DAS WIRTSCHAFTSMAGAZIN ZUR DIGITALISIERUNG

DIGITALE WELT

ZUKUNFT | EINFACH | ENTDECKEN

Ausgabe 2 ▪ April ▪ Mai ▪ Juni ▪ **2019**

Special Issue on Quantum Computing

Quantum Computing –
Quantum Technology and Optimization Problems

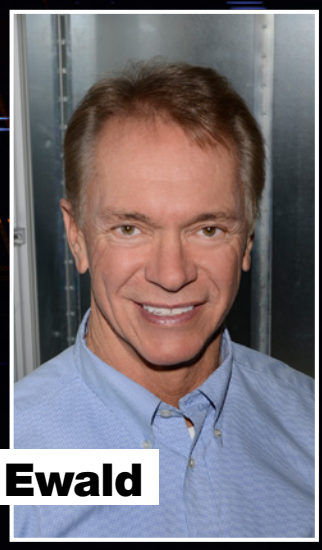
Analytics
Benchmarking and Hybrid Solution Methods

Visions
Machine Learning in the Quantum Era

Use Cases
Quantum Algorithms for Industry and Game Theory

CYBER SECURITY

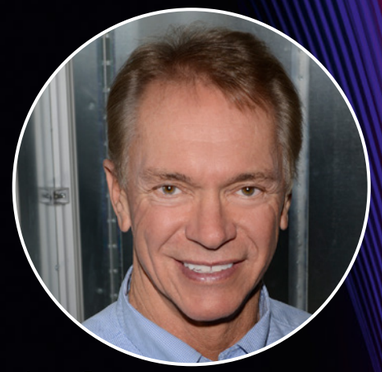
Managing Information Security in the Cloud



The President of D-Wave Systems on the future of QC

Bo Ewald

€ 19,50
€ 21,90



16 **HINTER DEN KULISSEN**
D-Wave Systems: In five years the future will arrive

86 **SZENE**
München

Die nächste DIGITALE WELT erscheint am 05.06.2019

Titel: Dmitriy Rybin&Shutterstock, Privat Fotos: Dmitriy Rybin&Shutterstock, Privat, Digitale Stadt München e.V.

PROF. DR. CLAUDIA LINNHOFF-POPIEN
Prof. Dr. Claudia Linnhoff-Popien holds the chair „Mobile and Distributed Systems“ at the Ludwig-Maximilians-Universität in Munich. She finished her Ph.D. thesis at the Technical University Aachen and gave lectures at the University GH Essen. She did postdoctoral research at the Washington University of St. Louis, Missouri, USA before she was appointed to a professorship at the LMU Munich in 1998. She is board member of the Institute for Informatics, member of the „Münchner Kreis“ and co-founder of the ALOQA GmbH. The latter had one million registered users when it was sold to Motorola Mobility in 2010 marking one of the biggest exits in the history of start-ups of German universities. Further, she is head of the lead project „Innovationszentrum Mobiles Internet“ of the Zentrum Digitalisierung. Bayern (ZD.B) funded by the state of Bavaria. She is also scientific advisor of the VIRALITY GmbH and chair of Digitale Stadt München e.V.

Quantum Computing – a new hype?

Quantum Computing is a key technology of the 21st century. Currently we are in the middle of the second quantum revolution. Nearly a century ago Albert Einstein, Nils Bohr, Werner Heisenberg, and many others laid the foundations of quantum physics. Any attempt by a computer scientist to understand these physics will most probably fail. This technology is now in the process of entering the world of computers. The opinions about quantum computing today range from “not even started” to “totally successful”.

Do you work for a company which plays along with every hype? Which always strives to be at the forefront of innovation? To be considered as being innovative, to be one step ahead of the competition, to recognize disruptive technologies which are created to generate platform business as much as possible in order to lay the foundation for the future? Many of these “seedlings”, established with vast resources and much euphoria, have grown into large enterprises, especially in the area of digitalization.

Often, however, such a vision is only hype. Many technologies are just too complex, require too much intervention in the infrastructure, or are just not readily accepted by the market. Blockchain is a prime example. Many business units have been created around consultation and implementation of Blockchain technology. Yet this technology is so storage-consuming and computing-intensive that it is suited mainly for the finance sector. Even the Bitcoin-US-Dollar rate climbed to almost 20,000 dollars by the end of 2017, only to crash below 4,000 dollars just over a year later.

What, however, is the situation with Quantum Computing?
This completely new technology has been rapidly gaining visibility in the last few years. While the basis of quantum mechanics spent almost 100 years being of more theoretical than practical relevance, now that they enable new applications in IT, the time has come when more or less all companies are diving into it.

Let us begin with the foundation – the hardware. Numerous companies claim to build quantum computers and to offer the technology in widely varying architectures. IBM already offers its customers the first solutions in form of a Quantum Gate Model, which is still very limited in storage and computing capacity. Moderate performance capacities are freely accessible and the IBM Q Hub provides an interface for the application of this computer model and is being made available to large enterprises. The providers Google and Microsoft are testing comparable computers whose utilization has so far been restricted to laboratories. The Canadian company D-Wave achieved a breakthrough in the maturity of quantum technology during the last few years with a Quantum Annealer This implementation of so-called adiabatic computing is suitable for a first practical utilization. Fujitsu is exploring the possibility of a practical use of the technology, but is relying on classical hardware elements in which not the technical novelty, but rather the embedding in a larger service package plays the crucial role.

The prices for this technology move in rather large circles – this is understandable because Research and Development are a high cost factor when you consider the extremely low number of units of the machines sold. For access to an IBM Q Hub a contract at a six-figure price can be negotiated and you pay a low eight-figure price

QTOP

First International Workshop on Quantum Technology and Optimization Problems (QTOP'19)

Garching/Munich, Germany, March 18, 2019
In cooperation with NetSys 2019, https://netsys2019.org/workshops/qtop19

QTOP Workshop – Schedule

09.00 - 09.10 **Conference Opening**
Sebastian Feld (LMU Munich, Germany),
Claudia Linnhoff-Popien (LMU Munich, Germany)

09.10 - 09.50 **Keynote**
An Introduction to Quantum Computing and its Application
Robert H. (Bo) Ewald (D-Wave Systems, Canada)

