notfallplan in die Tat um und kommunizierten nur noch über die Facebook-Seite und ließen einen Manager mit der Presse sprechen, um die wichtigsten Fakten zu kommunizieren. Das Notfall-Backup wurde daraufhin eingespielt, um die Systeme nach und nach wieder in Gang zu setzen. Das von den Cyberkriminellen geforderte Lösegeld wollte der Konzern nicht bezahlen.

Was ist Ransomware?
Es ist gerade für mittelständische Unternehmen zunächst einmal wichtig zu erkennen, mit was sie es tatsächlich zu tun haben. Bei Ransomware handelt es sich um eine kleine Malware, die Daten auf lokalen Speicherplatten als auch auf remote Netzwerken verschlüsselt. Sobald die Daten komplett verschlüsselt sind, wird ein Lösegeld gefordert. Zunächst ist das Verständnis wichtig, dass es kein einzelnes Tool gibt, um eine Ransomware abzuwehren. Der beste Weg, eine Ransomware-Infektion zu verhindern, ist die Mitarbeiter auf Security Awareness zu schulen und eine aktualisierten E-Mail- und Endpunktschutz zu implementieren.

Sicherheitsmaßnahme: Schnelle Erkennung und Einordnung der Ransomware-Infektion
Bei Ransomware ist einer der wichtigsten Aspekte, dass Unternehmen die Infektion und den Typ der Schadsoftware schnell erkennen müssen. Je länger die Ransomware ihr Unwesen treibt, desto größer ist der Schaden und je höher steigen die Kosten diese zu beheben. Im Fall der LockerGoga wurde die Schadsoftware so entwickelt, um auf sensible Benutzerdaten auf infizierten Geräten zuzugreifen und die dort gespeicherten Daten zu verschlüsseln. Sie versendet entweder bösartige E-Mails oder setzt andere Formen des Social Engineering ein, um Opfer zum Herunterladen einer bösartigen Datei zu verleiten oder auf einen Link zu klicken, der zum automatischen Herunterladen dieser Datei führt und/oder Exploit-Kits verwendet. Sobald das Opfer (also der Mitarbeiter) zum Öffnen des bösartigen Anhangs verleitet wurde, verschlüsselt die Ransomware die Dateien mit dem AES- oder einem ähnlichen Verschlüsselungs-Algorithmus.

Infektionen erkennen, bevor sie gefährlich werden
Um den Befall mit Ransomware zu erkennen, ist die Nutzung eines File-Systems sehr wichtig. Diese Software wird Unternehmen dabei helfen, nicht autorisierte Aktivitäten auf den IT-Systemen unter anderem bei der Erstellung von Daten oder der Umbenennung von Daten durch einen Nutzer oder einen Prozess zu erkennen. Abhängig von den zur Verfügung stehenden Log-Daten können sowohl der Nutzername als auch die IP-Adresse schnell identifiziert werden. Darüber hinaus wird auch erkannt, wie viele Daten betroffen sind.

Lösungsansatz Erkennung in Echtzeit
Ein SIEM-System ist noch besser dafür geeignet, da es Logs von Vorgängen, die bereits stattgefunden haben in Echtzeit sammelt. Die Möglichkeiten die Daten anzureichern, kann hier von großer Hilfe sein. Eine IP-Adresse kann in einen Gerätenamen übersetzt und ein Gerätename kann in eine spezifische Nutzeranfrage konvertiert werden. Auf diese einfache Art und Weise kann die Software einen Nutzer identifizieren, der etwas Ungewöhnliches verglichen mit seinem normalen Verhalten macht. Dadurch können sofort Maßnahmen ergriffen werden. Mit der Sicherheitssoftware wird eine gut durchgeführte und konfigurierte Sicherheitsmonitoring-Installation den Zeitraum für die Entdeckung der Infektion verkürzen und dadurch die potenziellen Schäden für das gesamte Unternehmen reduzieren. Wenn diese Sicherheitsmonitoring-Software darüber hinaus auch Möglichkeiten der verhaltensbasierten Angriffs-Erkennung durch maschinelles Lernen verfügen, unterstützt dies die zuständigen Sicherheitsverantwortlichen im Unternehmen zusätzlich.

Fazit
Ransomware ist eine stetige Bedrohung für Unternehmen, vor allem mittelständische Unternehmen, die sich keine Fachexperten für die IT-Sicherheit leisten können. Gerade hier müssen die Verantwortlichen auf automatisierte Software setzen, um Ransomware frühzeitig zu erkennen und entsprechende Gegenmaßnahmen einleiten zu können. Die Detektion muss an erster Stelle stehen, einen Notfallplan zu haben an zweiter Stelle. Darüber hinaus sollte ein regelmäßig gepflegtes, externes Backup vorhanden sein. Unternehmen sollten zusätzlich zu Sicherheitssoftware zur Gefahrenabwehr auch in Security Awareness-Trainings investieren, um die Mitarbeiter besser zu schulen, damit sie nicht auf etwas klicken, was eine Infektion auslösen kann.

Pascal Cronauer

Entwicklungen in der Bedrohungslandschaft.

Wie es im Jahr 2018 um die IT-Sicherheit der europäischen Unternehmen bestellt war.

Jedes Jahr publiziert der Cybersecurity-Anbieter SecureLink einen Annual Security Report. Die im Report aufgeführten Daten und Statistiken basieren direkt auf den Beobachtungen der fünf europäischen Cyber Defense Centers (CDC), die das Unternehmen betreibt. Es sind reale Daten über reale Angriffe, was realistische Schlussfolgerungen ermöglicht. Die künstliche Intelligenz übernimmt die Klassifizierung und Kennzeichnung der etwa 10 Billionen Zeilen an Rohdaten. 250.000 Mal hat sie gesagt: „Hey Mensch, schau dir das mal an!“ Das Analytik-Team hat davon etwa 21.000 als relevante Vorfälle eingestuft.

Kleine Unternehmen sind von Angriffen stärker betroffen
Eine der gewonnenen Erkenntnisse lautet: Die Größe ist entscheidend. Nach den Worten von Eward Driehuis, Chief Research Officer bei SecureLink, hat man den Kundenstamm in drei Bereiche unterteilt: bis 1.000 Mitarbeiter, zwischen 1.000 und 10.000 und über 10.000. Acht Prozent der Vorfälle ereignen sich in kleinen Unternehmen mit weniger als 1.000 Mitarbeitern, 19 Prozent im mittleren Bereich und die überwiegende Mehrheit von 73 Prozent in großen Unternehmen. Größere Unternehmen sind in absoluten Zahlen also stärker von Cyber-Angriffen betroffen. Aber wenn man die Daten im Verhältnis zu der Anzahl an Mitarbeitern betrachtet, ergibt sich ein ganz anderes Bild: Mittlere und große Unternehmen waren in relativen Zahlen gleichermaßen betroffen. Pro 100 Personen haben sie etwa 1,5 Angriffe pro Jahr. Bei den kleinen Unternehmen stieg die Zahl sogar um den Faktor fünf auf 9,1. Das sind etwa sechsmal mehr Angriffe pro Kopf als bei den mittleren und großen Firmen. Das bedeutet, dass 9 von 100 Mitarbeitern innerhalb eines Jahres in Sicherheitsvorfälle involviert sind. Ein 200-Mann-Unternehmen muss demzufolge mit 18 erfolgreichen Angriffen fertig werden. Kleine Unternehmen sind zudem schlechter gerüstet als die größeren. Sie werden häufiger getroffen und die Wirkung ist schlimmer. Cyber-Sicherheit ist nicht fair. Es empfiehlt sich „Brandschutzübungen“ abzuhalten, um sich darauf vorzubereiten. Denn die Frage ist nicht, ob ein Angriff passiert, sondern wann. Die gute Nachricht: 99 Prozent der Angriffe erfolgen als Schuss ins Blaue, sie zielen also nicht auf ein bestimmtes Unternehmen ab.

Ransomware lebt wie eh und je
Die zweite Erkenntnis: Ransomware startet ein Comeback. Seit der Bitcoin und andere Krypto-Währungen in den Keller gerauscht sind, lohnt sich herkömmliches Cryptojacking nicht mehr, wo es um die Rechenleistung des Opfers für das Mining geht. Lukrativ aber ist es für Cyber-Kriminelle geworden, Online Backups zu zerstören und dann eine Ransomware zu aktivieren, um das Unternehmen zu erpressen. Der generelle Ratschlag lautet, nicht zu bezahlen, weil man damit das ‚Geschäftsmodell‘ am Leben hält. Aber wenn ein CEO die Optionen hat, auf die Forderungen der Kriminellen einzugehen oder den Gang in den Konkurs anzutreten, wird er sich für ersteres entscheiden. „Es geht ja nicht nur um die Verantwortung für das Unternehmen, sondern für die Mitarbeiter, die ihre Familien finanziell unterhalten möchten“, so Driehuis.

Eine weitere Schlussfolgerung des Berichts betrifft die Auswirkungen der Cyber-Angriffe. Die geschäftskritischen Einschläge gingen um den Faktor zehn zurück. Gleichzeitig hat sich auch die Zahl der Angriffe mit geringfügigen Auswirkungen verringert, sodass die überwiegende Mehrzahl nun als mittelschwer einzustufen ist.

Social Engineering als Einfallstor
Was die Methoden betriff, um in ein Unternehmensnetzwerk zu gelangen, so steht Social Engineering am Beginn der meisten Angriffe, also das Ausspähen von Mitarbeitern. Die Mehrheit der Cyber-Attacken hat mit Social Engineering zu tun und nicht mit Exploits, Malware- oder Zero-Day-Angriffen – und Social Engineering

Andreas Dumont, Freier Journalist, Büro Andreas Dumont

ist schwer zu erkennen. Aus Sicht des Angreifers ist es durchaus sinnvoll, sich auf die Verhaltensmuster eines Menschen zu konzentrieren. Social Engineering nutzt alle verfügbaren Online-Informationen. Unternehmen sollten daher das Sicherheitsbewusstsein der Mitarbeiter stärken und sie bezüglich manipulativer Techniken schulen, die gegen sie eingesetzt werden könnten. Darüber hinaus sollten die Unternehmen eine Zwei-Faktor-Authentifizierung einsetzen. Die zweite, verbreitete Methode ist das automatisierte Scanning. Wenn etwa ein Plugin einer Webplattform nicht aktualisiert wird, entdecken das Hacker sehr schnell. Aber nicht nur die Kriminellen, auch die Sicherheitsbranche macht Fortschritte. „Es ist wie eine Art Bockspringen“, sagt Driehuis, „mal ist der eine vorne, mal der andere“.

Staaten als Bösewichte

War vor wenigen Jahren noch herkömmliche Cyber-Kriminalität so ziemlich alles, wogegen man sich wehren musste, kommt heute zunehmend eine neue Quelle der Bedrohungen dazu: ausgeklügelte Langzeitkampagnen (Advanced Persistance Threats, APT), die Staaten zugeschrieben werden. Die Ziele reichen von Wirtschaftsspionage über geopolitische Ziele bis hin zu Sabotage und physischem oder ökonomischem Schaden. Ein Beispiel ist der Angriff auf eine saudi-arabische, petrochemische Fabrik, der eine Explosion hervorrufen sollte. APT-Gruppen sind bestens ausgestattete, bezahlte und professionelle Hacker. Ihre Vorgehensweisen und Methoden sind weit schwieriger vorherzusehen und abzuwehren als diejenigen gewöhnlicher Krimineller, die sich in der Regel auf den finanziellen Profit konzentrieren. Viele Unternehmen leiden dabei sogar unter Kollateralschäden, sind also gar nicht das Ziel gewesen, aber durch eine Streuung doch betroffen von der Attacke.

Während der Bedrohungs-Analyse ist einer der schwierigsten Prozesse die Zuordnung, also die Identifizierung der Quelle einer Bedrohung. Manchmal dauert es Jahre und manchmal erweist sich eine Zuordnung sogar als falsch. Die Malware ‚Olympic Destroyer‘ etwa war bei einem Angriff auf die Olympischen Spiele in Südkorea voller Hinweise auf Nordkorea. Das aber wird mittlerweile als falsche Fährte betrachtet, die bewusst vom eigentlichen Schöpfer gelegt wurde. Heutzutage geht man davon aus, dass Russland für das Schadprogramm verantwortlich ist.

Fazit

Zusammenfassend lässt sich sagen, dass auf der Liste der APTs vor allem Russland und Nordkorea für Schlagzeilen sorgen. Der Iran erhöht seit Jahren seine Kapazitäten und Vietnam konzentriert sich zunehmend auf die lokale Geopolitik. China unterhält die meisten APT-Gruppen, die sich alle auf die Industriespionage konzentrieren. Darum werden Nationalstaaten und organisierte Kriminelle nun zur hauptsächlichen Gefahr und sie stellen natürlich eine größere Bedrohung dar, als die ehemaligen Einzelkämpfer mit ihren wenigen Möglichkeiten und Ressourcen.

Andreas Dumont

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 herausgefunden, 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.

Jelle Wieringa, Security Awareness Advocate, KnowBe4

Fazit

Viele Nutzer sind auf Social Media-Plattformen (Facebook, LinkedIn und Twitter) aktiv. Kriminelle nutzen diese wiederrum, um Profilinfor-

mationen 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

Cyberangriffe 2019: Warum sind Unternehmen und Privatpersonen immer noch so verwundbar?

Dietmar Schnabel, Regional Director Central Europe, Check Point Software Technologies

Täglich werden weltweit mehrere Millionen Cyberangriffe gestartet. Nicht alle sind erfolgreich, aber dennoch ist klar: die Gefahrenlage bleibt für Unternehmen wie Privatpersonen akut. Erschreckend ist, wie einfach es die Angreifer haben, wenn sie E-Mail-Konten oder Firmennetzwerke kapern. Bislang galt die Devise, dass erst etwas passieren müsste, bis in Sicherheitsmaßnahmen investiert wird. Dies scheint nun außer Kraft gesetzt zu sein – eine gefährliche Entwicklung.

Das neue Jahr war noch nicht einmal richtig gestartet, da machte ein 20-jähriger aus Hessen mit der spektakulären Veröffentlichung von mehr als 1.000 E-Mailkonto-Daten von zahlreichen Prominenten und Politikern in Deutschland auf sich aufmerksam. Was sich, im Nachhinein, wie ein Streich eines Jugendlichen anhört, verdeutlich umso mehr, wie schwach das Thema IT-Sicherheit hierzulande ausgeprägt ist. Zwar war die Aufregung zunächst groß, ebbte aber genauso schnell wieder ab wie eine Flutwelle in der Nordsee.