09.50 - 10.45 **Session 1: Analysis of Optimization Problems**
Session Chair: Michel Barbeau, Carleton University, Canada
Embedding inequality constraints for quantum annealing optimization
Tomás Vyskocil (Los Alamos National Laboratory, USA), Scott Pakin (Los Alamos National Laboratory, USA), Hristo N. Djidjev (Los Alamos National Laboratory, USA)
Assessing Solution Quality of 3SAT on a Quantum Annealing Platform
Thomas Gabor (LMU Munich, Germany), Sebastian Zielinski (LMU Munich, Germany), Sebastian Feld (LMU Munich, Germany), Christoph Roch (LMU Munich, Germany), Christian Seidel (Volkswagen Data:Lab, Germany), Florian Neukart (Volkswagen Group of America, USA), Isabella Galter (Volkswagen Data:Lab, Germany), Wolfgang Mauerer (OTH Regensburg; Siemens Corporate Research), Claudia Linnhoff-Popien (LMU Munich, Germany)
Principles and Guidelines for Quantum Performance Analysis
Catherine C. McGeoch (D-Wave Systems, Canada)

10.45 - 11.15 **Coffee Break**

11.15 - 12.30 **Session 2: Quantum Gate Algorithms**
Session Chair: Sebastian Feld, LMU Munich, Germany
Nash embedding and equilibrium in pure quantum states
Faisal Shah Khan (Khalifa University, Abu Dhabi), Travis S. Humble (Oak Ridge National Lab, USA)
A Quantum Algorithm for Minimising the Effective Graph Resistance upon Edge Addition
Finn de Ridder (Radboud University, Netherlands), Niels Neumann (TNO, Netherlands), Thijs Veugen (TNO, Netherlands; CWI, Netherlands), Robert Kooij (Singapore University of Technology and Design, Singapore; Delft University of Technology, Netherlands)
Variational Quantum Factoring
Eric Anschuetz (Zapata Computing, USA), Jonathan Olson (Zapata Computing, USA), Alán Aspuru-Guzik (Zapata Computing, USA), Yudong Cao (Zapata Computing, USA)
Function Maximization with Dynamic Quantum Search
Charles Moussa (TOTAL American Services, USA; Oak Ridge National Laboratory, USA), Henri Calandra (TOTAL SA, France), Travis Humble (Oak Ridge National Laboratory, USA)

12.30 - 13.30 **Lunch Break**

13.30 - 15.15 **Session 3: Applications of Quantum Annealing**
Session Chair: Catherine C. McGeoch, D-Wave Systems, Canada
Flight Gate Assignment with a Quantum Annealer
Tobias Stollenwerk (DLR, Germany), Elisabeth Lobe (DLR, Germany), Martin Jung (DLR, Germany)
Solving Quantum Chemistry Problems with a D-Wave Quantum Annealer
Michael Streif (Volkswagen Group, Germany), Florian Neukart (Leiden University, Netherlands; Volkswagen Group of America, USA), Martin Leib (Volkswagen Group, Germany)
Solving large Maximum Clique problems on a quantum annealer
Elijah Pelofske (Los Alamos National Laboratory, USA), Georg Hahn (Lancaster University, UK), Hristo Djidjev (Los Alamos National Laboratory, USA)
Quantum Annealing based Optimization of Robotic Movement in Manufacturing
Arpit Mehta (BMW AG, Germany), Murad Muradi (BMW AG, Germany), Selam Woldetsadick (BMW AG, Germany)
Quantum Annealing of Vehicle Routing Problem with Time, State and Capacity
Hirotaka Irie (DENSO Corporation, Japan), Goragot Wongpaisarnsin (Toyota Tsusho Nexty Electronics, Thailand), Masayoshi Terabe (DENSO Corporation, Japan), Akira Miki (DENSO Corporation, Japan), Shinichirou Taguchi (DENSO Corporation, Japan)
Boosting quantum annealing performance using evolution strategies for annealing offsets tuning
Sheir Yarkoni (D-Wave Systems, Canada; Leiden University, Netherlands), Hao Wang (Leiden University, Netherlands), Aske Plaat (Leiden University, Netherlands), Thomas Bäck (Leiden University, Netherlands)

15.15 - 15.45 **Coffee Break**

15.45 - 17.15 **Session 4: Foundations and Quantum Technologies**
Session Chair: Wolfgang Mauerer, OTH Regensburg, Germany
Quantum Photonic TRNG with Dual Extractor
Mitchell A. Thornton (Southern Methodist University, USA), Duncan L. MacFarlane (Southern Methodist University, USA)
Secure Quantum Data Communications Using Classical Keying Material
Michel Barbeau (Carleton University, Canada)
Continuous-variable Quantum Network Coding Against Pollution Attacks
Tao Shang (Beihang University, China), Ke Li, Ranyiliu Chen (Beihang University, China), Jianwei Liu (Beihang University, China)
On the Influence of Initial Qubit Placement During NISQ Circuit Compilation
Alexandru Paler (Johannes Kepler University, Austria)
Towards a Pattern Language for Quantum Algorithms
Frank Leymann (University of Stuttgart, Germany)

General Chairs

Sebastian Feld	LMU Munich, Germany
Claudia Linnhoff-Popien	LMU Munich, Germany

Program Committee

Nick Chancellor	Durham University, UK	Luke Mason	Science & Technology Facilities Council, UK
Bo Ewald	D-Wave Systems, Canada	Wolfgang Mauerer	OTH Regensburg, Germany
Markus Friedrich	LMU Munich, Germany	Catherine C. McGeoch	D-Wave Systems, Canada
Thomas Gabor	LMU Munich, Germany	Masayuki Ohzeki	Tohoku University, Japan
Markus Hoffmann	Google, Germany	Jonathan Olson	Zapata Quantum Computing, USA
Faisal Shah Khan	Khalifa University, Abu Dhabi	Dan O'Malley	Los Alamos National Laboratory, USA
Dieter Kranzlmüller	LRZ, Germany	Tobias Stollenwerk	DLR, Germany

for a Quantum Annealer, or rent it as a cloud-service with a fixed quota of computing capacity. In this case, you are talking about a four-figure sum for several months of participation. So, dare to tackle the adventure, find the right concept according to your requirements and test it for your company.

This brings us to the real problem – how to implement. This consists of two phases.
For a start, you need an expert inside or outside of the company, with whom you can collaborate, who shows you the possible areas quantum technology can be used for in your enterprise. Make yourself familiar with, and identify areas in which quantum technology can be used to solve optimization problems. Look at examples from other industries and learn from success stories! Adapt the highly complex and difficult to scale mathematical problems to the specific conceptual formulations of your environment and determine where you can achieve this "wow-effect", when you can see where you can solve the problem with quantum technology.