Einige Wochen später folgte dann die Nachricht, dass im Darknet immer mehr Datensätze aufgetaucht sind, die Benutzernamen und Passwörter zu E-Mailkonten von mehr als 770 Millionen Privatnutzern enthielten. Seitdem vergeht keine Woche, ohne entsprechende Meldungen. Was sich zunächst danach anhört, als würde es ausreichen einfach nur das Passwort zu ändern, ist die Entwicklung und Gestaltung solcher E-Mail-Services ein tiefgreifendes. Vor allem E-Mailkonten von klassischen Service Providern sind betroffen, darunter Google Mail, Web.de, GMX.de aber auch andere Anbieter. Auf Seiten der Regierung musste also schnell gehandelt werden, weshalb nun ein Cyberabwehrzentrum Plus errichtet und ein neues Frühwarnsystem für Hackerangriffe vom Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgebaut werden soll. Dies kann man getrost als Aktionismus ablegen, denn verändern wird es an der aktuellen Lage nichts.

In Deutschland finden täglich Angriffe im hohen sechsstelligen Bereich statt und das nicht erst seit kurzem – im Gegenteil, die Tendenz ist steigend und die Angriffe werden zunehmend großflächiger. Laut dem aktuellen Lagebericht des BSI [1] stieg beispielsweise die Anzahl, der sich im Umlauf befindlichen und bekannten Schadprogramme von 600 auf über 800 Mio. Allein mit diesen Malware-Signaturen durchgeführte Angriffe stiegen nach Informationen der Behörde auf 390.000 pro Tag – das sind 110.000 mehr als im Vorjahr. Die Geschwindigkeit, mit der die Angriffe durchgeführt werden können und der Fokus der Angreifer verändert sich ebenfalls. Mit mittlerweile 190 GBit pro Sekunde werden nun nicht mehr nur Browser oder Betriebssysteme attackiert, sondern unter anderem auch Geräte im IoT, Prozessoren, Chips und Überwachungskameras.

Unsicherheits-Faktoren: Mensch, Hardware und ungeschützte Infrastruktur

Und es wird den Angreifern in vielen Fällen sehr leicht gemacht, dass eine Attacke erfolgreich endet: menschliches Fehlverhalten, veraltete Hardware oder nicht ausreichend gesicherte IT-Infrastruktur, beziehungsweise fehlende Security-Mechanismen. Das Hasso Plattner Institut analysierte für eine Studie zur Passwortnutzung rund eine Milliarde Nutzerkonten [2], die aufgrund von Datenlecks frei im Internet verfügbar waren. Besonders auffällig war hier, dass 20 Prozent der Nutzer identische Passwörter für unterschiedliche Accounts nutzen oder diese nur geringfügig abändern (27 Prozent). Das meistgenutzte Passwort ist laut dieser Studie „123456“. Dieser Punkt wird vor allem dann relevant für Unternehmen, wenn Mitarbeiter vermehrt ihre IoT-Geräte mit in das Unternehmensnetzwerk bringen, die nicht ausreichend gesichert sind. Diese Möglichkeit können sich Cyberkriminelle zu Nutze machen, um die IT des Unternehmens zu attackieren.

Ein weiterer Punkt, der bei der Security immer noch bedacht werden muss – auch wenn sich mittlerweile der Großteil der IT im virtuellen Bereich abspielt – ist die Hardware. Veraltete Geräte, die sich immer noch in den Netzwerken befinden, obwohl sie vielleicht überhaupt nicht mehr genutzt werden (Stichwort Shadow IT), können hier ein Einfallstor bieten. Dazu kommt außerdem, dass diese nicht ausreichend aktualisiert werden oder aufgrund ihres Alters möglicherweise auch kein Update mehr zur Verfügung gestellt bekommen. So bleiben vorhandene Schwachstellen bestehen und Hintertüren ungewollt offen. Ein gutes Beispiel für Hardware als

Einfallstor war die entdeckte Schwachstelle bei Faxgeräten im letzten Jahr.

Eine der größten Herausforderungen für Unternehmen ist die Tatsache, dass die verwendeten Sicherheitstools und -systeme, den hochentwickelten Hackerangriffen nicht mehr gewachsen sind. Diese modernen Hacking-Tools ermöglichen den Kriminellen ein schnelles Vorgehen und eine weitreichende Infizierung des Unternehmensnetzwerks. Sogenannte Multi-Vektor-Angriffe können nur durch eine integrierte und einheitliche Sicherheitsstruktur abgewehrt werden. Das bedeutet also, dass ältere Generationen von Security-Tools mit modernen Technologien ergänzt werden und Unternehmen sich somit weg von einer reinen Angriffserkennung hin zu einer proaktiven Angriffsabwehr bewegen.

Fazit

Die Wahrscheinlichkeit, Opfer eines Cyberangriffs zu werden, ist Teil unseres Alltags. Nun geht es darum, sich entsprechend zu schützen und zu versuchen, einen Schritt weiter zu denken. Unternehmen dürfen sich nicht mehr ausschließlich auf die reine Angriffserkennung und -abwehr fokussieren, sondern müssen ihre IT-Security auf eine neue Stufe heben. Idealerweise basiert die Sicherheitsstruktur auf einer Kombination von vorbeugenden, erkennenden und korrigierenden Verfahren. Dann wird es für Security-Teams möglich sein, präventiv zu handeln und ihre Unternehmen, aber auch deren Mitarbeiter zu schützen und ihnen Hinweise für einen besseren Schutz ihrer privaten E-Mailkonten zu geben.

Dietmar Schnabel

Referenzen: **[1]** https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html **[2]** https://hpi.de/en/news/jahrgaenge/2016/sicherheitsrisiko-passwort-hpi-studie-zur-mehrfachnutzung-von-passwoertern.html

2.4 ATTACK VECTOR USER

Stellen Insider Threats das größte Sicherheitsrisiko für Unternehmen dar?

Bei der Diskussion rund um das Thema IT-Sicherheit geht es oftmals um Fälle, in denen Unternehmen oder andere Organisationen Opfer eines gezielten Angriffs von außen werden und wie hier Datenverluste vermieden werden können. Bei aller Fokussierung auf Attacken von außen, tritt die Gefahr, welche die eigenen Mitarbeiter für den jeweiligen Betrieb spielen, häufig in den Hintergrund. Dabei sind sowohl aktuelle als auch ehemalige Beschäftigte gemeint. Selbstverständlich muss in diesem Zusammenhang betont werden, dass nicht alle Innentäter böswillig handeln – in einigen Fällen begehen Angestellte aus Unwissenheit Fehler, die den Datenschutz betreffen und zu Kompromittierungen führen können. Zum Ende letzten Jahres erschien die Studie „Insider Threat 2018 Report“ des Marktforschungsunternehmens Crowd Research Partners, die gemeinsam von der Online-Plattform Cybersecurity Insiders und der Information Security Community auf LinkedIn mit Unterstützung von Quest Software in Auftrag gegeben wurde. Laut der Studie fühlen sich 90% der befragten Unternehmen anfällig gegenüber dem Risiko, das von Innentätern ausgeht. Es gibt einige Aspekte innerhalb des Betriebs, der die Wahrscheinlichkeit, Opfer eines solchen zu werden, stark erhöht. Zu diesen Aspekten gehört der Umstand, dass zu viele Nutzer über umfangreiche Zugriffsrechte verfügen (37%). Auch die Tatsache, dass es eine große Menge an Geräten gibt, die den Zugriff auf sensible Daten erlauben, stellt einen Risikofaktor dar (36%). Zuletzt nennt die Studie noch die steigende Komplexität der Informationstechnologie als Faktor (35%). Die gute Nachricht ist in diesem Zusammenhang, dass sich zahlreiche Firmen der großen Gefahr, die von Insider Threats ausgeht, durchaus bewusst sind. So halten zwei Drittel der Organisationen geplante Angriffe von innen oder auch versehentliche Datenschutzverletzungen für wahrscheinlicher als Attacken von außen.

Auch die Tatsache, dass in den Medien immer wieder über Fälle von Datenklau und Angriffen durch eigene Mitarbeiter berichtet wird, trägt dazu bei, die Bedrohungslage zu erkennen. Wie Anfang dieses Jahres erst bekannt wurde, gelang es vor einigen Jahren einem AXA-Mitarbeiter im britischen Manchester, tausende Pfund nebenher zu verdienen, indem er Kundendaten entwendete und weiterverkaufte. Wie polizeiliche Ermittlungen ergaben, konnte der Versicherungsmitarbeiter wöchentlich etwa 100 Datenzeilen per Whatsapp an seinen Komplizen weitergeben – einen ehemaligen Mitarbeiter des Unternehmens. Der externe Partner überwies dem Innentäter schließlich in regelmäßigen Abständen Summen zwischen 250 und 650 Pfund. Er selbst erhielt mehrere Tausend Pfund von einer Schadenmanagementgesellschaft im Gegenzug für die Daten. Insgesamt sechs Monate lang konnten die Täter dieses Vorgehen aufrechterhalten. Der Fall zeigt, wie Kriminelle mit einfachen Mitteln Daten aus dem Betrieb abführen und zu Geld machen können. In diesem speziellen Falle dürfte der Imageschaden und Vertrauensverlust besonders verheerend für den Versicherungsdienstleister sein.

Es sei darauf hingewiesen, dass im Zeitalter der EU-DSGVO der böswillige Mitarbeiter möglicherweise nicht für einen finanziellen Gewinn handelt,

sondern durch das Durchsickern von Informationen versucht, dem Ruf des Unternehmens zu schaden und sicherzustellen, dass es eine beträchtliche Geldstrafe erhält. Dieses „hacktivistische" Verhalten kann weitaus größere Auswirkungen auf das Unternehmen haben als ein üblicher Ansatz, der zu finanziellen Gewinnen führt.

Die Frage ist also, wie Arbeitgeber sich vor solch einem Fall schützen und das Risiko eines unbefugten Datendiebstahls minimieren können. Die Antwort auf diese Frage beinhaltet zwei verschiedene Dimensionen – die technische und die organisatorische. Eine der bewährtesten Methoden auf technischer Ebene ist die Implementierung einer Lösung aus dem Bereich Data Loss Prevention (DLP). Damit diese effektiv ist, müssen alle Ausgangspunkte abgedeckt sein – E-Mail, Web und Endpunkt.

Dr. Guy Bunker, Chief Technology Officer, Clearswift

Durch die Suche nach sensiblen Informationen und die Blockierung der Übertragung dieser oder dem Redigieren wird das Risiko für Datenabfluss gemindert. Es bedeutet auch, dass unbeabsichtigte Fehler durch Angestellte – welche eine der größten Quellen für Informationsverlust darstellt – ebenfalls gemildert werden können.

Weiterhin gibt es auf organisatorischer Ebene eine Reihe von Verhaltensmaßnahmen, die im einzelnen Fall sinnvoll sein können. Ein Punkt ist hier, im Blick zu behalten, ob Mitarbeiter ungewöhnliche Dinge tun. Während dies in der Theorie einfach klingt, verhält es sich in der Praxis deutlich schwieriger. Im Wesentlichen geht es um „seltsame" Aktivitäten und Datenzugriff, beziehungsweise -übertragung. Nehmen wir jedoch das einfache Beispiel von einem Angestellten im Bereich Accounting, der eine andere Person vertritt, die im Urlaub oder krank ist. Ihre Zugriffsrechte werden für ihren regulären Aufgabenbereich anders sein, da sie eine andere Rolle einnehmen – dies schafft ein „False Positive" und eine Häufung dieser kann das System letztendlich unpraktisch und unzuverlässig machen.

Schließlich sei in diesem Zusammenhang außerdem noch die Personalabteilung erwähnt, die stets „am Puls der Mitarbeiter" bleiben sollte, insbesondere derjenigen, die ihre Kündigung eingereicht haben oder Angestellte, welche die Personalabteilung bereits wegen verschiedenen Themen aufgesucht haben. Auf diese Weise können die jeweiligen Manager auf mögliche Probleme aufmerksam gemacht werden und es bietet sich Ihnen die Möglichkeit, im stetigen Kontakt mit dem Arbeitnehmer zu bleiben – in diesem Falle wissen die Vorgesetzten, auf welche Warnzeichen sie achten sollten. Im begründeten Verdachtsfall ist es von Vorteil, dass die Personalabteilung in der Regel auch Zugriff auf Dinge wie etwa Telefonprotokolle hat, sodass sie Berichte über ungewöhnliche Aktivitäten zu diesen Themen erstellen kann. Ein Beispiel wäre, dass ein Beschäftigter in einem Monat 100% mehr Anrufe tätigt, oder wenn ein vermeintlicher „Lieferant" besonders viele Anrufe erhält, etc.

Die erste Option, die Anschaffung einer DLP-Lösung ist in der Regel die kostengünstigste, da Einzelpersonen, die zum Innentäter werden, normalerweise mehrere Versuche unternehmen, bis ihr Plan, Daten aus dem Betrieb abzuführen, gelingt. Oftmals versuchen sie, E-Mails an ihre privaten Accounts zu senden – wenn dies nicht funktioniert, versuchen sie, sich in ihren Privat-Account einzuloggen oder Daten auf einen USB-Stick zu kopieren. Jedes dieser Ereignisse sollte einen Alarm an die IT (oder HR, beziehungsweise Audit und Compliance) auslösen – als Signal, dass ein solcher Vorgang einer weiteren Untersuchung bedarf.

Insgesamt lässt sich festhalten, dass es bei effektiver Sicherheit immer um Menschen, Prozesse und Technologien gehen muss. Mitarbeiter müssen ihre Verantwortlichkeiten (und Konsequenzen) verstehen, insbesondere im Umgang mit kritischen Informationen. Dies sollte sich auch darauf erstrecken, welche technischen Lösungen es gibt, die ihnen helfen, ihre Arbeit zu erledigen und die Informationen sicher zu halten. Alleine darüber zu sprechen, wird in vielen Fällen dazu führen, dass diejenigen, die erwägen, Unternehmensdaten für persönliche Zwecke zu nutzen, davon abgehalten werden. Schließlich wissen diese nun, dass die Organisation ein Auge auf ihre Aktivitäten hat – nicht wegen kriminellen Aktivitäten, sondern vorwiegend wegen unbeabsichtigten Fehlern. Doch dies wird auch unerlaubte Pläne zur Datenkompromittierung eindämmen.

Wichtig ist hier, dass das Unternehmen in jedem Falle „offen" sein muss, denn ein ehrlicher Fehler ist genau dies, ein Fehler. Falsch wäre es hier, direkt zum Schluss zu gelangen, dass etwas Böswilliges geplant wurde. Es müssen Prozesse sowie Richtlinien für den Umgang mit kritischen Informationen und Maßnahmen im Falle einer Verletzung vorhanden sein. Technologie ist die letzte Verteidigungslinie – und sollte Richtlinien und Prozesse durchsetzen und letztlich das Unternehmen, seine Mitarbeiter und Kunden sicher halten.