Begin with the absolute classics – with the travelling salesman problem, in which a salesperson has to travel to, for example, five locations by choosing the optimal route to deliver the products. This optimization problem is the basis of programming an industrial robot, which has to, for example, place five welding spots in the optimal sequence, and, at the same time, cover the least distance. Consider the rucksack problem, or the graph-coloring problem. In live situations, these task definitions can then be used for the gate allocation problem in which the gates at an airport are assigned optimally to airplanes, or to portfolio optimization in the financial sector, or the optimal placement of commercials in the breaks of a TV program. These are all apparently small modules, which are integrated into the large unit. However, they require huge amounts of computing time, if they are not practically insolvable for a sufficient number of cities, points, gates, shares, and advertising clips. Start with these kinds of modules! Look for applications in your everyday business situations, for which you can identify suitable optimization issues. Reserve a small budget and look at applications and solutions, you carry very little risk in this case.

It takes more courage, however, to tackle a major project. In mid-2018, I ran across a press release by Microsoft and DEWA. DEWA (Dubai Electricity and Water Authority) is a company, which is comparable to our domestic public utilities, as it supplies Dubai with grids and infrastructure. This press release stated that the city of Dubai was to be supplied with quantum-based solutions in order to optimize the infrastructure. In the context of a presentation at an international quantum congress in Abu Dhabi, I took a detour to Dubai and talked to a colleague. This is a genuinely big project! With the help of international experts, the attempt was made to solve it. There are no results yet, but the large goal produces large ambitions.

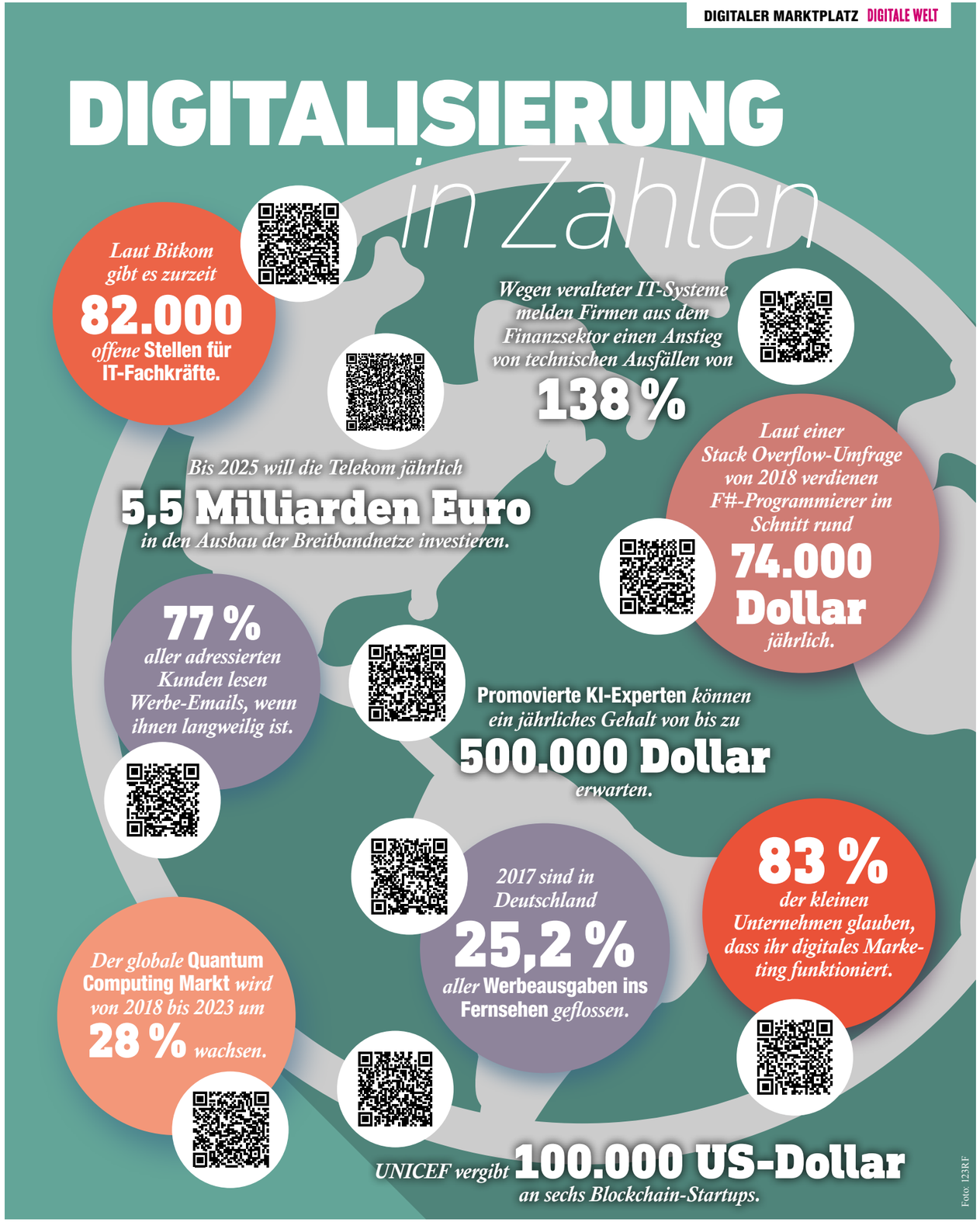
This is the future! Trained experts of tomorrow are required! It is foreseeable that a huge demand will exist within a few years. In our title story "In five years the future will arrive", Bo Ewald states that the technology is very close to breakthrough. University graduates in five years are the beginners of today. We therefore have to act today, and that is why we are doing it! During the summer semester of 2018, I started to include Quantum Computing in the traditional lectures on "Computer Architecture". 500 – 700 computer science students of the LMU Munich not only learn the traditional von Neumann model every year, but also get the chance to program a D-Wave Quantum Annealer.

They do not work on a simulator or a "quantum-inspired" computer, but on a genuine Quantum Annealer. They learn to write down an Ising formula and to fill out a QUBO matrix, that is, to "feed" the computer.

So, what will our world look like in five years?
Quantum computers today are not yet capable of being used in a highly scalable manner for optimization problems. However, they have something in common with traditional computing technology there – hardware is doubling continuously, we can observe exponential growth, even if it is at an early stage. That is why there is reason for hope that soon a valuable technology will be available on the market. This would be especially suitable for optimization issues. There will be traditional computers as well as quantum computers in a universal infrastructure, in case of optimization, the quantum computer will be of great advantage. Problems which so far have been practically unsolvable will be able to be solved in a manageable timeframe.

What does this mean for your enterprise?
Now is the time to be occupied with quantum computing. Learn to understand problem situations from the viewpoint of quantum computing, and to recognize when a computer of this kind will be an advantage. Observe which problem situations exist within your organization, which would be suitable for quantum computing. Start early in bringing a small problem onto a computer of this kind, or to several computer families. Grow with quantum technology, and, in case you do not have the capacity, find a partner who will accompany you on this exciting journey as early as possible.