Das Thema Insider Threats stellt eine ernstzunehmende Gefahr für die Cybersicherheit von Organisationen jeglicher Größe und Branche dar. Dem Betrieb böswillig gestimmte Mitarbeiter haben legitimen Zugriff auf kritische Informationen und wissen, wo sie sich befinden. Sie nutzen die Daten schließlich täglich zur Erfüllung ihrer Aufgaben. Während ein Hacker in das Unternehmen eindringen und die Anwendungen oder den Speicherort finden, in die Anwendung eindringen und schließlich die Daten kopieren und aus dem Unternehmen herausholen muss, hat der Mitarbeiter alle diese Informationen bereits. Theoretisch könnte dies also verheerender sein als andere Mittel des Datendiebstahls – allerdings gilt es hier zu beachten, dass die Menschen im Wesentlichen nur das Beste möchten – in der Regel auch für seine Arbeitgeber. Die allermeisten Angestellten sind nicht bösartig gestimmt und haben keine schlechten Absichten, sie erhalten ein Gehalt,

um einen Job zu erledigen – und dies ist es auch, was sie tun. Unternehmen dürfen nicht plötzlich davon ausgehen, dass jeder Arbeitnehmer darauf aus ist, geistiges Eigentum des Unternehmens (einschließlich Kundendaten) zu entwenden und zu verkaufen, aber sie dürfen gleichzeitig auch nicht nachsichtig mit der Idee sein. Es ist ein schmaler Grat zwischen beiden – und einer, der durch eine verbesserte Kommunikation über Risiken und Konsequenzen, die Investition in neue Richtlinien und Prozesse und die Verwendung geeigneter Technologien angegangen werden muss.

Dr. Guy Bunker

Richtiges Nutzerverhalten in Zeiten von Hackerangriffen

Datenleaks treten immer häufiger auf. Einer der schwerwiegendsten Leaks in jüngster Zeit kam durch einen Hack zustande und hatte zur Folge, dass private Daten, darunter Briefe, Chatverläufe und sogar Kreditkartendaten, an die Öffentlichkeit gelangt sind. Nutzer sollten daher ein paar Ratschläge beachten, um sicherzugehen, dass ihre Informationen und die ihres Unternehmens nicht Teil des nächsten Datenskandals werden.

Wie Anfang dieses Jahres bekannt wurde, war es einem 12-jährigen Youtuber gelungen, mitunter persönliche Daten von hunderten von Politikern abzufangen und zu veröffentlichen. Möglich gemacht hat dies eine Sicherheitslücke beim E-Mail-Provider GMail, im Zuge derer Passwörter der Betroffenen Nutzer ohne vorangegangene Prüfung zurückgesetzt werden konnten. War dies geschehen, konnte der Hacker Konten kompromittieren, die mit dem GMail-Konto verknüpft waren.

Neben Privatnutzern werden auch Unternehmen immer häufiger das Ziel von Cyber-Attacken. Besonders häufig sind hier Ransomware-Attacken, bei denen Daten verschlüsselt werden und erst gegen Bezahlung eines Lösegelds in Form von Kryptowährungen wieder entschlüsselt werden. Dies ist allerdings keine Garantie, kritische Informationen wiederzuerlangen – oftmals bleiben die Daten trotz Zahlung verschlüsselt. Die Frage ist also, wie einzelne User und Unternehmen sich vor solchen Attacken schützen können.

Daten richtig sichern

Ganz allgemein lässt sich festhalten: Informationen sind wertvoll, seien es solche von Privatpersonen oder betriebsinterne Daten. Deshalb bilden sie ein lukratives Ziel für Cyber-Kriminelle, die diese Informationen abgreifen und gewinnbringend verkaufen wollen.

Als erstes sollte der Zugang zu privaten und geschäftlichen Daten bestmöglich vor unberechtigtem Zugriff geschützt werden.

Eine der häufigsten Methode, um unberechtigten Zugriff auf Daten zu erhalten, ist der sogenannte Brute-Force-Angriff. Vergleichbar mit einem Dietrich, der die einzelnen Zylinder eines Schlosses manipuliert, bis sie in der richtigen Position sind, werden bei einem Brute-Force-Angriff solange Buchstaben-, Zahlen- und Zeichenfolgen in das Passwortfeld eingeben, bis der richtige Code durch Zufall gefunden wird.

Hier gilt: Je länger und komplexer das Passwort, desto zeit- und kostenintensiver und damit weniger lukrativ ist ein solcher Angriff. Nutzer sollten deshalb darauf achten, dass ihre Passwörter eine ausreichende Länge haben und mit Sonderzeichen und alternierenden Groß- und Kleinbuchstaben versehen sind. Unternehmen können Richtlinien für ihre Mitarbeiter aufstellen, in denen geregelt ist, wie komplex Passwörter zu sein haben und ob, bzw. in welchen zeitlichen Abständen sie ausgetauscht werden sollten.

Um den Schutz vor Datenverlust weiter auszubauen hilft auch eine Zwei-Faktor-Authentifizierung (2FA). Neben Benutzernamen und Passwort wird beim Login zusätzlich noch ein weiterer Faktor zum Zugriff verlangt. Die gängigsten 2FA-Mechanismen sind Hardwaretokens, Smartcards oder auch per SMS versandte Bestätigungscodes.

Besitzt ein möglicher Cyber-Krimineller diesen zweiten Faktor nicht, erhält er keinen Zugriff auf die Daten.

Arved Graf von Stackelberg, Geschäftsführer / CSO, DRACOON

Augen auf bei der Wahl des Cloud-Speichers

Auch die richtige Wahl des Cloud-Speichers kann dabei helfen, Daten effektiv zu schützen. Besonders im Unternehmen müssen Kunden- und Mitarbeiterdaten, aber auch andere, beispielsweise produktionsrelevante Daten, schnell verfügbar und gleichzeitig bestmöglich geschützt sein.

Nicht zuletzt im Zuge neuerer Verordnungen zum Datenschutz können Datenleaks hier weitreichende Schäden verursachen. Zum einen verlieren Kunden das Vertrauen in das Unternehmen, das Opfer eines Hacks geworden ist und dadurch ihre Daten verloren hat. Zum anderen drohen Betrieben im Falle eines erfolgreichen Angriffs empfindliche Strafen.

Entscheider sollten deshalb bei der Wahl einer Cloud-Speicher-Lösung einige Dinge beachten.

1. Bestmögliche Verschlüsselung von Daten

Bei vielen Cloud-Anbietern findet nur eine serverseitige Verschlüsselung der Daten statt. Das heißt, dass die Informationen, die ein Nutzer in der Cloud speichern will, auf seinem Gerät und während der Übertragung ins Rechenzentrum unverschlüsselt und somit vor unberechtigtem Zugriff nicht ausreichend geschützt sind.

Deshalb ist darauf zu achten, dass Daten zusätzlich schon auf dem Gerät des Nutzers und während des Transports im Netzwerk verschlüsselt werden. Einige Speicherlösungen für die Cloud bieten solche Ende-zu-Ende-Verschlüsselungen standardmäßig an und stellen die Art ihrer Kryptographie quelloffen zur

Verfügung. Damit können technisch versierte Nutzer die Qualität der Verschlüsselung selbst überprüfen.

2. Detailliertes Berechtigungsmanagement
Kunden-, Finanz- und Produktionsdaten sind mitunter die wertvollsten Informationen, die Unternehmen besitzen können. Deshalb sollte der Zugriff darauf nur den Personen bzw. Abteilungen möglich gemacht werden, die berechtigtes Interesse daran haben.

Ein feingliedriges Management von Lese- und Bearbeitungsrechten ermöglicht es Unternehmen, den Zugang zu ihren Daten effektiv abzusichern. Zum Beispiel sind Finanzdaten für die Buchhaltung von zentraler Bedeutung, für die IT-Abteilung eher weniger. Mit dem richtigen Rechtemanagement kann bestimmten Abteilungen der Zugriff auf Daten, die sie nicht benötigen, gesperrt werden.

3. Auf Ransomware-Schutz achten
Auch Cloud-Speicherorte sind vor Ransomware-Angriffen nicht gefeit. Hier kann eine Versionierung gelöschter Daten Abhilfe schaffen. Das heißt, dass ältere Versionen von Daten sobald sie bearbeitet und gespeichert werden, nicht endgültig gelöscht, sondern als unveränderlich im Papierkorb gespeichert werden.

Hatte eine Ransomware-Attacke Erfolg, sind die aktuellen Versionen zwar verschlüsselt, ältere Versionen, die sich im Papierkorb befinden, können aber wiederhergestellt werden. Selbst wenn die neuesten Versionen verschlüsselt bleiben, kann die Arbeit fortgesetzt werden. Kostspieliger Arbeitsstillstand im Unternehmen wird somit verhindert.

4. Hohe Nutzerfreundlichkeit
Nur wenn die Endnutzer im Unternehmen die neue Cloud-Lösung akzeptieren, werden sie diese auch benutzen. Deshalb sollten Firmen die Lösung auswählen, welche die größte Nutzerfreundlichkeit verspricht.

Dazu gehören unter anderem eine schnelle und einfache Implementierung in die bestehenden IT-Strukturen und danach ein reibungsloser Betrieb der Lösung. Weitere Vorteile können sein:

1. Einbindung des Cloud-Speichers in die gewohnten Ordnerstrukturen: Anstatt über den Browser auf den Speicher zugreifen zu müssen, wird er als normaler Ordner im Dateisystem angezeigt
2. Nutzung für E-Mail-Anhänge: Einige Cloud-Speicher-Anbieter stellen Outlook-Plugins zur Verfügung, mit deren Hilfe User Anhänge beifügen können, die sonst zu groß für den Anhang wären. Anstatt dass die Datei direkt an die Mail angehängt ist, wird sie in die Cloud hochgeladen und ein Zugangslink in der Mail angezeigt.
3. Zugriff per App: Um auch mobil auf gespeicherte Dateien zugreifen zu können, sollte die Lösung für die gängigsten mobilen Betriebssysteme als App verfügbar sein. Eigenes Branding: Eine anpassbare Oberfläche sorgt dafür, dass Anwender schneller Vertrauen zur Lösung gewinnen und sie besser akzeptieren.

Fazit
Angriffe auf Daten von Privatnutzern und Unternehmen werden auch in Zukunft nicht abnehmen, sondern eher häufiger werden. Um sich bestmöglich vor Cyber-Kriminellen zu schützen, ist die Implementierung eines sicheren Cloud-Speichers ein wichtiger Schritt. Wenn Entscheider bei der Auswahl der Lösung ein paar wichtige Punkte beachten, können sie ihr Sicherheitsniveau beträchtlich steigern und ihre Daten somit effektiv schützen.

Arved Graf von Stackelberg

Wie sich die Schulung des Cybersicherheitsbewusstseins weiterentwickeln muss

Das Cybersicherheitsbewusstsein von Mitarbeitern kann bei der Verhinderung von Datenlecks und Malware-Infiltrationen eine enorme Rolle spielen – Organisationen müssen jedoch die von ihnen angebotenen Schulungsmaßnahmen verbessern. Wie eine Studie von Egress zeigte, glauben mehr als drei Viertel der Führungskräfte, dass Mitarbeiter im vergangenen Jahr Unternehmensdaten aus Versehen gefährdet hätten, 92 Prozent der Mitarbeiter gaben allerdings an, nichts getan zu haben, um Daten zu gefährden. Dieses Phänomen ist häufig anzutreffen: Menschen sind zwar überzeugt, die Regeln zu kennen, aber zwischen Theorie und Praxis klafft oft eine Lücke. Schulung kann hier einen großen Unterschied machen – wenn alles richtig läuft. Es gibt drei wesentliche Strategien, die bei der Erstellung eines funktionierenden Programms helfen können, an dessen Ende ein verbessertes Bewusstsein für Cybersicherheit steht.

Schulungsmaßnahmen an unterschiedliche Mitarbeitergruppen anpassen.
Mitarbeiter auf unterschiedlichen Verantwortlichkeitsebenen und mit unterschiedlichem Wissen benötigen unterschiedliche Maßnahmen zur Schulung des Cybersicherheitsbewusstseins. In Bezug auf die drei Hauptgruppen im Unternehmen sind folgende Ansätze in Betracht zu ziehen:

- IT- und Cybersicherheitsexperten — Personal, das für IT-Sicherheit und andere Personen mit privilegiertem Zugriff auf IT-Systeme verantwortlich ist, erfordert eingehendere Schulung. Der Fokus sollte auf situationsbedingten Schulungen liegen. Dabei sollten auch moderne Techniken zum Schutz vor Cyberbedrohungen aufgezeigt werden.
- Nicht-IT-Mitarbeiter — Schulungen für Nicht-IT-Mitarbeiter müssen regelmäßig, spannend, kurz und für

ihre Jobfunktion relevant sein. Das Hauptaugenmerk muss auf Grundkenntnissen über Cybersicherheitsrisiken und gute Sicherheitsgewohnheiten.

- Führungskräfte und Direktoren — Schulungen für das Management sollten stärker auf die Geschäftsbedürfnisse ausgerichtet werden: Sie sollte grundlegende Sicherheitsprinzipien umfassen, aber auch Details zu den Folgen von sicherheitsrelevanten Ereignissen für das Unternehmen und seine Stakeholder. Das Management sollte sowohl über Geldstrafen bei Sicherheitslücken als auch über den bleibenden Schaden für die Reputation des Unternehmens Bescheid wissen.

Spannende Schulungen regelmäßig führen.

Zu viele Unternehmen bieten Cybersicherheitsschulungen nur zum Zeitpunkt der Einstellung oder im Rahmen einer jährlichen Update-Übung an. Damit Cybersicherheitsschulungen effektiv sind, muss sie in kleinen, verdaulichen Einheiten angeboten werden, die für die Mitarbeiterzielgruppe spannend sind.

Beispielsweise ist ein fünfminütiges Schulungsvideo, das reale Situationen nachstellt, wahrscheinlich besser geeignet, die Aufmerksamkeit eines Geschäftsanwenders zu fesseln als ein dickes IT-Schulungshandbuch. Und höchstwahrscheinlich wird der Unterricht auch besser verinnerlicht und wiederholt.

Doch auch bei den Schulungsvideos gibt es ein paar Dinge zu beachten: Videos, die ihre Inhalte mit Hilfe einer Prise Humor vermitteln, sind bei Zuschauern häufig beliebter als dröge aufgelistete „Dos and Don'ts". Auch sollten die Schulungen per Video eine gewisse Qualität aufweisen und im besten Fall von einem darauf spezialisierten Unternehmen gedreht werden. So wird sichergestellt, dass sowohl die Qualität stimmt als auch die Inhalte auf die bestmögliche Art und Weise vermittelt werden.

Schulung sollte eine kontinuierliche und fesselnde Erfahrung sein, und darauf ausgerichtet, die Verhaltensweise und Einstellung von Mitarbeitern zu ändern. Die Anzeichen für einen Angriff sollten bekannt sein und es gilt, die Mitarbeiter zu ermutigen, sofort die IT-Abteilung zu kontaktieren, wenn etwas verdächtig erscheint. Telefonnummern und andere Kontaktinformationen müssen bekannt und erreichbar sein, damit alle wissen, wer anzurufen ist.