For more information on this subject, please feel free to visit our QAR-Lab, see:
http://www.mobile.ifi.lmu.de/qar-lab/. We are looking forward to your visit!



Very digital Person:

FREDMUND MALIK

Komplexität: Rohstoff der neuen Zeit

Anlässlich des Vortrags von Bestseller-Autor Prof. Dr. Fredmund Malik bei der DIGICON 2018 haben wir mit ihm ein Gespräch über ganzheitliche Managementmethoden im Zeitalter der digitalen Transformation geführt.

Was erwarten Sie sich von der DIGICON? Worüber werden Sie sprechen?

Ich erwarte mir von der DIGICON, dass sich die Forschung auf dem allerneuesten Stand präsentiert und sie einem breiteren Publikum zugänglich gemacht wird. In meinem persönlichen Beitrag werde ich darüber sprechen, wie die Digitalisierung in Organisationen passt und welche Herausforderungen dadurch entstehen, insbesondere beim Management von Digitalisierungsprojekten.

Was ist Ihre Definition von Digitalisierung?

Der Begriff „Digitalisierung" selbst ist ja gewissermaßen irreführend, denn die Digitalisierung haben wir im Grunde, seit es funktionierende Transistoren gibt. Heute können wir alles mit allem global vernetzen und diese Vernetzung ist das entscheidend Neue an der Digitalisierung; nicht das Digitale. Durch diese Vernetzung werden die beiden ganz großen dominierenden Koordinatoren der Menschheit bedeutungslos; nämlich Raum und Zeit. Das bringt eine Veränderung unseres Weltbildes wie bei Kopernikus. Nur diesmal ist es für das Leben der Menschen von direkter Relevanz. Denn ob wir in einem heliozentrischen oder einem geozentrischen Weltbild leben, hatte für den Alltag des Weinbauern aus der Toskana zur Zeit von Galileo und Kopernikus eigentlich keine Bedeutung. Daher müssen Führungskräfte weit in die Zukunft denken, Szenarien bauen, die Strategien dazu entwerfen, und wenn es dann weniger wuchtig kommt, umso besser. Doch es ist gefährlich diese Dinge zu unterschätzen, wie das etwa Kodak in den Neunzigerjahren mit der digitalen Fototechnik getan hat. Das passiert, weil die meisten Men-

„Ohne Kybernetik hätten wir beispielsweise keine Fahrerassistenzsysteme in Autos, keine funktionierenden Intensivstationen und keinen funktionierenden Flugverkehr."

schen im Neuen oft nur das Alte sehen. Es genügt also nicht zu sehen, es erfordert einen Erkenntnisakt, und erst wenn dieser erfolgt ist, kann man beginnen Strategien zu entwickeln.

Was meinen Sie, wenn Sie von einem holistischen Management-Ansatz sprechen?

Ich gebe Ihnen ein Beispiel: Eltern sind holistisch denkende Menschen. Wenn sich ein Kind etwa beim Fahrradfahren ein Knie aufschlägt, dann gehen die Eltern nicht sofort in die Klinik, sondern sie tragen das Pflaster selber auf. Natürlich gibt es Verletzungen, bei denen man wirklich zum Arzt muss. Aber man muss nicht gleich alles in Spezialgebiete aufteilen. Ein Unternehmer muss ebenfalls holistisch denken, denn ein Unternehmen kann man nur als Ganzes verstehen und lenken. Die Arbeitsteilung in den Wissenschaften ist nötig, weil wir die Fachdisziplinen natürlich brauchen. Aber wir brauchen auch ein Zusammenspiel. Die Leitung von Entwicklungsabteilungen in der Pharmaindustrie liegt daher beispielsweise sehr häufig in der Hand von Medizinern, anstatt in den einzelnen Fachdisziplinen, weil der Fokus weiterhin der Patient ist, also das Ganze. Das heißt für die Wirtschaft, dass man versuchen muss, sich am Kunden zu orientieren und diesen zufrieden zu stellen.

Woher kommt dieser holistische Ansatz?

Die Grundlagenwissenschaft hierzu sind die Komplexitätswissenschaften. Hier wiederum sind vor allem die Systemwissenschaften, die Kybernetik und die Bionik zu erwähnen. Wir versuchen also, aus der belebten Natur und aus den Ergebnissen der Evolution Erkenntnisse zu gewinnen, welche wir auf menschliche Organisationen übertragen können. Kybernetisches Management heißt demnach, die Erkenntnisse dieser Komplexitätswissenschaften einerseits technisch für die Computer und die Digitalisierung anzuwenden, andererseits auf die Organisationen: Regulierung, Lenkung und Steuerung, insbesondere selbst regulieren, selbst organisieren und selbst lenken sind die Fähigkeiten, die wir bei Organismen in der gesamten belebten Welt sehen. Die Computer nähern sich daran an und beides hat seine Wurzeln in der Kybernetik.

„Heute können wir alles mit allem global vernetzen und diese Vernetzung ist das entscheidend Neue an der Digitalisierung; nicht das Digitale. Durch diese Vernetzung werden die beiden ganz großen dominierenden Koordinatoren der Menschheit bedeutungslos; nämlich Raum und Zeit. Das bringt eine Veränderung unseres Weltbildes wie bei Kopernikus.“

Wo findet Kybernetik schon praktische Anwendung?

Ohne Kybernetik hätten wir beispielsweise keine Fahrerassistenzsysteme in Autos, keine funktionierenden Intensivstationen und keinen funktionierenden Flugverkehr. Um Letzteres noch etwas näher auszuführen: Durch die Art, wie weltweit Air Traffic Control ausgeübt wird, gibt es so gut wie keine Unfälle. Gemessen an der Dichte des Flugverkehrs, an der Witterungsbelastung, den längst überlasteten Flughäfen, den zu geringen Pistenkilometern und anderen Unzulänglichkeiten, funktioniert das System trotzdem perfekt. Kybernetik ist also eine Universaldisziplin und manifestiert sich in spezifischeren Gebieten wie Biokybernetik. Doch das, was all diesen Disziplinen inhärent und gleich ist, sind diese selbstregulierenden Systeme. Der allerbeste Beweis dafür, dass Kybernetik funktioniert, ist, dass sie von Kriminellen angewandt wird, wie etwa beim Cybercrime. Es ist eine riesige Aufgabe für die Digitalisierung und für die „gute Kybernetik“, diese Kriminalität in Schach zu halten.

Was bedeutet das für das Management?