Unterschiedliche Formate verwenden.

Die Kombination einer Vielzahl von Formaten kann das Schulungsprogramm wirksamer machen. Hier einige Optionen, die zu erwägen sind:

- Schulung im Frontalunterricht — Ein wesentlicher Nutzen der interaktiven Schulung ist die Anwesenheit einer realen Person, die schwierigere Themen erklärt und Fragen für eine ganze Gruppe beantwortet. Einige Unternehmen bieten sowohl Live- als auch webbasierte Schulung an und nutzen eine Vielzahl von Methoden, wie Rollenspiele und Simulationsspiele, damit die Interaktion eher wechselseitig als einseitig ist. Webinars sind eine gute Möglichkeit bei geografisch verteilten Mitarbeitern.
- Eine Webseite für das Sicherheitsbewusstsein — Die Webseite könnte in unterschiedliche Abschnitte aufgeteilt sein, die Gebiete wie Malware, Falschmeldungen, Dateifreigabe und Copyright umfassen. Sie könnte auch Übungslektionen zum Selbststudium für Nutzer enthalten, mit Miniquizzen am Ende eines jeden Abschnitts, um sicherzustellen, dass das Material tatsächlich gelernt wurde.
- Hilfreiche Hinweise — Verantwortliche könnten überlegen, Schulungen mit Tipps und Erinnerungen zu ergänzen, die beim Einloggen oder bei anderen Gelegenheiten auf den Nutzerbildschirmen angezeigt werden. Diese Tipps können Schlüsselpunkte wiederholen, die während der Schulung besonders betont wurden, wie beispielsweise "Bewahren Sie Ihr Passwort niemals an einem Ort auf, der außer von Ihnen auch für andere zugänglich oder einsehbar ist."
- Penetrationstest — Es ist klug, die Effektivität des Programms anhand regelmäßiger Penetrationstests zu bewerten. Sie können zum Beispiel sehen, welche Nutzer auf Links in einer Phishing-Email klicken und welche das über die vorgeschriebenen Kanäle melden. In einem zweiten Schritt können diejenigen Mitarbeiter, die auf die gefälschten E-Mails hereingefallen sind, erneut gesondert geschult werden. Hier gilt es, keine dem Mitarbeiter gegenüber bedrohliche Atmosphäre zu schaffen, sondern sein Bewusstsein für mögliche Bedrohungen zu schärfen.

Fazit

Der Aufbau einer starken Cybersicherheitskultur kann nicht gewährleisten, dass es niemals zu Sicherheitsvorfällen kommen wird. Es wird immer irgendjemanden geben, der die grundlegenden Sicherheitspraktiken vernachlässigt und Daten gefährdet. Darüber hinaus besteht stets die Gefahr, dass Sie Opfer eines Hackerangriffs oder einer böswilligen Insideraktivität zu werden.

Cybersicherheitsschulung ist zwar ein wichtiger erster Schritt zur Reduzierung von Risiken für die Datensicherheit, doch müssen Sie auch Verfahren und Instrumente einführen, mit denen Sie die Möglichkeit haben, Ihre Daten und Systeme zu kontrollieren. Idealerweise sollten Sie ein profundes Verständnis dafür erlangen, welche Daten Sie besitzen und was am meisten zu schützen ist. Darüber hinaus sollten Sie in der Lage sein, schnell verdächtige Aktivitäten rund um diese Daten zu erkennen. Das wird Ihnen helfen, die Sicherheit Ihrer sensiblen Daten zu gewährleisten, Geld zu sparen und gleichzeitig den Ruf Ihres Unternehmens zu wahren.

Jürgen Venhorst

Jürgen Venhorst, Country Manager DACH, Netwrix

E-Mail-Sicherheit: Alte Brandherde durch neuen Brennstoff noch gefährlicher

Immer wieder sorgen neue Arten von Malware und zunehmend ausgefeiltere Angriffsmechanismen von Cyberkriminellen für Schlagzeilen. Aktuell warnen Sicherheitsexperten beispielsweise vor Fileless Malware. Dabei wird der Schadcode nicht permanent auf dem betroffenen System gespeichert. Stattdessen wird dieser im Arbeitsspeicher nachgeladen. Es gibt keine permanente Kopie auf dem Endgerät. Gängige Antivirenprogramme erkennen diese Art von Schadsoftware meist nicht. Selbst wenn ein Unternehmen nur explizit genehmigte Anwendungen per Whitelisting erlaubt, kann die Fileless-Malware eingeschleust und ausgeführt werden.

Das Problem ist, dass es neben neuen Bedrohungen auch noch bekannte Gefahrenherde gibt, die von vielen Organisationen nicht adressiert werden. Dabei geht es nicht um die riesigen Angriffe, wie die jüngste Attacke gegen Telegram, die für Schlagzeilen sorgte. Vielmehr lassen sich heute die meisten Unternehmen mit relativ einfachen Mitteln angreifen, dadurch wächst die Gefahr Opfer einer Attacke zu werden. Besonders beliebter Angriffsvektor ist dabei das Versenden von verseuchten E-Mails – in Kombination mit unterschiedlichen Mechanismen, um Firmen zu schaden.

Michael Heuer, VP Europe (EU), Mimecast

Der ESRA-Report prüft regelmäßig die Belastung von Geschäfts-E-Mails von über 30.000 Organisationen weltweit. Dabei wurden in den letzten Jahren insgesamt über 232 Millionen Mails gescannt. Die aktuellen Ergebnisse stammen aus einer Untersuchung im Frühjar 2019. Das Researcher-Team veröffentlicht diese jedes Quartal in einem Report. Ziel ist es, Organisationen einen besseren in E-Mail-basierte Angriffe zu geben. Die Mails kommen als Blindcopy aus Organisationen unterschiedlicher Größe und wurden dort durch verschiedene Sicherheitsmechanismen vorab gefiltert. Trotzdem stellt sich heraus, dass über elf Prozent aller E-Mails (mehr als 25 Millionen) schadhaft sind.

Schadhafte URLs und Impersonation-Angriffe nicht bedacht

Ein Großteil der ungewollten E-Mailverkehrs ist Spam, genau genommen 99,6 Prozent: Mehr als jede zehnte empfangene Nachricht ist Junk. Man muss aber bedenken, dass die meisten Unternehmen Spam-Filter haben, die Zahl an versendeten Mails ist also nochmals höher. 24 908 981 nicht-erkannten Spam-Mails sind viel, haben aber eine positive Nachricht: Die riesige Menge an Werbe- und Ramsch-Mails sind nervig, halten Angestellte vom Arbeiten ab, sind aber erstmal keine direkte Gefahr.

Rund 26.713 Mails waren mit Schadsoftware belastet und schafften es in die Netzwerke der Firmen. Sie konnten die Schutzmechanismen umgehen und der Erfolg einer Attacke hängt dann nur noch von einem falschen Mausklick ab. Gerade die Speicher-basierte Malware wird nicht erkannt. Mit Technologie allein kann solchen Gefahren nicht begegnet werden, daher bleibt als letzte Verteidigung noch die Awarness der Nutzer, die solche Bedrohungen erkennen – auch, wenn sie von den Abwehrtools als sicher eingestuft wurden. Der Faktor Mensch ist dennoch kritisch, da in 23.872 Mails zusätzlich keine echte Schadsoftware, aber gefährliche Dateiformate enthalten, die für von den Angreifern missbraucht werden können (wie .exe, .src oder .jsp).

Wie wichtig die Aufmerksamkeit der Nutzer ist, wird besonders deutlich, wenn man sich schädliche E-Mails anschaut, die besonders stark auf die Interaktion der Nutzer setzen – und nicht auf Schadcode. In über 53.753 Fällen konnten die Reseacher Attacken mit gestohlenen Identitäten nachweisen. Dabei geht es um Angriffe, die kontextbezogene Informationen nutzen. Beispielsweise geben sich die Kriminellen als Geschäftspartner, Kunde oder Mitglied der Führungsetage aus und schicken Rechnungen oder Bezahlfreigaben. Es kommt aber keine Malware zum Einsatz, sondern es wird allein auf die Mitarbeit der Opfers gebaut.

Die Zahl der Fälle von solchen Impersonation-Attacken ist mehr als doppelt so hoch wie die Menge an mit Schadsoftware verseuchten E-Mails. Besonders das Thema CEO-Fraud ist ein großes Problem, sodass das BKA sogar eine dezidierte Warnung veröffentlichte. Außerdem steigt die Menge an Mails mit versuchten URLs. Insgesamt wurden 463.546 unterschiedliche Links gefunden, die dazu dienen, schädliche Inhalte nachdem Anklicken auf die Geräte des Opfers nachzuladen.

E-Mail ist Hauptkommunikationsmittel für Unternehmen

Das Business Continuity Institute ist in einer Umfrage der praktischen Analyse dieser Bereiche nachgegangen. Befragt wurden 369 IT-Entscheider aus 63 Ländern nach ihren Prioritäten zu den Themen Datenaustausch und Kommunikation. Ein wichtiger Teil der Untersuchung drehte sich dabei um die eingesetzte Technologie. Nahezu alle Organisationen (97 Prozent) geben E-Mail-Adressen der Mitarbeiter als Hauptkommunikationsmittel an. Daher ist es logisch, dass

Cyberkriminelle das Potential für sich nutzen möchten.

Fast alle Arten von Onlinekriminalität werden über E-Mail ausgerollt. Ransomware, Trojaner, CEO-Fraud, Spam, Phishing, Social Engineering, Malware und sogar Kryptominer nutzen E-Mail als Angriffsvektor – und das leider erfolgreich. Da die Täter ihre Vorgehensweise immer weiter verfeinern, greifen einzelne Sicherheitsmechanismen nicht mehr. Der ESRA-Report macht deutlich, dass eine große Menge an schädlichen Inhalten ihren Weg in die Unternehmen findet.

In Deutschland spricht sich daher unter anderem das Bundesamt für Sicherheit in der Informationstechnik (BSI) für eine generelle Erhöhung der Widerstandskraft von Prozessen aus und kommt in seinem aktuellen Lagebericht zur IT-Sicherheit auf diesen Punkt zurück. Wörtlich heißt es: „Der Schlüsselfaktor Resilienz, der in Zukunft immer bedeutsamer wird, sollte sowohl bei großen Unternehmen als auch bei KMU mehr Bedeutung bekommen. Vorfalltrainings sind hier ein wichtiger Faktor."

Jedes Unternehmen sollte sich die Frage stellen: Wie resilient bin ich eigentlich? Gibt es eine abgestimmte Sicherheitsstrategie, die neben technischen Maßnahmen auch die Belegschaft mit inkludiert. Wichtig ist dabei, dass die Mitarbeiter als „Last Line of Defence" aktiv geschult und in die Abwehr miteinbezogen werden. Denn die Gefahr von Attacken ist real.

Michael Heuer

2.5 WHAT YOU CAN DO

Der Preis der Vorreiter-Rolle: Warum Unternehmen bei der Integration aufkommender Technologielösungen vorsichtig sein sollten

Der Wandel im Technologiesektor passierte innerhalb der letzten Jahre rapide und schreitet weiter unaufhaltsam voran: Scheinbar über Nacht sehen sich Unternehmen konfrontiert mit neuen Möglichkeiten: Sei es mit KI-gesteuerten Lösungen, den Möglichkeiten kommerzieller Drohnen, Edge Computing, Cloud Storage und natürlich der allgegenwärtigen IoT-Software, die bereits überall zu finden ist – vom Wohnzimmer bis hin zur Straßenlampe. Viele zukunftsorientierte Unternehmen nutzen diese neuen Technologien, um mehr Effizienz sowie besseren Service und mehr Rentabilität zu erreichen. Aber setzen sich diese Unternehmen auch neuen Bedrohungen aus, um auf dem neuesten Stand zu bleiben?

Tatsache ist, dass mit neuen Entwicklungen, auch komplett neue Angriffsmöglichkeiten entstehen. Ob es sich nun um die mangelnden Sicherheitsmerkmale des „smart-fridge" im Büro oder den weitreichenden Zugang zu Arbeitsplatz-Apps wie Skype oder Slack handelt – jede neue Innovation birgt das Risiko der Ausnutzung durch Cyber-Kriminelle oder Innentäter. Wie sollten Unternehmen also vorgehen, um diese Bedrohungen abzuschwächen?

Michael Kretschmer, VP EMEA, Clearswift

Schatten-IT als Sicherheitsrisiko für Unternehmen

Bei der Einführung neuer Technologien sollte stets die erste Überlegung zur Cybersicherheit lauten: Auf was können diese Lösungen zugreifen? Auf Netzwerke, Server, Anwendungen, Dateien? Unternehmen müssen das Risiko, dass neue Anwendungen in ihrem Netzwerk auftreten können, sorgfältig abschätzen, bevor sie mit der Implementierung beginnen, da dies eine Reihe neuer Angriffsmöglichkeiten eröffnen könnte. Obwohl es einige Zeit gedauert hat – und es ist noch ein langer Weg – sehen die meisten Firmen die Probleme, die sich durch die Nutzung Cloud-basierten Speicher- und File-Sharing-Anwendungen ergeben, zum Beispiel OneDrive oder Dropbox. Schließlich bedeutet die Tatsache, dass die Datei von einem seriösen Ort stammt noch nicht, dass diese automatisch sicher ist.

Mit Malware behaftete Dokumente, die über einen Link in einer E-Mail oder in sozialen Medien ausgetauscht werden, sind schließlich an der Tagesordnung – auch wenn es Technologien gibt, die das Risiko in diesem Bereich minimieren. Ist die Schadsoftware aber erst einmal im Unternehmen, kann sie sich verwandeln und neue Payloads mit Hilfe der Steganographie herunterladen, um ihre Anweisungen zu erhalten. In diesem Zusammenhang ist es allerdings wichtig zu betonen, dass böswillige Cyberkriminelle, die neue Technologien missbrauchen, bei Weitem nicht die einzige Gefahr für Betriebe darstellen.

Wie der jüngste La Liga-App-Skandal gezeigt hat, sind bereits viele mobile Anwendungen in der Lage, eine Reihe von Funktionen in einem Netzwerk im Hintergrund auszuführen, ohne dass der Nutzer dabei immer sofort zu erkennt, dass sie dies tun. Daher ist es möglich, dass ein mit Malware infiziertes Mobiltelefon das Netzwerk über eine übersehene Zugriffsberechtigung – oftmals über eine arbeitsbasierte Anwendung – infizieren kann. Aus diesem Grund ist es für Firmen essentiell, dass Anwendungen, die

Zugriff auf das Unternehmensnetzwerk haben, überprüft werden. Nur ist sichergestellt, dass sie keine Bedrohung durch ihre Zugangsanfragen darstellen. Hier wird die Tatsache zum Problem, dass Mitarbeiter vieler Betriebe regelmäßig neue Apps herunterladen und installieren, oftmals ohne das Wissen der IT-Abteilung. Diese Anwendungen haben dann Zugriff auf die Kamera, das Mikrofon, die Kontakte, etc. Diese Praxis ist selbstverständlich problematisch, denn es ist sehr schwierig nachzuverfolgen, was die App mit diesem gewährten Zugriff tut.