Management ist die bewegende Kraft überall dort, wo viele Menschen nur gemeinsam etwas erreichen können. Bei der heutigen hohen Komplexität in großen Organisationen geht es oft gar nicht mehr anders als mit kybernetischen Managementmethoden. Doch viel wichtiger als das Management von Mitarbeitern, ist das Managen von unten nach oben, also die Frage, wie man seinen Chef oder seine Chefin managt, sowie die Frage, wie man seine Kollegen managt, über die man kein Weisungsrecht hat.

Was ist der Schwachpunkt in den meisten Organisationen?

Wenn man ein typisches Organigramm anschaut, kann man die einzelnen Kästchen im Großen und Ganzen mit der Anatomie des Menschen vergleichen: das Herz, die Niere, der Magen und so weiter. Doch kein Organigramm hat ein Nervensystem! Das würde im Körper keine drei Sekunden funktionieren. Daher ist das Nervensystem, also die Kommunikation, der schwache Punkt in den Organisationen: Die Kommunikation wird der bestehenden Komplexität absolut nicht gerecht. In Organisationen müssen viele Menschen mit vielen Menschen kommunizieren und das betrifft alle Arten der technisch-gestützten Information, wie etwa E-Mails, und der nicht technisch-gestützten Information, wie etwa all die tausenden Sitzungen, die in Organisationen stattfinden. Das, was die DNA für die Zelle tut, nämlich die Organisation, Steuerung, Lenkung und Regulierung der Zelle zu bewirken, das tut das Nervensystem für den Organismus; in beinahe invarianter Weise: So ist etwa bei sämtlichen Säugetieren die Grundarchitektur von Nervensystemen an sich immer dieselbe. Das tun analog Operating Systems für Computer. Das heißt, die Operating Systems sind analog in ihrem Funktionieren und ihrer Struktur mit der DNA und den Nervensystemen. Sie befähigen ihre Organismen zu funktionieren: Das ist Management für Organisationen natürlich unter Zuhilfenahme von Computern und anderen technischen Stützen.

Sie haben die Methode des „Makro-Change Managements“ entwickelt. Was ist der Unterschied zwischen Ihrer Methode und dem „Mainstream Change Management“?

Wir sehen, wie instabil der digitale Wandel ist. Frühere, gut funktionierende, herkömmliche Change-Methodiken werden mit den heutigen Umständen einfach nicht mehr fertig. Vor Kurzem haben wir eine große Umfrage mit etwas mehr als 200 Führungskräften aus C-Level-Positionen durchgeführt, vor allem mit CEOs, CIOs und CDOs. Unsere Frage war: „Was lässt Sie nachts nicht schlafen?“ Eine Antwort von mehr als 80 Prozent war, dass den heutigen Herausforderungen mit den herkömmlichen Managementmethoden nicht mehr beizukommen ist. Eine zweite Antwort war – die ebenfalls von mehr als 80 Prozent angegeben wurde –, dass bisheriges Change-Management den großen, breitflächigen, tiefgreifenden Wandel verhindert. Denn, um Einstein hier zu zitieren: „Probleme kann man niemals mit derselben Denkweise lösen, durch die sie entstanden sind.” Die Kausalität von Change sagt ja: „Ändere zuerst die Menschen und dann werden sie anders handeln.“ Aber das funktioniert auf Dauer nicht, weil die Menschen gerne so bleiben möchten, wie sie sind. Ich habe also über Möglichkeiten nachgedacht, Menschen Instrumente in die Hand zu geben, welche die Angst davor, sich selbst ändern zu müssen, gar nicht erst aufkommen lassen. Jeder von uns hat das mit dem Handy erlebt: Das Handy hat uns die Möglichkeit gegeben, ganz neu zu kommunizieren, ohne dass wir uns als Vorbedingung dafür ändern mussten. Doch im Laufe der Zeit hat das Handy uns verändert. Um diesen Effekt immer wieder zu erzielen, haben wir die Syntegrationsverfahren entwickelt.

„Management ist die bewegende Kraft überall dort, wo viele Menschen nur gemeinsam etwas erreichen können. Bei der heutigen hohen Komplexität in großen Organisationen geht es oft gar nicht mehr anders als mit kybernetischen Managementmethoden.“

Wofür steht der Begriff „Syntegration”?

Syntegration ist ein Kunstwort aus Synergie und Integration. Mit dem Syntegrationsverfahren können wir aus der Enge des Kleinsystems ausbrechen: Denn wir brauchen relativ viele Menschen, um Organisationen handhaben zu können. Bei der Syntegration geht es um die Vernetzung: Man muss Menschen auf die richtige Art und Weise vernetzen. Diese Vernetzung muss ganz bestimmten, mathematischen Prinzipien entsprechen, weil sie sonst eher das Gegenteil bewirkt. An diesem Punkt müssen zwei wichtige Naturgesetze der Evolution genannt werden, nämlich Vernetztheit und Simultanität bzw. Synchronizität. Das heißt, das was wir mit bisherigen Methoden nur getrennt machen konnten, können wir mit dem Syntegrationsverfahren vernetzt machen. Was bisher sequenziell verlaufen ist, können wir jetzt simultan bewältigen, also gleichzeitig. Wenn vorher getrennte Dinge zusammenkommen, dann gibt es Innovation, Evolution und Kreativität.

Könnten Sie das bitte anhand eines Beispiels erklären?

Um ein Beispiel aus der Chemie zu nennen: Nimmt man Wasserstoff- und Sauerstoff-Atome und lässt sie getrennt, passiert gar nichts. Wenn ich sie richtig vernetze, gibt es Wasser. Wasser ist etwas radikal Neues. Das ist also evolutionäres Geschehen. Wenn ich die Atome jedoch falsch vernetze, dann entsteht etwas Schlechtes, ein explosives Gemisch – landläufig Knallgas genannt –, das sich selber zerstört. Es ist also eines der Ziele des Makro-Changes die Komplexität zu nutzen: Das bringt Überlegenheit und neue Qualitäten, wie sie auch in der Natur entstanden sind, denn alle höheren Eigenschaften resultieren aus mehr Komplexität. Komplexität ist demnach der neue Rohstoff der neuen Welt. Trotzdem wollen viele Führungskräfte und Mitarbeiter Komplexität immer gleich reduzieren. Manchmal ist das auch in Ordnung, denn natürlich können diese komplexen Prozesse auch empfindlich gestört oder missbraucht werden und es kann zu Zusammenbrüchen kommen. Aber vom Prinzip her wird uns die Nutzung von Komplexität neue Lösungen bringen. Gerade in einem auseinanderbrechenden Europa braucht man sie, weil sie rasch und zuverlässig wirken.