Firmen müssen auf die Details achten

Auch wenn Unternehmen die Bedrohung durch die beabsichtigte Nutzung einer App oder eines Geräts bewertet haben, müssen sie weiterhin auf neue Bedrohungen achten, die beispielsweise durch einen Bug in der Anwendung oder als unerwarteter Nebeneffekt auftreten können. IoT-Geräte stellen in dieser Hinsicht eine besondere Herausforderung dar, da diese kompakten Geräte – oft mit nur einer einfachen Aufgabe – leicht übersehen werden können, aber häufig an das Firmennetzwerk angeschlossen sind, um scheinbar harmlose Informationen hoch- und herunterzuladen. Wenn diese jedoch kompromittiert worden sind, können sie zweckentfremdet werden, um kritische (Geschäfts-)Informationen zu sammeln und zu versenden. Fakt ist schließlich, dass sämtliche Daten für jemanden einen Wert haben, sodass selbst eine Ansammlung scheinbar belangloser Informationen wertvolle Auskünfte geben kann, wenn sie in die falschen Hände gerät. Jüngste Datenpannen haben Schwachstellen selbst in den verborgendsten Teilen der IoT-Technologie aufgedeckt. Ein oft zitierter Vorfall betraf die Darstellung der genauen Perimeter einer streng geheimen US-Militärbasis, nachdem ein Strava-Fitnessgerät die genaue Position und den Umfang einer solchen Basis zeigte. In diesem Fall war der Militär-Stützpunkt bereits gut bekannt – aber was wäre, wenn es sich um eine Übernachtungsbasis in einem Kampfgebiet gehandelt hätte?

In einem anderen Fall war ein Casino in Nordamerika das Ziel eines signifikanten Datenverstoßes, nachdem Hacker ein übersehenes IoT-Tankthermometer gefunden hatten, das an das Netzwerk angeschlossen war, sodass 10 GB gehackte Daten an einen Knotenpunkt in Finnland weitergeleitet werden konnten. Diese Verstöße lehren uns, dass selbst wenn ein Gerät unbedeutend erscheint oder in seiner Funktion als sicher angesehen wird, es dennoch eine Bedrohung für das gesamte Unternehmensnetzwerk darstellen kann. Schließlich können Cyberangriffe auf die unwahrscheinlichste Weise auftreten, und dies ist eines der Probleme. Denn, wenn Betriebe ihre eigene Technologie-Landschaft nicht verstehen, wie können sie diese dann verwalten und schützen?

Schöne Neue Welt? – Realistische Einordnung der neuen Technologien ist essentiell

Es ist schwer vorstellbar, welche unzähligen Hintertüren und Schlupflöcher entstehen können, wenn Unternehmen beginnen, völlig neue technische Lösungen in ihre Geschäftsprozesse zu integrieren. Beispielsweise ist es für jede Firma schwierig, die vielfältigen Gefahren vorherzusagen, welche die Technologie der Künstlichen Intelligenz für die Datensicherheit darstellen könnten. Laut einer jüngst erschienenen Gartner-Studie hat die Einführung von KI in den letzten Jahren exponentiell zugenommen und mittlerweile haben über 37% der Betriebe eine Funktion der KI übernommen. Grundsätzlich setzen immer mehr Unternehmen auf einen KI-gestützten Arbeitsplatz, um die Effizienz der Entscheidungsfindung zu steigern. Da wir immer mehr Daten sammeln, brauchen wir Hilfe, um den Wald von den Bäumen sehen zu können – und KI kann diese Hilfe leisten. Während KI jedoch häufig für das „Gute“ genutzt wird, haben längst auch Cyber-Kriminelle ihr Potenzial erkannt. Ein Betrieb kann einen Angriff auf einen Datenspeicher-Server im Vorfeld erkennen und verfügt über Mechanismen, um das Problem zu beheben – aber es besteht gleichzeitig die Möglichkeit, dass seine eigenen KI-Lösungen manipuliert und für den Zugriff und die Übertragung dieser Daten mit seinen eigenen Berechtigungen verwendet werden können. Diese Möglichkeit sollte von Firmen in keinem Falle übersehen werden.

Darüber hinaus könnten die rasanten Entwicklungen im Hinblick auf Deep-Fake-Video und -Audio in Zukunft eine erhebliche Bedrohung darstellen, da Hacker theoretisch eine scheinbar authentische Videoanweisung vom CEO senden könnten. Diese würde Mitarbeiter dazu bringen, kritische Daten zu teilen oder eine Rechnung zu bezahlen. Doch auch ohne Deep-Fake stehlen Betrüger bereits heute beträchtliche Mengen an Geld. Während Unternehmen also den Geschäftswert der aufstrebenden Zukunftstechnologien betrachten, müssen sie gleichzeitig auch die potenziellen Risiken abwägen, denen sie sich im Zuge dessen aussetzen.

Die richtigen Fragen stellen – Ein erster Schritt zu mehr Sicherheit

Vor diesem Hintergrund erscheint die offen-

sichtliche Lösung für Unternehmen, Regulierungsstellen innerhalb des Betriebs zu schaffen. Diese könnten das Risiko bestimmen, welche mit der Implementierung neuer Anwendungen und Technologien einhergehen. Allerdings lässt sich dies in der Praxis kaum konkret umsetzen. Dafür ist die Geschwindigkeit des Wandels schlicht zu groß, als dass ein einzelner Ausschuss mithalten könnte. Diese Tatsache bedeutet nicht, dass Unternehmen in diesem Zusammenhang schlichtweg aufgeben sollen – es heißt nur, dass sie noch wachsamer sein müssen. Während Firmen über Auditfähigkeiten für Anwendungen auf Laptops verfügen, ist es jetzt notwendig, sich mit der Übertragung auf mobile Geräte zu befassen. Konkret heißt dies: „Welche Anwendungen wurden installiert, gibt es bekannte Probleme?“. Dieser Ansatz greift aber zu kurz, denn hier könnte es bereits zu spät sein und Malware könnte in das Unternehmen gelangt sein, beziehungsweise geschäftskritische Daten könnten bereits kompromittiert worden sein. Weitere Fragen wären: „Macht die Sperrung der vom Betrieb bereitgestellten mobilen Geräte Sinn, damit Mitarbeiter keine unbefugten Apps installieren können?“, „Stellt BYOD zu viele zusätzliche Herausforderungen an die Informationssicherheit?“. Unternehmen sollten sich unbedingt mit getrennten (virtuellen) Netzwerken und USB-Steuersoftware vor IoT- und USB-Geräten schützen.

Grundsätzlich ist es ist wichtig, dass Unternehmen die neuen Risiken berücksichtigen, die sich im Rahmen aufkommender Technologien ergeben, und vorsichtig mit potenziellen Angriffsmöglichkeiten umgehen, die sich daraus ergeben. Dies bedeutet nicht, dass Firmen auf neue Technologien verzichten sollten, sondern dass sie hierbei einen überlegten Ansatz verfolgen sollten. Es bietet sich an, mit IT-Partnern und Lösungsanbietern über die potenziellen Gefahren von New Tech zu sprechen. Das Feedback dieser sollte dann Teil des Entscheidungsprozesses darüber werden, welche Schritte als nächstes zu unternehmen sind. Es ist wichtig, sich der Bedrohungen bewusst zu sein, die sich aus neuen Technologien ergeben können, aber es ist ebenso wichtig, optimistisch zu bleiben, was den Wert dieser neuen Lösungen angeht. Schließlich bieten sie Unternehmen ungeahnte Möglichkeiten und helfen Ihnen bei der Optimierung der Geschäftsprozesse.

Michael Kretschmer

Sicherheitsansätze für Digitalisierungsprojekte: Das richtige Werkzeug ist Waffe und Segen zugleich

Das Spannungsfeld zwischen Business-Agilität, IT-Security und Compliance ist groß. Moderne Sicherheitsmaßnahmen mit multifunktionalem Zusatznutzen können digitale Prozesse beschleunigen. Mehr Erfolg für weniger Kosten. Zu schön, um wahr zu sein?

Der ambitionierte IT Security-Verantwortliche befindet sich in einem immensen Spannungsfeld. Einerseits soll er sicherstellen, dass sämtliche Geschäftsprozesse und jede eingesetzte Software die aktuellen Sicherheitsnormen erfüllen. Anderseits wird erwartet, dass die Mitarbeiter sicherheitsbewusstes Handeln erlernen, stets umsichtig sind und keine Fehler machen. Zudem möchten das Management und die Umsatzverantwortlichen, dass neue Ideen in möglichst kurzer Zeit mit ‚richtigen‘ Kunden in der Praxis ausprobiert werden können. Sie wollen zusätzliches Geschäft, digitale Nähe und höhere Loyalität bestehender Kunden schaffen.

Darüber hinaus gibt es diverse regulatorische Richtlinien, branchenspezifische Compliance-Anforderungen und neue Bedürfnisse auf dem Markt, die mit teils drakonischen Strafen – wie bei der DSGVO bis zu vier Prozent des Umsatzes – geahndet werden können. Eine komplexe Vielfalt von Herausforderungen und eine große und scheinbar unmögliche Aufgabe für den IT-Security-Verantwortlichen. Die Auswirkungen der fortschreitenden digitalen Transformation sind nicht nur im IT- und im Business-Bereich, sondern auch im IT-Security-Bereich zu spüren. Um heute erfolgreich zu sein, sind Management- und Kommunikationsfähigkeiten sowie Kooperationsbereitschaft und unternehmerisches Denken für Sicherheitsverantwortliche genauso essentiell, wie Fachwissen im IT-Security-Bereich.

Roman Hugelshofer, Managing Director Application Security, Ergon Informatik/ Airlock

Digitalisierungsprojekt mit Augenmaß und Kundenorientierung

Man stelle sich ein Unternehmen vor, beispielsweise eine Versicherung, die sich mittels digitaler Innovationen von der Konkurrenz abheben möchte. Mit dem Ziel, neue Kunden anzuwerben, wird eine neue Digitalisierungsinitiative lanciert. Alle Beteiligten sind bestrebt, das gemeinsame Ziel zu erfüllen: ‚on time‘ und ‚on budget‘. Alle Projektmitarbeiter arbeiten agil und in kurzer Zeit wird ein Minimum Viable Product (MVP) erstellt, welches durch den frühen Einsatz von User Experience (UX) Design schnell visuell überzeugt und das Management begeistert.

Technische Fragen bezüglich Modularisierung, Leistungsfähigkeit und zukünftiger Erweiterbarkeit oder auch die mögliche Integration von Diensten von Drittanbietern, werden übersehen oder absichtlich nicht berücksichtigt. Während vielerorts schon Vorfreude und Euphorie über die schnelle Innovation ausbricht, tritt die IT-Security auf die Bremse und moniert, dass dieser MVP so keinesfalls live gehen kann.

Warum die Skepsis? Wichtige Industriestandards wurden nicht eingehalten, die Auditierbarkeit ist nicht gegeben, die Verwaltung der Benutzeridentitäten wurde außen vorgelassen – ganz zu schweigen von einer starken Benutzer-Authentifizierung. Zahlreiche ungeahnte Risiken lauern im Hintergrund.

Ziele der Security kollidieren mit übergeordneten Geschäftsinteressen

Die Ziele der IT-Security sehen vor, dass business-relevante Prozesse ausnahmslos alle relevanten Sicherheitsanforderungen erfüllen – sei es eine Bank, eine Versicherung, eine Behörde oder ein Industriekonzern. Die Business-Seite will nichts über ungenügende Sicherheit, eine Verlangsamung oder gar eine Verteuerung von Projekten wissen. Das Ziel ist, Kunden in möglichst kurzer Zeit zu beeindrucken.

Die Ansprüche steigen stetig. Architekturen und Lösungen, die höchste Sicherheitsanforderungen erfüllen, flexibel und multifunktional betrieben werden können und es den Unternehmen ermöglichen, neue Ideen und Initiativen rasch umzusetzen, sind rar. Viele reine Security-Lösungen stellen lediglich eine Art Schutzsystem dar. Zusätzliche Budgetanfragen für nachträgliche Sicherheitsmaßnahmen sind unerwünscht und problematisch. Findet man jedoch eine Lösung, die messbaren Zusatznutzen mit sich bringt, kann die Security von der Bürde zum Beschleuniger digitaler Chancen werden.

Wer ohne Security digitalisiert, riskiert Image, Umsatz und die Zukunft des Unternehmens

Unvorsichtiges Verhalten kann ein negatives Nachspiel haben: Hohe Kosten können beispielsweise für die Zahlung von Strafgeldern oder Anwaltsgebühren entstehen, durch regulatorische Sanktionen, die Datenwiederherstellung, die Unterbrechung der Betriebstätigkeit, den Verlust vertraulicher Daten oder gar durch eine Cyber-Erpressung anfallen. Am schwerwiegendsten sind jedoch die Kosten eines Reputationsschadens und die damit verbundenen, finanziellen Konsequenzen. Unternehmen sollten daher zusätzlich zur Innovationsagenda ein lebhaftes Interesse daran haben, die Privatsphäre sowie die Integrität ihrer Kunden, Partner, Lieferanten und der eigenen Mitarbeiter zu schützen. Kurz gesagt: ein signifikanter Sicherheitsvorfall kann ein Unternehmen in den Konkurs treiben.

Verteidigung ist nicht alles

Sicherheitsmaßnahmen zur Verteidigung allein reichen nicht aus: Nebst der Herausforderung, Angriffe sofort erkennen zu müssen, um adäquat darauf reagieren zu können, werden heute weitere multifunktionale Werkzeuge gefordert.

Das richtige Werkzeug kann Schutz und Hilfsmittel zugleich sein. Einerseits dient es der Verteidigung, anderseits als wertvolles Mittel, um neue Initiativen zu ermöglichen. So stiften moderne Sicherheitsarchitekturen einen anhaltenden Zusatznutzen für das Business und gleichermaßen für die Einhaltung der Sicherheitsrichtlinien.

Mit Elan zu neuen Erfolgen

Um mit dem Zuwachs neuer Web-Technologien Schritt halten zu können und gleichzeitig von Legacy-Systemen nicht gebremst zu werden, behelfen sich IT-Profis mit einer konsolidierten Betrachtung relevanter Fragestellungen:

- Was kann ich beisteuern, um Business-Initiativen zu unterstützen?
- Wie kann ich dem Business als Beraterfunktion zur Seite stehen, um frühzeitig Sicherheitsmaßnahmen angehen zu können?
- Wie reduziere ich das Risiko für das Unternehmen, welches interne Anwender bewusst oder unbewusst darstellen können?
- Gibt es eine Architektur, die es uns erlaubt, schnell auf neue Business-Anforderungen zu reagieren, ohne unsere eigenen Prozesse oder Sicherheitsvorgaben zu verletzen?
- Wie bleibt meine Applikationslandschaft agil, bzw. muss ich bei jeder neuen Anforderung ein Analyseprojekt starten, ob die Business-Logik betroffen ist und dies in der Folge hohe Komplexität, Aufwand und Risiken mit sich bringt?
- Mit welchen Werkzeugen kann ich mein Team ausrüsten, um adäquat auf solche Fragestellungen und die berechtigten Wünsche des Business reagieren zu können?
- Wie gelingt das onboarding eines neuen Kunden mittels eines niederschwelligen und einfachen Benutzererlebnisses?

Die Business-Logik bzw. die Zielanwendungen müssen abgesichert und die zentrale und sichere Benutzerverwaltung und -authentifizierung zuverlässig gewährleistet werden, über alle bestehenden und zukünftigen Services hinweg, die für die Erreichung der Geschäftsziele notwendig sind.

Es ist richtig, die IT-Security als relevantes Geschäftsrisiko zu betrachten. Deswegen aber auf Experimente zu verzichten oder mittels punktueller Lösungen auf das Prinzip der Hoffnung zu setzen, ist keine nachwirkende Option. Besser ist es, sich mittels langfristiger, resilienter Lösungen einen Wettbewerbsvorteil zu verschaffen: denn der Druck zu noch mehr Digitalisierung und immer schneller und flexibler zu sein, wird auch in Zukunft nicht abreißen. Lösungen müssen dem Spannungsfeld von Business-Agilität, IT-Security und Compliance standhalten. Heute und morgen.

Roman Hugelshofer

Ethisches Hacken erklärt: Warum Unternehmen Unsummen zahlen, um sich hacken zu lassen

Ethisches Hacking ist ein Vorgang des Eindringens in ein System oder in Netzwerke, um Bedrohungen, Schwachstellen in diesen Systemen herauszufinden, die ein Angreifer finden und ausnutzen kann, was zu Datenverlust, finanziellem Verlust oder anderen größeren Schäden führt. Der Zweck des ethischen Hackings besteht darin, die Sicherheit des Netzwerks oder der Systeme zu verbessern, indem die während des Tests festgestellten Sicherheitsanfälligkeiten behoben werden.

Ethische Hacker können dieselben Methoden und Werkzeuge verwenden, die von den böswilligen Hackern verwendet werden, jedoch mit der Erlaubnis der autorisierten Person, um die Sicherheit zu verbessern und die Systeme vor Angriffen böswilliger Benutzer zu schützen. Von ethischen Hackern wird dabei erwartet, dass sie alle während des Prozesses festgestellten Schwachstellen und Schwächen dem Management melden.

Wer ist ein ethischer Hacker?
Ein ethischer Hacker ist ein erfahrener Fachmann, der über hervorragende technische Kenntnisse und Fähigkeiten verfügt und Schwachstellen in Zielsystemen erkennen und ausnutzen kann. Er arbeitet mit der Erlaubnis der Eigentümer von Systemen. Ein ethischer Hacker muss die Regeln der Zielorganisation oder des Eigentümers sowie das Recht des Landes einhalten. Ihr Ziel ist die Beurteilung der Sicherheitslage einer Zielorganisation.

Ethisches Hacken – Wireless Hacken
Ein drahtloses Netzwerk besteht aus zwei oder mehr Geräten, die über Funkwellen in einem begrenzten Raumbereich miteinander verbunden sind. Die Geräte in einem drahtlosen Netzwerk haben die Freiheit, in Bewegung zu sein, aber in Verbindung mit dem Netzwerk zu stehen und Daten mit anderen Geräten im Netzwerk zu teilen. Einer der wichtigsten Punkte, dass sie so verbreitet sind, ist, dass ihre Installationskosten sehr günstig und schneller sind als die Drahtnetze. Drahtlose Netzwerke sind weit verbreitet und können leicht eingerichtet werden. Sie verwenden den IEEE 802.11-Standard. Ein drahtloser Router ist dabei das wichtigste Gerät in einem drahtlosen Netzwerk, das die Benutzer mit dem Internet verbindet.

Die Funktionsweise von Routern
Router verbinden ein Modem (z. B. ein Glasfaser-, Kabel- oder DSL-Modem) mit anderen Geräten, um die Kommunikation zwischen diesen Geräten und dem Internet zu ermöglichen. Die meisten Router, sogar drahtlose Router, verfügen normalerweise über mehrere Netzwerkanschlüsse, um zahlreiche Geräte gleichzeitig mit dem Internet zu verbinden. In der Regel stellt ein Router eine physische Verbindung über ein Netzwerkkabel mit dem Modem über den Internet- oder WAN-Anschluss her und dann über ein Netzwerkkabel physisch eine Verbindung zur Netzwerkschnittstellenkarte in allen verfügbaren kabelgebundenen Netzwerkgeräten.

Ein WLAN-Router kann zudem über verschiedene WLAN-Standards mit Geräten verbunden werden, die den jeweils verwendeten Standard unterstützen. Die der WAN- oder Internetverbindung zugewiesene IP-Adresse ist eine öffentliche IP-Adresse. Die dem LAN oder der lokalen Netzwerkverbindung zugewiesene IP-Adresse hingegen ist eine private IP-Adresse. Die einem Router zugewiesenen privaten IP-Adressen sind in der Regel das Standard-Gateway für die verschiedenen Geräte im Netzwerk.

In einem drahtlosen Netzwerk verfügen wir über Access Points, Erweiterungen von Funkstrecken, die sich als logische Switches, sogenannte Verteiler, verhalten. Drahtlose Netzwerke bieten zwar große Flexibilität, haben jedoch Sicherheitsprobleme. Ein Hacker kann die Netzwerkpakete ausspähen, ohne sich in demselben Gebäude befinden zu müssen, in dem sich das Netzwerk befindet. Da drahtlose Netzwerke über Funkwellen kommunizieren, kann ein Hacker das Netzwerk von einem nahe gelegenen Ort aus leicht erkennen. Die meisten Angreifer verwenden Netzwerk-Sniffing, um die SSID zu finden und ein drahtloses Netzwerk zu hacken. Wenn die Wireless-Karten in Sniffing-Modi konvertiert werden, werden sie als Überwachungsmodus bezeichnet.

Alexander Eser, Co-Founder & Managing Director, Kaufberater.io

Gleichwertiger Datenschutz für Kabel
WEP (Wired Equivalent Privacy) ist ein Sicherheitsprotokoll, das entwickelt wurde, um drahtlose Netzwerke zu schützen und sie privat zu halten. Es verwendet eine Verschlüsselung auf der Datenverbindungsschicht, die den unbefugten Zugriff auf das Netzwerk verbietet. Der Schlüssel dient zum Verschlüsseln der Pakete, bevor die Übertragung beginnt. Ein Integritätsprüfungsmechanismus überprüft, ob die Pakete nach der Übertragung nicht geändert werden.

Die Vorteile des ethischen Hackens
Der Hauptvorteil ethischer Hacker besteht darin, dass die Hacker die Sicherheitsmaßnahmen eines Unternehmens in einer kontrollierten, sicheren Umgebung testen dürfen. Diese Hacker können Unternehmen dabei unterstützen, zu bestimmen, welche ihrer Computersicherheitsmaßnahmen wirksam sind, welche Maßnahmen aktualisiert werden müssen und welche Maßnahmen sie für gefährliche Eindringlinge wenig oder gar nicht abschreckend finden. Die Daten aus diesen Tests ermöglichen dem Management, fundierte Entscheidungen darüber zu treffen, wo und wie die Informationssicherheit verbessert werden kann.

Wenn die Hacker das System des Unternehmens vollständig erforscht haben, melden sie einen Bericht über die gefährdeten Bereiche des Systems. Diese Bereiche können sich auf die Technologie beziehen, z. B. das Fehlen einer ausreichenden Passwortverschlüsselung, oder in auf Menschen basierenden Systemen, z. B. Administratoren, die Passwörter an nicht autorisiertes Personal vergeben. Aufgrund dieser Schwachstellen kann das Management sicherere Verfahren installieren, um zu verhindern, dass Angreifer die Computernetzwerke oder die Fehler ihres eigenen Personals ausnutzen.

Die Hacker können auch die Techniken demonstrieren, die von unethischen Eindringlingen verwendet werden. Diese Demonstrationen zeigen dem Management, wie Diebe, Terroristen und Vandalen ihre Systeme angreifen und ihre Geschäfte zerstören können. Wenn das Management die Konzepte der „bösen“ Hacker fest im Griff hat, kann es auch lernen, wie diese Eindringlinge daran gehindert werden, diese Techniken zu nutzen, um in ihre verwundbaren Systeme einzudringen.

Unternehmen, die mit vertraulichen Daten umgehen, müssen verstehen, dass sie als potenzielle Ziele eines Hackerangriffs dienen. Kleinere Unternehmen, denen die Ressourcen für eine angemessene Netzwerksicherheit fehlen, bieten Hackern verführerische Chancen. Der Einsatz von ethischen Hackern kann diesen Unternehmen zeigen, wie anfällig sie für einen Angriff sind und wie verheerend die Folgen eines solchen Angriffs sein können.

Braucht man wirklich ethische Hacker?
Es ist sicherlich nicht zwingend, die Dienste ethischer Hacker in Anspruch zu nehmen, aber herkömmliche Sicherheitssysteme haben wiederholt keinen ausreichenden Schutz vor einem Feind, der an Größe und Vielfalt wächst, geboten, wie die Erfahrungen zeigen. Mit der Verbreitung von intelligenten und verbundenen Geräten sind Systeme ständig gefährdet. In der Tat wird Hacking finanziell als lukrativer Weg betrachtet, natürlich auf Kosten von Organisationen. Während eine Hardware einfach zu schützen ist, Stellen Informationen ein größeres Problem dar. Sie können an mehr als einem Ort existieren, in Sekundenschnelle transportiert und ohne es zu bemerken gestohlen werden.

Die IT-Abteilung des eigenen Unternehmens kann sich demnach, sofern man nicht über ein großes Budget verfügt, dem Angriff von Hackern als unterlegen erweisen, und wertvolle Informationen können gestohlen werden, bevor man es überhaupt merkt. Daher ist es sinnvoll, die IT-Sicherheitsstrategie eine Dimension hinzuzufügen, indem man ethische Hacker einstellen, die die Möglichkeiten von echten Hackern kennen. Andernfalls könnte in dem Unternehmen die Gefahr bestehen, dass man unwissentlich Lücken im System offen hält. Um Hacking zu verhindern, ist es wichtig zu verstehen, wie die Hacker denken. Offensichtlich sind die Vorgehensweisen der Hacker einzigartig und für konventionelle Systemsicherheitsrollen schwierig zu handhaben. Um somit für ausreichend Sicherheit im eigenen Unternehmen zu sorgen, ist die Einstellung eines ethischen Hackers unabdingbar. Alexander Eser

Awareness-Bildung durch Live-Hacking: Cyberrisiken erfahrbar machen

Trotz zahlreicher Presseberichte über Sicherheitsvorfälle bleibt das Risiko von Cyberangriffen oft sehr abstrakt. Live-Demonstrationen typischer Hacker-Angriffe zeigen, wie Kriminelle vorgehen und wie leicht sie oft in Systeme eindringen können. Sie schaffen so Awareness und machen Cyberrisiken direkt erfahrbar.

Erfolgreiche Hacker-Angriffe können erhebliche Folgen haben, wie zahlreiche prominente Beispiele zeigen. So werden sich die meisten Leser noch an die erfolgreiche Ransomware-Attacke durch den Erpressungstrojaner WannaCry im

Mai 2017 auf die Deutsche Bahn erinnern, dessen Zahlungsaufforderung auf den Anzeigetafeln vieler Bahnhöfe zu lesen war. Jüngste Beispiele für prominente Opfer sind das Industrieunternehmen Krauss Maffei, bei dem es aufgrund einer Trojaner-Attacke im Dezember 2018 zu Produktionsausfällen kam, und das Klinikum Fürstenfeldbruck, das im November 2018 ohne Rechnerunterstützung auskommen musste, weil Malware den IT-Betrieb komplett lahmgelegt hatte.

Trotz dieser zum Teil spektakulären Beispiele, die nur die Spitze es Eisbergs darstellen, bleibt das Thema IT-Sicherheit oft abstrakt. Geschäftsführer, Abteilungsleiter und Mitarbeiter erkennen zwar das Risiko, stellen aber keine Verbindung zum eigenen Verhalten und zu den täglichen Entscheidungen her. Das kann erhebliche Folgen haben. Sicherheitsmaßnahmen werden ignoriert oder umgangen, um schneller entwickeln, produzieren und ausliefern zu können. Investitionen in IT-Sicherheit werden endlos diskutiert und immer wieder verschoben. Auch schlichte Bequemlichkeit stellt ein erhebliches Risiko dar. Nicht umsonst lautet das beliebteste Passwort 2018 „123456".

Wir haben daher nach einem Weg gesucht, die Folgen solcher Entscheidungen und Routinen erfahrbar zu machen, und die Bedeutung jedes Einzelnen für die IT-Sicherheit eines Unternehmens demonstrieren zu können. Erste Erfahrungen mit Live-Hacking-Vorträgen auf Messen und Konferenzen waren sehr positiv, das Interesse ungemein. Das hat uns motiviert, das Konzept auch für Veranstaltungen in Unternehmen zu nutzen und weiterzuentwickeln.

Der Aufbau eines solchen Live-Hacking-Events ist recht einfach. Wir benötigen dazu weder Spezialequipment noch besonders ausgestattete Räume. Zwei Laptops und ein Beamer genügen. Mit verteilten Rollen zeigen die Präsentatoren als Angreifer und Opfer, wie Cyberattacken funktionieren, und wie einfach es oft ist, Sicherheitsmaßnahmen zu umgehen oder auszuschalten.

Mit unseren Schulungen adressieren wir sowohl den alltäglichen Umgang mit Laptops, Smartphones oder E-Mails, als auch industriespezifische Situationen im IoT- oder Robotik-Umfeld. Dazu haben wir drei Szenarien entwickelt, die wir in Unternehmen live präsentieren können. Projektbezogen gehen wir auch gerne auf die individuellen Anforderungen und Situationen beim Kunden ein.

Szenario 1: Gefährliche Manipulation von Industrieanlagen

Das Internet of Things (IoT) bietet enorme Chancen, erhöht aber auch die Angriffsfläche, über die Kriminelle in Industrieanlagen eindringen können. Die Manipulation von Maschinen und Werkzeugen ist besonders dann sehr gefährlich, wenn Menschenleben gefährdet werden. Wie Hacker vorgehen, zeigen wir am Beispiel eines App-gesteuerten industriellen Kühlsystems, das wir mit Standard-PC-Bauteilen wie einem CPU-Lüfter simulieren. Der erfolgreiche Angriff zeigt, dass Industrieanlagen selbst in vermeintlich sicheren Umgebungen mit zweifacher Transportverschlüsselung, Anti-Virus, Firewall und Intrusion-Detection-Systemen (IDS) nicht vor Manipulation gefeit sind.