Wozu werden diese Syntegrationsverfahren konkret benutzt?

Die Syntegrationsverfahren führen zur schnellen und nachhaltigen Konsensbildung. Sie sind mindestens sechzig Mal so schnell, wie herkömmliche Kooperationsmethoden, weil sie simultan wirken. Es ist aber jeder Großguppen-Workshop ein Syntegrationsverfahren. Bei der Syntegration geht es nämlich um die gezielte, durchdachte und bewusste Anordnung von Menschen, so, dass sie sich in der richtigen Weise vernetzen können. Die Urformen davon gab es historisch gesehen beispielsweise schon in den Stammesgesellschaften.

Sie sprechen oft von der „Großen Transformation“. Könnten Sie das bitte näher ausführen?

Wir haben jetzt im Prinzip drei Welten, in denen wir leben müssen: Wir müssen trotz Digitalisierung in der bisherigen Welt weiterleben und brauchen dafür Strategien, denn diese Welt ist ja noch da. Zudem brauchen wir eine Strategie für die neue Welt, um neue Potenziale aufzubauen, damit wir sie haben, wenn die bisherigen Geschäftsformate oder auch die bisherige Politik einfach nicht mehr tauglich sind. Wir brauchen zudem eine dritte Denkweise, eine dritte Befähigung, nämlich für die große Transformation, also um von der alten in die neue Welt zu kommen. Die ist ja für alle neu: sogar für die Digitalisierungsspezialisten. Ich vergleiche das manchmal bildhaft mit der Geburt einer neuen Welt, denn es ist eine Metamorphose auf einem gigantischen Niveau.

Von Florentina Hofbauer

Fotos: Privat

Fredmund Malik

Fredmund Malik ist Autor von mehr als zehn preisgekrönten Bestsellern und rund 300 weiteren Publikationen. Sein Klassiker Managing Performing Living wurde unter den besten 100 Geschäftsbüchern aller Zeiten ausgewählt.

1984 gründete er das Malik Institute in St. Gallen, das er als Präsident und CEO leitet. Seitdem gehört das Institut zu den führenden Wissensorganisationen für kybernetische Denk- und Managementlösungen. Er ist Sonder- und Honorarprofessor an drei renommierten chinesischen Universitäten. Er war Professor für Allgemeine Unternehmensführung, Governance und Führung an der Universität St. Gallen, Schweiz (1974 - 2004), und Gastprofessor an der Wirtschaftsuniversität Wien (1992 - 1998). Er promovierte und habilitierte sich in system-cybernetic corporate management.

Maliks Studien umfassen die Bereiche Logik und Wissenschaftsphilosophie, Wirtschafts- und Sozialwissenschaften, Systemtheorie und Kybernetik komplexer Systeme.

WAS BEDEUTEN HÄKCHEN IM HINBLICK AUF WOHLBEFINDEN UND GELASSENHEIT?

Die Situation von Karl K. spiegelt den Alltag vieler Menschen: Wieder einmal ist er morgens um 4:00 Uhr aufgewacht. Und das Gedankenkarussell hat sofort angefangen sich zu drehen. Um viele kleine und große Sorgen. Als ihn der Wecker dann zwei Stunden später aus dem Halbschlaf aufschreckt, ist er wie gerädert.

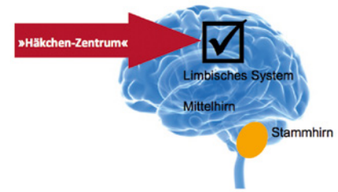
Seine 15-jährige Tochter, der er vor dem Badezimmer begegnet, sagt mit dunklen Ringen unter den Augen: „Ich hab sooooo lange gelernt." Karl K. denkt sich: wahrscheinlich hat sie wieder die ganze Nacht mit »facebook« verbracht. Das ist eine seiner großen Sorgen.

Zwei Stunden später sitzt er in der ersten Besprechung des Tages. Er ist in Gedanken jedoch bei der E-Mail des Projektleiters eines wichtigen Kunden. Sicher, er hätte sich schon längst in die besondere Problematik dieses Change Request bei der Einführung der neuen Software einarbeiten müssen. Andererseits sind die E-Mails dieses Projektleiters immer so formuliert, dass er sich schon ärgert, wenn er nur den Namen des Absenders im Postfach findet. Und irgendwie werden seine Aufgaben immer mehr, und gleichzeitig erledigt er immer weniger. Und die Steuererklärung müsste auch längst abgegeben sein....

Wie soll er das alles eigentlich noch weitere 20 Jahre schaffen? Die Hypotheken für das Haus müssen abbezahlt werden. Seine Frau, die ihm nicht glauben will, dass die Tochter exzessiv chattet. Seine eigenen Schlafstörungen.... Und sein Arzt liegt ihm schon in den Ohren, sein Blutdruck sei zu hoch, die Zuckerwerte ebenfalls und er soll doch den Stress einfach etwas reduzieren … Leicht gesagt, aber wie sollte das funktionieren?

»Heute habe ich wieder nichts geschafft!« Wie oft hören wir das im Selbstgespräch oder von anderen. Dieser Satz verhindert Entspannung und die Aktivierung des Belohnungszentrums im Gehirn. Die Folge kann sein, dass sich das Hamsterrad noch schneller dreht, Schlafstörungen auftreten, und man morgens gegen 4 Uhr die vielen offenen Punkte wälzt. Über die Zeit des wahrgenommenen »Nicht-Schaffens« schwindet das Zutrauen in die eigenen Fähigkeiten. Das Gefühl der Selbstwirksamkeit sinkt. Mit dem stärker werdenden Gefühl, dass man die wichtigen Dinge eh nicht umsetzt, erhöht sich das Gefühl der Hilflosigkeit. Das Depressionsrisiko steigt.

Was passiert in unserem Gehirn? Von jedem bewussten Vorhaben wird in einem Zentrum unseres Gehirns eine »Blaupause«, also eine Kopie abgelegt. Wenn wir etwas fertig haben oder es ist erledigt, wird die Blaupause gelöscht.[1]



Menschen, die mit den Händen etwas Sichtbares schaffen, geben diesem Zentrum automatisch positive Impulse. So kann sich beispielsweise ein Dachdenker nach getaner Arbeit ein Bild seiner Leistung machen. Das Stoffwechselsystem schüttet Hormone aus, die das Belohnungszentrum im Gehirn und mit ihm die Glücksbotenstoffe aktivieren.

Menschen, die nichts Sichtbares schaffen, deren Stapel immer höher werden, deren E-Mail-Posteingangskorb abends genauso voll ist wie morgens, brauchen persönliche Rituale, um ihre offenen Blaupausen im Gehirn abzuhaken. Daher kommt der Ausdruck »Häkchenzentrum«.