Szenario 2: Mobile Hack aus Endanwendersicht über offene WLAN-Netzwerke

In diesem Szenario demonstrieren wir, wie leicht Hacker über die „Evil-Twin"-Methode an Passwörter, Kreditkartennummern und andere vertrauliche Daten gelangen können. Sie installieren dazu im öffentlichen Raum ein WLAN, dessen Name (SSID) mit der eines offiziellen Angebots identisch ist, also zum Beispiel „WIFI-onICE" im Zug oder „Telekom_LH-Lounge" am Flughafen. Hat sich der Nutzer schon einmal in eines dieser offiziellen Netze eingeloggt, merken sich die Geräte die SSID und verbinden sich nun automatisch. Dabei können sie nicht zwischen dem richtigen und dem falschen Angebot unterscheiden. Ist das Signal des Hackernetzes stärker als das des echten, verbindet sich der Nutzer nicht mit den Servern der Bahn oder der Telekom, sondern mit dem PC des Hackers. Dieser kann den gesamten Netzverkehr mitschneiden und dann in aller Ruhe sensible Daten auslesen.

Szenario 3: Eindringen in unternehmensinterne Systeme mittels Social Engineering

Dieses Szenario soll Mitarbeitern demonstrieren, wie schnell sie selbst Opfer eines Angriffs werden können. Der Angreifer sendet dabei eine täuschend echte Phishing-Mail, mit der er den Mitarbeiter dazu bringt, Schadsoftware auszuführen. Dadurch erhält der Angreifer Zugriff auf interne Systeme und kann aufbauend tiefer in die Infrastruktur eindringen.

Die Vorteile des Live-Hacking

Unternehmen sind rechtlich dazu verpflichtet, ihre Mitarbeiter im Umgang mit IT-Ressourcen und sensiblen Daten zu schulen. So schreibt etwa die seit Mai 2018 wirksame Europäische Datenschutzgrundverordnung (EU-DSGVO) entsprechende Maßnahmen im Bezug auf personenbezogene Daten vor und verlangt eine Dokumentation der durchgeführten Schulungen. Anderenfalls drohen hohe Strafen.

Thomas Jakubiak, Abteilungsleiter in der Information Security, msg

Um ihrer Pflicht nachzukommen, setzen Unternehmen heute bevorzugt auf Web-based Trainings. Sie sind unkompliziert, kostengünstig und zeitlich flexibel zu nutzen. WBTs haben sicher ihre Berechtigung und sind ein wichtiger Baustein in der Awareness-Schulung, sie haben aber auch einen erheblichen Nachteil. Das Thema IT-Sicherheit bleibt abstrakt, wird mit dem Abschlusstest „abgehakt" und wieder zu den Akten gelegt. Eine nachhaltige Veränderung des Sicherheitsverständnisses und des Verhaltens unterbleibt häufig. Live-Hacking-Events sind daher die ideale Ergänzung zu WBTs, weil sie die Angriffsmöglichkeiten erfahrbar machen und Betroffenheit erzeugen. Ihr Einfluss auf das Verhalten von Mitarbeitern ist daher wesentlich höher als bei WBTs und wirkt über einen langen Zeitraum.

Fazit

Cyberrisiken bleiben trotz vieler spektakulärer erfolgreicher Angriffe allzu oft abstrakt. Das fehlende Verständnis und der fehlende persönliche Bezug können erhebliche Folgen für die IT-Sicherheit haben. Investitionen werden nicht getätigt, Sicherheitsmaßnahmen einem schnelleren Time-to-Market geopfert oder aus Bequemlichkeit und Unwissen unterlaufen. Live-Hacking schafft hier das notwendige Bewusstsein auf allen Ebenen und in verschiedensten Szenarien. Die Anwendungsfelder reichen vom täglichen Umgang mit Passwörtern, E-Mails oder Wi-Fi-Netzen bis hin zu Industrieszenarien im IoT- und Robotik-Bereich. Nach unseren Erfahrungen stoßen Live-Hacking-Events bei Mitarbeitern und Führungsebene auf hohes Interesse, sorgen für Betroffenheit und führen zu nachhaltigen Veränderungen im Verhalten – und damit zu einer deutlichen Steigerung der Informationssicherheit im Unternehmen.

Thomas Jakubiak

Wie Gefahren erkannt und Systeme effektiv vor Cyber-Angriffen geschützt werden können

Der Schutz vor unbefugtem Zutritt endete für Unternehmen früher sprichwörtlich am Werktor. Im Zeitalter der Digitalisierung gibt es aber neben Gefahren physischer Form auch weitere Arten von Bedrohungen: Cyberattacken, die ortsunabhängig von jedem Ort der Welt erfolgen können. Insbesondere für Unternehmen, für die die Störfallverordnung gilt, ist der Schutz vor Hackern und Co. eine höchst wichtige Aufgabe. In dem Wissen um diese neue Gefahrendimension hat die Kommission für Anlagensicherheit (KAS) deshalb Leitsätze aufgestellt, um Cyber-Angriffen vorzubeugen. Jedoch kann die Umsetzung der daraus sich ergebenden Anforderungen eine große Herausforderung für Unternehmen darstellen. Sie können aber auf Hilfe bauen, um geeignete und effiziente Maßnahmen zu implementieren.

Der Leitfaden der KAS gegen Eingriffe Unbefugter fokussierte noch im Jahr 2002 physische Gefahren und Barrieren für technische Anlagen. Inzwischen hat die Kommission diesen Sicherheitsbegriff deutlich erweitert, da er überholt ist. Seit November 2017 konkretisiert das Merkblatt KAS-44 daher die Anforderungen an die IT-Security in jenen Betrieben, für die die Störfallverordnung gilt.

Ob Biogasanlagen, Chemiewerke mit mehreren Produktionsstätten, oder Lager von großen Mengen gefährlicher Stoffe: Sie alle sind von der KAS-44 direkt betroffen. Weil industrielle Produktionsanlagen einen besonderen Schutz erfordern, stellen sie besondere Anforderungen an die IT-Sicherheit. Denn im Zuge der Digitalisierung wird ein solcher Betrieb stetig weiter vernetzt, so z. B. mit autonomen Produktionsanlagen, digitalisierten Prozessen oder Fernwartung. Dadurch ergeben sich potenzielle Angriffspunkte. Verschafft sich ein Hacker erfolgreich Zugang, kann er den gesamten Betrieb lahmlegen – was schwerwiegende Folgen nach sich ziehen kann.

IT-Sicherheit – neu gedacht

Die KAS-44 enthält Leitsätze anstelle von Vorschriften. Diese sind dazu gedacht, ein Bewusstsein für die Bedrohungen zu erzeugen und Unternehmen auf mögliche Sicherheitslücken hinzuweisen. So soll vor allem auf Managementebene eine Sensibilisierung erfolgen. Zwar sind sich Großkonzerne zumeist über die Gefahrenlage bereits im Klaren;, es sind jedoch gerade die mittelständischen Unternehmen, in denen die Awareness fehlt. Insbesondere für diese Firmen kann das Eindringen eines Hackers nicht nur einen enormen Reputationsschaden bedeuten. Sondern ein erfolgreicher Angriff kann sich schnell zu einem geschäftskritischen Faktor entwickeln.

Und das Gefahrenpotenzial nimmt zu: Man muss nicht nur mit Attacken rechnen, die quasi aus jeder Richtung kommen können. Sondern die gesamte IT eines Unternehmens – äußere Parameter, normale Unternehmens-Firewalls oder andere IT-Schutzmechaniken – wird zur Angriffsfläche.. Oft nehmen Hacker auch Schnittstellen aufs Korn.

Unternehmen stehen daher vor der Aufgabe, ihre IT-Sicherheit von Grund auf neu zu überdenken. Dabei reicht es nicht, den Fokus allein auf autonome Anlagen und Prozesse der Industrie

4.0 zu legen. Es müssen vielmehr die optimalen Sicherheitsmaßnahmen bestimmt werden und im gesamten Unternehmen zur Anwendung kommen – anderenfalls droht, dass die Schnittstellenproblematik weiterhin besteht.

Hinsichtlich der Anforderungen für Firewalls und Perimetersicherheit, galten bisher wenige regulatorische Verfahren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfahl Unternehmen oder Organisationen, die zu den kritischen Infrastrukturen zählen, ein ISMS (Information Security Management System). Fallen Betriebe aber unter die Störfallverordnung, benötigen gerade sie heute sogar ein erweitertes ISMS.

Die Realität sieht indes anders aus: Viele Unternehmen beschäftigen sich mit der Basis-IT-Sicherheit. Maßnahmen, die der aktuellen Bedrohungslage angemessen sind, haben sie noch gar nicht ins Auge gefasst.

Wie geht ein KAS-44-konformes Risikomanagement vor und welche Tools setzt es ein?

Wird das Risikomanagement KAS-44-konform aufgesetzt, besteht es aus den Bausteinen Identifizierung, Analyse und Bewertung.

In einem der ersten Schritte gilt es somit, den Status Quo festzustellen: Alle relevanten IT-Assets und die Netzwerkarchitektur des Unternehmens müssen erfasst werden. Die KAS-44 empfiehlt, in einem Asset Register alle für die Sicherheit relevanten Komponenten zu sammeln. Allerdings setzen viele Unternehmen die dafür benötigten Standardtools nicht ein oder die Tools erfassen nicht segmentübergreifend alle Assets. Unterstützung bietet hierzu eine externe Beratung.

Sie analysiert die Basis-Dokumentation im Unternehmen und verschafft sich ein objektives Bild der Lage. Um im Netzwerk Angriffsflächen zu identifizieren, bieten Tools hierfür wertvolle Hilfe.

Anschließend folgen eine Gefährdungsanalyse, die Ermittlung des Schutzbedarfs und eine Gap-Analyse. Diese bilden die Basis, um schlussendlich den anzustrebenden Sicherheitsstandard festzulegen.

Als nächstes folgen eine Analyse des Risikomanagements, die Prüfung auf Vollständigkeit und eine Risikenbewertung. Das weitere Vorgehen umfasst Attacken auf die IT-Strukturen, wobei entsprechende Tools wie eine Angriffssimulation zum Einsatz kommen. Das Resultat bildet eine Liste an Maßnahmen, um die Sicherheit der Infrastruktur zu optimieren.

Für das Unternehmen können dies schmerzhafte Eingriffe sein, denn gewachsene Strukturen müssen verändert und Standards neu gedacht werden. Bequeme Abläufe, etwa der Fernzugriff von diversen Devices, sind ggf. nicht mehr ohne erweiterte Sicherheitsmaßnahmen möglich.

Wie man Cyber-Angriffen vorbeugen kann

Eines der größten Probleme im Zusammenhang mit der Prävention von Cyber-Attacken ist es zu erkennen, dass man unter Beschuss genommen wird oder die Infrastruktur eventuell schon korrumpiert wurde. Dafür wird als Teil des ISMS ein Incident Management benötigt, das Vorfälle konsistent aufzeichnet. Allerdings besteht eine Herausforderung darin, Sensoren an den richtigen Stellen anzubringen und die wichtigen von den unwichtigen Meldungen zu trennen. Ähnlich einem IPS/IDS-System (Intrusion Detection und Intrusion Prevention) entsteht ein Datenaufkommen, das in den meisten Fällen nicht mit gängigem Know-how gefiltert werden kann. Daher wird ein SIEM (Security Information and Event Management) nötig: In diesem können alle relevanten Daten aus Security-Instanzen geordnet, gesammelt und mit Zeitstempel versehen ausgewertet werden. Damit können aus Ereignissen, die für sich genommen nicht kritisch erscheinen, aber in Kombination mit anderen kumulierten Prozessen und Veränderungen, Angriffsmuster erfasst, ausgewertet und entschärft werden.

Außerdem ist es wichtig, von Beginn an Szenarien zu antizipieren und Prozesse vorbereitet zu haben, die im Worst Case zum Einsatz kommen können, also eine Art Cyber-Notfall-Kit. Ein Unternehmen sollte zudem dazu fähig sein, zu entscheiden, ob es im Falle eines Angriffs weiter online bleibt oder offline geht und eine Unterbrechung des Betriebs in Kauf nimmt. Hat ein Unternehmen zu wenig Erfahrung im Umgang mit Angriffen, wird es die Systeme lieber komplett abschalten und die damit verbundenen Verfügbarkeits-Ausfälle in Kauf nehmen.

Dann muss das Ziel sein, ohne Gefährdung der Infrastruktur schnell wieder auf einer sauberen Basis online zu gehen. Nötig dafür ist ein nicht korrumpierter Zugang nach außen. Um die Infrastruktur wieder online zu bringen, ist hierzu eine vorbereitete Konfiguration sinnvoll. Diese kann schlicht aus einem Router, einer SIM-Karte mit LTE-Volumen und einer Handvoll Tools auf einem USB-Stick bestehen.

Unternehmen benötigen eine gute Sourcing-Strategie

Diese Sicherheitsmaßnahmen stellen für Unternehmen hohe Hürden dar: Sie installieren teure und aufwändige Technologien, müssen Prozesse aufsetzen, die bis zur Automatisierung viel

Jürgen Bruder, CSO/Leiter Cyber- & Informationssicherheit, TÜV Technische Überwachung Hessen GmbH

Nadja Müller, IT-Journalistin, Wordfinder PR

Manpower verschlingen und sind dann oft immer noch nicht in der Lage, Bedrohungen realistisch einzuschätzen. Um den Anforderungen gerecht werden zu können, benötigen Unternehmen deswegen eine gute Sourcing-Strategie und Klarheit darüber, was sie inhouse selbst übernehmen und welche Tasks sie outsourcen wollen. Der Aufwand zum Beispiel für das Incident Management ist oft so hoch, dass es sich wenigstens teilweise empfiehlt, es extern zu vergeben. Zudem sind Scheuklappendenken und Betriebsblindheit oft stark verbreitet, Das macht es wichtig, eng mit einem Dienstleister zusammenzuarbeiten, der eine breite Expertise und Erfahrung vorweisen kann. Gefragt ist hierbei die Kombination verschiedener Kenntnisse: Einerseits fundiertes Know-how zur Anlagensicherheit, andererseits tiefes Verständnis für aktuelle Cyber-Bedrohungen.

Darüber hinaus brauchen Dienstleister entsprechende Berechtigungen. Denn Störfälle betreffen nicht nur IoT-Anwendungen, sondern auch das OT-Umfeld. Die Sourcing-Strategie umfasst deshalb ein Service Level Agreement (SSA). Unternehmen brauchen die juristische wie technische Expertise für den Fall, dass der Dienstleister nicht leisten kann. Gerade im Cyber-Bereich treten häufig breitflächige Kumulschäden auf. Das ist dann der Fall, wenn ein und derselbe Cyber-Angriff eine Vielzahl von Infrastrukturen betrifft. So kann es passieren, dass der Dienstleister verschiedene Kunden hat, die aber alle von einem Schaden betroffen sind, was selbst ein großes Haus überlastet.