Was hilft zu mehr Gelassenheit und dem positiven Gefühl, »etwas geschafft zu haben«?

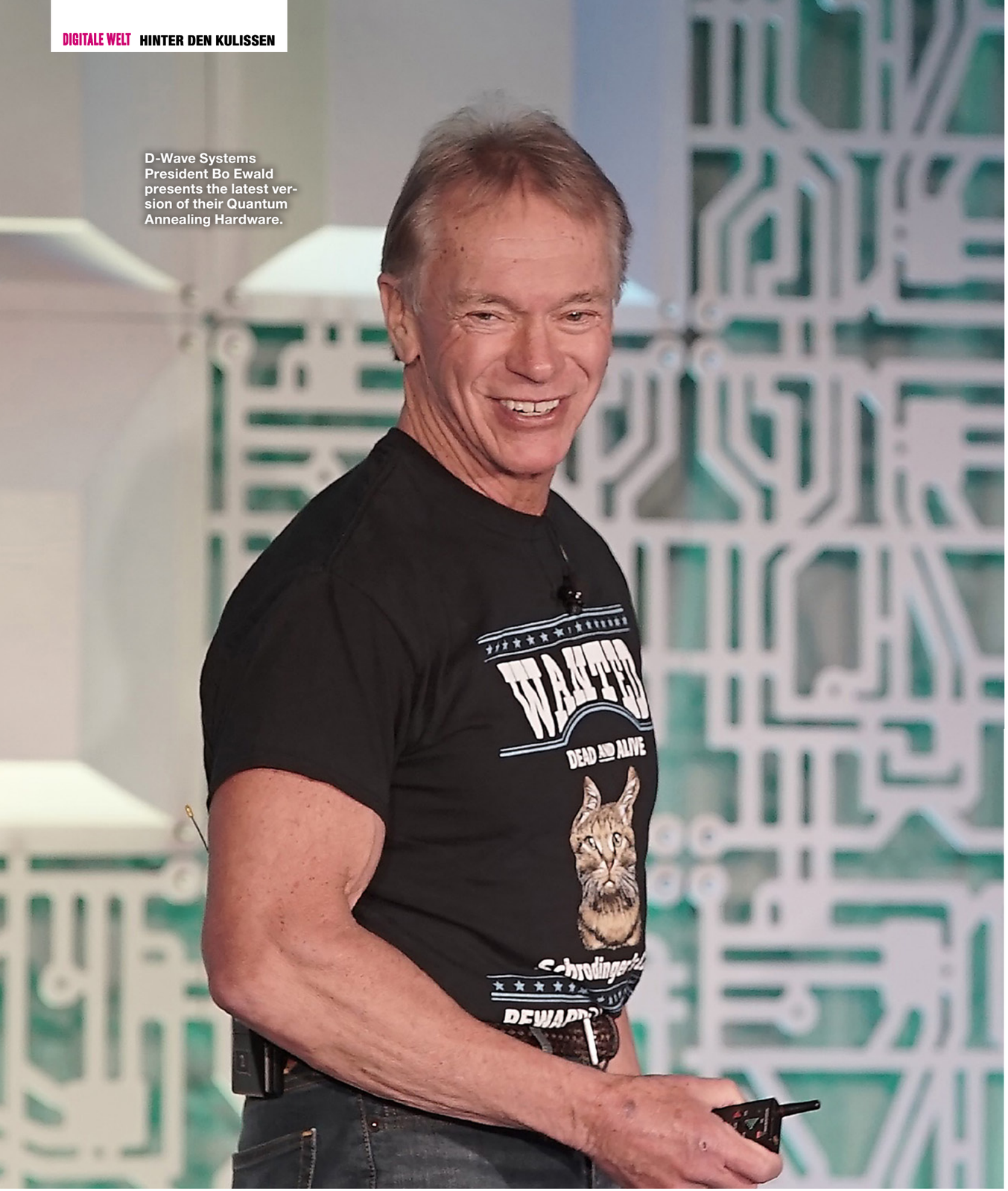
- Ein passendes persönliches Ritual: z. B. handschriftliches Notieren von Aufgaben und dem »Erledigt-Häkchen«.
- Bewusste Reflexion der »Häkchen« vor oder beim abendlichen Heimweg.
- Selbst wenn man nichts von dem erledigt hat, was man sich vorgenommen hatte, ist es wichtig, die anderen Dinge zu würdigen, die man gemacht hat, ohne sie geplant zu haben.
- Im Team ein passendes Ritual, z.B. zum Start in den Tag oder zum Abschluss der Woche: »Was haben wir erledigt? Wo stehen wir jetzt?...«

Wichtig ist, das Ritual sollte so in den Ablauf eingefügt werden, dass es auch machbar ist. Sonst könnte es dazu führen »Ritual nicht geschafft«, was wiederum zu einer weiteren Verstärkung des Hamsterrades führen würde.

Dr. Petra Bernatzeder,
Diplom-Psychologin, Geschäftsführung upgrade human resources GmbH

Referenzen: [1] E. Pöppel: Reafferenzprinzip oder „Zeigarnik-Effekt" G. Hüther: Bedienungsanleitung für ein menschliches Gehirn, 2010

Foto: Privat



D-Wave Systems President Bo Ewald presents the latest version of their Quantum Annealing Hardware.

In five years the future will arrive

D-Wave is the first company ever to sell quantum computers. The publisher of DIGITALE WELT Magazin flew to Vancouver and spoke in person to Bo Ewald, the president of this pioneering tech company. He shared some exciting insights about the quantum computing world and made some startling predictions for the future.

What did you do before you started working at D-Wave?

By education I am a structural engineer. When I was in graduate school in the seventies I did early work in computer graphics. There we made, what was probably the first ever made, computer generated movie superimposed on a real landscape. This was an engineering application for the U.S. department of transportation. At the time they were building the interstate highway system and one leg of the road led through a canyon. They wanted to generate an image to see what the new road would look like and then superimpose that on real film. This is how I got involved with computers. We've used the "Control Data Corporation" data 6600 computer. This computer company is long gone but at the time they made the fastest computers on the market. One of the three founders of "Control Data" was a man named Seymour Cray.