Ausblick

Zur Umsetzung der Empfehlungen der KAS-44 bietet sich eine externe Beratung für Unternehmen an – insbesondere für jene, die mit den Maßnahmen der IT-Sicherheit noch am Anfang stehen und zudem nicht über die personellen Ressourcen verfügen, um dieser Aufgabe gerecht zu werden. Externe Anbieter können Schwachstellen schnell identifizieren und bei den umfangreichen Aufgaben wie der Erstellung von Asset Register, dem Risiko- und Incident Management sowie der Erkennung von Security-Vorfällen zur Seite stehen, um die Sicherheit der IT-Anlagen systematisch zu verbessern. Unternehmen steigern damit ihre Produktionssicherheit und minimieren ihr Ausfallrisiko. So hilft externes Know-how aus Anlagen- und Cyber-Sicherheit dabei, gleichzeitig Kosten und Zeit zu sparen und die Wirtschaftlichkeit zu optimieren.

Jürgen Bruder, Nadja Müller

Manifesto For a Quantum Leap with Quantum Computers

Right now is a rare moment in human history, comparable to the invention of fire-making, artificial intelligence, or genetic scissors. Quantum computing is here, and with it, the question: How will we reinvent ourselves with it? Before we reject this quantum physical, historical chance, we should first take stock.

Yes, many people are experiencing exhaustion as a result of digitalization. Given the existence of ever-faster machines, and their commercialization as human beings, people no longer feel they are being taken on board.

A programmer said to me the other day: "The world is already under stress. What good is Quantum Computing if we tear ourselves apart as humanity?" True, we humans have been suffering from ourselves since Prometheus stole fire from the gods. Population growth, environmental degradation, political unrest, oppression, terrorism, trade war, irrationality, genetic manipulation. And also: Overtaxing humankind with technology and the associated isolation.

But this time it is different. The sacred quantum country has opened its doors. Ahead of us is a green meadow. And we can put our engineering skills, our thinking, and our chances as humanity once again entirely back to zero hours and accept the challenge.

This time it's not just about unbeatable cryptography, ingenious database searches, and military and metabolic simulations. This time it is in our hands to use the technical means to answer the delicate, complex questions of humanity in a sustainable, commercially successful, and human-friendly advanced way.

So please let us not focus on the race between nations, companies, and vain scientists. Of course, such developments are always about money, system supremacy, and superior benefits. But it is up to us to develop our world with this revolutionary Ultima Ratio Technique. Let's imagine and simulate together – and at the same time exponentially faster and more efficiently – how we can live together fantastically.

Instead of immediately commercializing this super-thought away or breaking it down into patent disputes like prey, we can make the discovery a cross-national field of reconciliation. What if we collect the big questions of humanity worldwide and then answer them with the help of quantum computers? Only then will we be able to find ways in which diversity and coexistence, technology and being fully human can coexist and make sense.

Let us write history together with quantum computers.

Uwe Walter is a storytelling and change expert for media and industrial enterprises. He advises clients as diverse as YouTube stars, start-ups, bloggers, publishers, radio and television stations and film productions. His expertise: How do I generate reach through future-proof storytelling?

Photo: personal

After the presentations, there was a panel discussion with (from left to right): Dr. Christian Braun (CIO Stadtsparkasse), Ulf Hollinderbäumer (Cassini Consulting AG), Eduardo Morral (Co-Founder and Managing Director Teratrace GmbH), Benjamin Wimmer (Senior Consultant at Cassini Consulting AG) and Klaus Illigmann, Head of Department HA I/2 "Population, Housing and PERSPECTIVE MUNICH")

Dr. Christian Braun, CIO Stadtsparkasse, presented the challenges and opportunities of banking in the age of digitalization.

MUNICH

Digitale Stadt München e. V.

DigiTalk – "Data, Platforms, Digital Fitness: The Enablers of SmartCity"

On Thursday, 24,10.2019, the DigiTalk "Data, Platforms, Digital Fitness: The Enablers of SmartCity" took place in the DigitalCenter of the Munich Stadtsparkasse, at Marienplatz. Uksa Bhatti, customer consultant at Stadtsparkasse München, and Benjamin Wimmer, head of the Smart City working group at Digitale Stadt München and senior consultant at Cassini Consulting AG, led through the programme and the evening. Dr. Christian Braun, CIO Stadtsparkasse, gave an impressive insight into the challenges and opportunities of banking in the age of digitalisation.

MünchenTV also reported on the DigiTalk at the Stadtsparkasse München.

The large hall of the DigitalCenter of the Stadtsparkasse München houses various "digitization islands" that provide digital banking services to citizens.

Photos: Digitale Stadt München e. V.

ADVISORY BOARD

Patric Fedlmeier
CIO Provinzial Rheinland

Norbert Gaus
Executive VP SIEMENS

Sandro Gaycken
Direktor ESMT

Michaela Harlander
Vorstand Harlander-Stiftung

Markus Heyn
GF BOSCH

Martin Hofmann
CIO Volkswagen

Manfred Klaus
Sprecher der GF Plan.Net

Andrea Martin
CTO IBM

Niko Mohr
Partner McKinsey

Christian Plenge
BL Messe Düsseldorf

Frank Rosenberger
Group Director TUI

Ralf Schneider
CIO Allianz Group

Stephan Schneider
Manager Vodafone

Marc Schröder
GL MG RTL Deutschland

Uwe Walter
Waltermedia

Michael Zaddach
Flughafen München

IMPRESSUM

VERLAG
Vogel Communications Group GmbH & Co. KG, Max-Planck-Str. 7/9, 97064 Würzburg, www.vogel.de
Geschäftsführer
Matthias Bauer, Florian Fischer, Günter Schürger

REDAKTION
Chefredaktion Claudia Linnhoff-Popien (V. i. S. d. P.)
Chef vom Dienst Robert Müller
Fachbeirat Patric Fedlmeier, Norbert Gaus, Sandro Gaycken, Michaela Harlander, Markus Heyn, Martin Hofmann, Manfred Klaus, Andrea Martin, Niko Mohr, Christian Plenge, Frank Rosenberger, Ralf Schneider, Stephan Schneider, Marc Schröder, Uwe Walter, Michael Zaddach
Redaktion Hannes Mittermaier
Blog Steffen Illium, Tanja Zecca, Tamara Tomasevic
Redaktionsassistenz Katja Grenner
Mitarbeiter dieser Ausgabe Thomy Phan, Kyrill Schmid
Schlussredaktion Mona Beach/Starfish Digital

ANFRAGEN AN DIE REDAKTION
redaktion@digitaleweltmagazin.de

GRAFIK
Layout Stefan Stockinger, www.stefanstockinger.com

ANZEIGEN
Ansprechpartner Tanja Zecca, Tel. +49 89 2180-9171, E-Mail: anzeigen@digitaleweltmagazin.de
Es gilt die gültige Preisliste, Informationen hierzu unter www.digitaleweltmagazin.de/mediadaten

HERSTELLUNG
ColorDruck Solutions GmbH, Gutenbergstraße 4, 69181 Leimen

ABO-SERVICE
DataM-Services GmbH, Aboservice Digitale Welt, Franz-Horn-Str. 2, 97082 Würzburg,
Tel. +49 931 4170-435
E-Mail: abodigitalewelt@vogel.de
Digitale Welt erscheint einmal pro Quartal

ABONNEMENT-PREISE
Jahres-Abo inklusive Versandkosten: Inland 78,00 €, Ausland 87,60 €; ermäßigtes Abo für Schüler, Studenten, Auszubildende: Inland 39,00 €
Der Bezug der Zeitschrift Digitale Welt ist im Mitglieds-Beitrag des Verbandes VOICE - Bundesverband der IT-Anwender e.V., Digitale Stadt München e.V. und Hannover IT e.V. enthalten.

HERAUSGEBER
Prof. Dr. Claudia Linnhoff-Popien, Institut für Informatik, Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 München,
Tel. +49 89 2180-9153, www.digitaleweltmagazin.de

CALL FOR CONTRIBUTION

for DIGITALE-WELT-Blog

The next DIGITALE WELT will be released on 03.06.2020

Become part of our top-class authorship and place your digital topics of tomorrow on today's platform with over **1,000,000*** clicks so far.

OUR TOPICS ARE:

- ✓ **Machine Learning**
- ✓ **Quantum Computing**
- ✓ **Internet of Things**
- ✓ **Blockchain**
- ✓ **Cyber Security**
- ✓ **Human Resources**

ARE YOU INTERESTED?
Then do not hesitate to contact the DIGITALE WELT-Office via email: **blog@digitaleweltmagazin.de**

***Our articles were published online at www.digitaleweltmagazin.de/blog and achieved the above-mentioned number of clicks in the period 01. August 2017 – 27. January 2020.**

Guide to the publication of technical papers

PLEASE NOTE THE FOLLOWING POINTS FOR YOUR SUBMISSION:

1. Your paper meets the following requirements:
   - Focuses on the key topics of DIGITALE WELT
   - Title (max. 60 characters incl. spaces)
   - Blog post length: 7,000-15,000 characters including spaces
   - Full article length: 15,000 - 40,000 characters including spaces
   - Written exclusively for DIGITALE WELT
   - All graphics and pictures are free of rights
   - Does not contain any advertising
2. CV and picture of the author:
   To introduce you as an author we need:
   - Your full name
   - Any academic titles
   - Position in the company (max. 40 characters)
   - Name of your company (max. 25 characters)
   - Portrait image with min. 300 DPI resolution
   - CV with max. 300 characters incl. spaces
3. Consent to Publish:
   For publication in print & online media, we require the fully completed and signed declaration of consent. Please find it at digitaleweltmagazin.de/consent

YOU WILL BENEFIT FROM THE FOLLOWING SERVICES:

- Your high-quality contribution will be published in our Online Blog of the DIGITALE WELT Magazine
- The best contributions are to be published in our print magazine, additionally
- High range by distribution via Social Media
- This service is of course free of charge for you

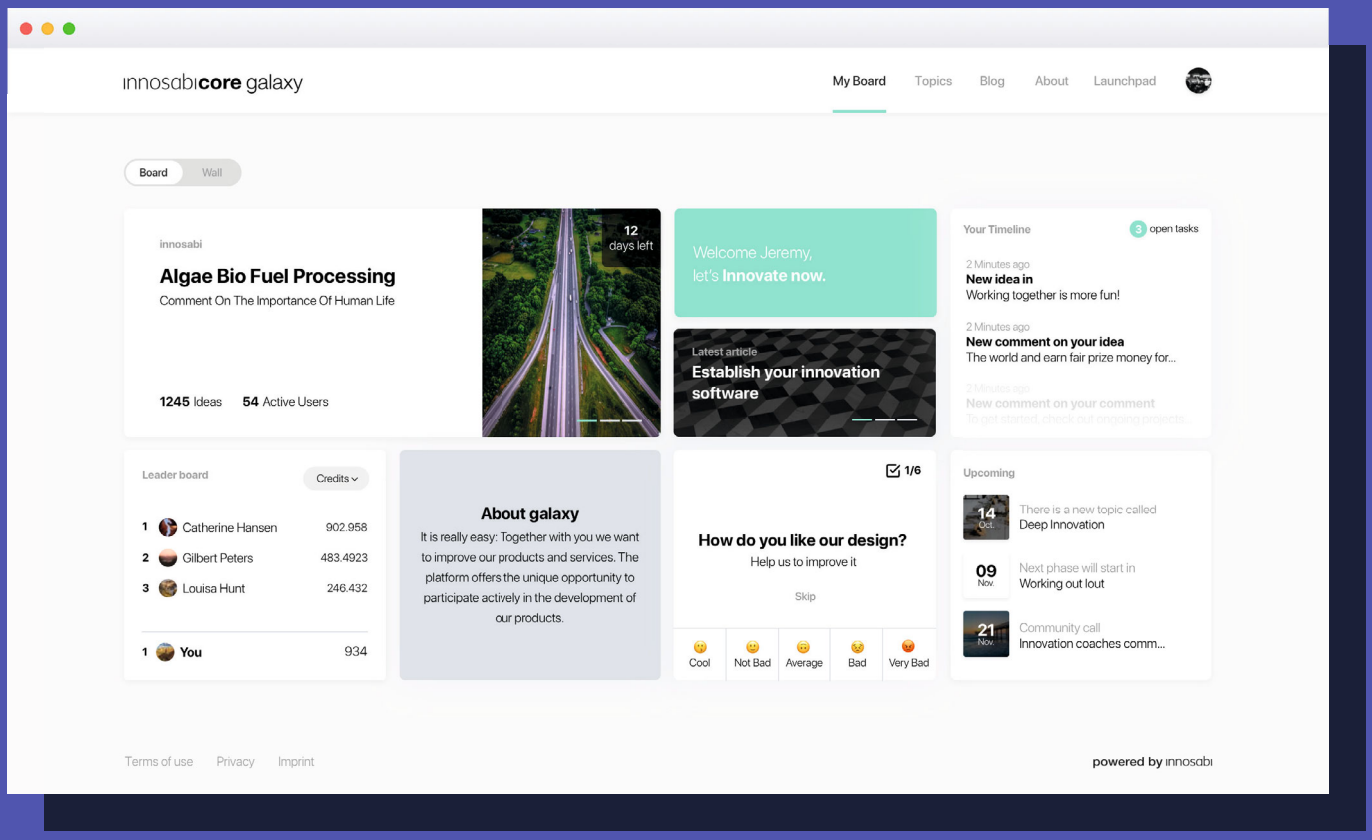
Send us your complete documents by use of our online form at **digitaleweltmagazin.de/submit**

A listing of our current and past "Call-For-Contributions" can be found at digitaleweltmagazin.de/calls

We look forward to your technical contribution with your expert knowledge.

Your DIGITALE WELT Team

innosabi**core** galaxy



Connecting sparks of genius

Für noch mehr Innovation und Kollaboration in deinem Unternehmen.
Bring alle Stakeholder zusammen und schaffe einen zentralen Anlaufpunkt für dein Ökosystem.
Die einzige Software, die du dafür brauchst:
innosabi core galaxy.

Innovation war noch nie so einfach.
innosabi.com

Pioneers in Artificial Intelligence

HYVE

Create AI-powered business solutions & products with HYVE, the leading innovation company.

TAWNY

Revolutionize human-machine collaboration with TAWNY, the award-winning Emotion AI startup.

We are your partner to start your Emotion AI journey!

hyve.net

+ 49 89 189081 - 100

info@hyve.net

tawny.ai

+ 49 89 189081 - 402

info@tawny.ai

Haus der Innovation, Schellingstraße 45, 80799 Munich, Germany