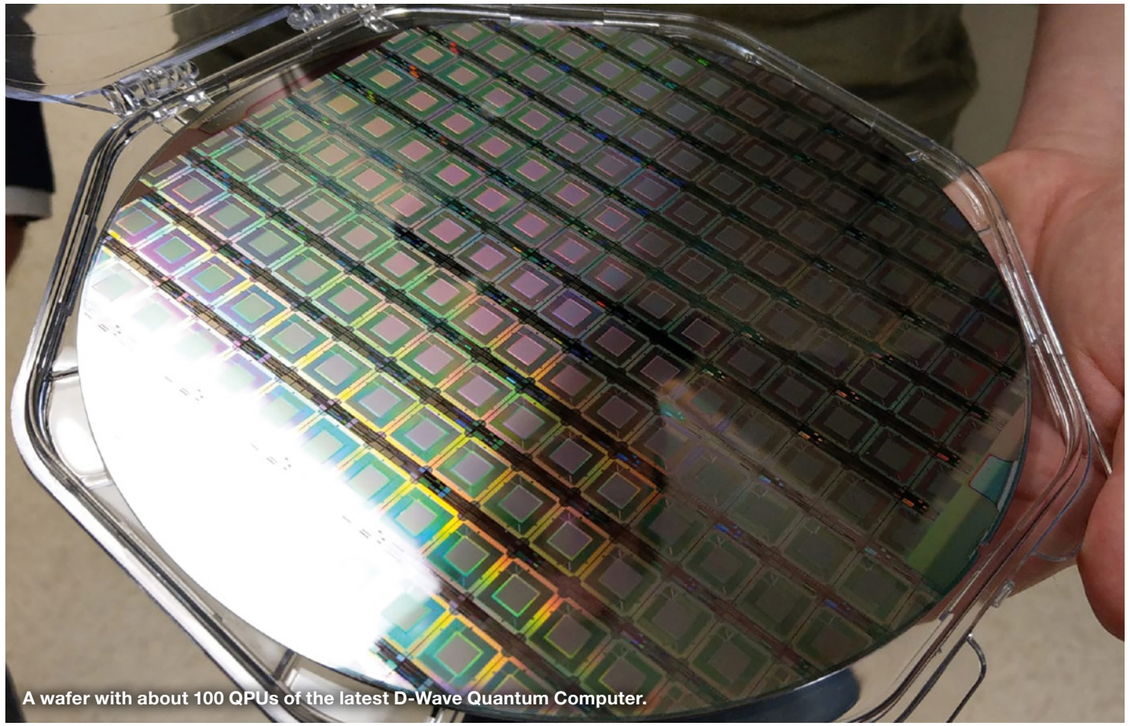
After I joined the army, which we all did in those days, I went to Los Alamos National Laboratory in New Mexico to do computer graphics work. That was in the mid seventies, about the time when the first Cray supercomputer had been built. So my first job there was putting up a high performance graphic system connected to the Cray. However Cray had no operating system. Basically it was a piece of hardware. So Los Alamos wrote its own operating system. After a while they asked, if I would run that project. This is how I came to learn more about software, operating systems and supercomputers.

After a little while I ended up running the computer division in Los Alamos. I was about thirty years old at the time. Back then, Los Alamos was the most powerful computing center in the world and we pioneered many things. It was a terrific place to work. So I learned about general management of technology and business, because we had about 10,000 customers. It was in 1982 when I first read about quantum computing in a paper that came out on the topic by Richard Feynman. One year later, in 1983, Feynman gave a talk in Los Alamos about using the basis of quantum physics to try to build a different kind of computer. At that occasion I even had the chance to talk to him in person. However after that I forgot about quantum computers for a while.

"What quantum computing really needs is more smart people who think about how to apply it."

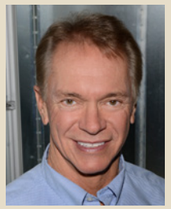
When did you decide to start a quantum computing company?

In fact I didn't start the company. After I left Los Alamos I went to Cray where I became the president. Then I was the CEO of Silicon Graphics and had some start up



A wafer with about 100 QPUs of the latest D-Wave Quantum Computer.

Robert Ewald



Robert "Bo" Ewald leads D-Wave's international business as President and is responsible for global customer operations for the company. Mr. Ewald has a long history with other leading technology organizations, government projects, and industry efforts. He has experience in large and startup businesses having been the CEO of visualization and HPC leader Silicon Graphics Inc., President of supercomputing leader Cray Research, President and CEO of Linux pioneer Linux Networx and Executive Chairman of Perceptive Pixel, Inc. He started his career at the Los Alamos National Laboratory where he led the Computing and Communications Division. He has served on the boards of directors of both public and private companies and has participated in numerous government and industry panels and committees. He was appointed to the President's Information Technology Advisory Council by both the Clinton and Bush administrations.

companies. About ten years ago one of the head hunters in Silicon Valley called me up and told me about that crazy company up in Vancouver that works in quantum computing. Since I knew more about high performance and advanced computing than most people in the field they asked me to talk to them. D-Wave had only recently been founded and I thought it was an interesting idea. However, I was very busy at the time, later of course I joined.

Please explain the research approaches of the early days of quantum computing.

In order to create a computer you marry two things: One is the architecture of the computer, so a set of instructions that a computer executes to do things. The other is the technology you are going to use to implement. From 1982 to about 1998 the industry was working on quantum gate model computers. The concept of it was based on digital computers, because digital computers are gate model computers. So they tried to create quantum gates and linking them together to do some function. So the architecture was a gate model quantum computer. The implementation question was: How can we build the qubits? There are around five different concepts on building qubits now. One is to use superconducting technology, which is what we and most others do. But other people also try to trap ions for example and then there are three or four other ways.

You don't produce general purpose quantum computers, you make quantum annealing machines, which are especially useful for optimization problems. Hereby the computer has to choose the best option of numerous possibilities. With a higher number of qubits quantum computers get more powerful. How many qubits do D-Wave computers operate with?

The company has been able to double the number of qubits every two years or so. It started with 128 qubits around six years ago but then the next jump was 500 qubits which is roughly four times as many. The next jump was 1,000 qubits and then 2,000 and the next one will be between 4,000 and 5,000 qubits. However, it will take a little longer than two years for that jump.

Who are your customers and where are they from?

In general the biggest market is in the U.S., not in Canada. However, generally you have to differentiate between cloud customers like Volkswagen and system customers, who buy an entire computer.

Not all of our customers want to be announced, but what we can say is the following: Lockheed Martin has installed three different D-Wave computers. The Quantum Artificial Intelligence Lab – a collaboration between Google, NASA and the USRA – has a D-Wave computer as well. Furthermore our computers were purchased by Los Alamos National Laboratory and Oak Ridge National Laboratory is our largest cloud customer. Our hope is that by the end of this year we have contracts for two or three more. Maybe two in the U.S., one in Europe – hopefully in Germany – and one in Japan.

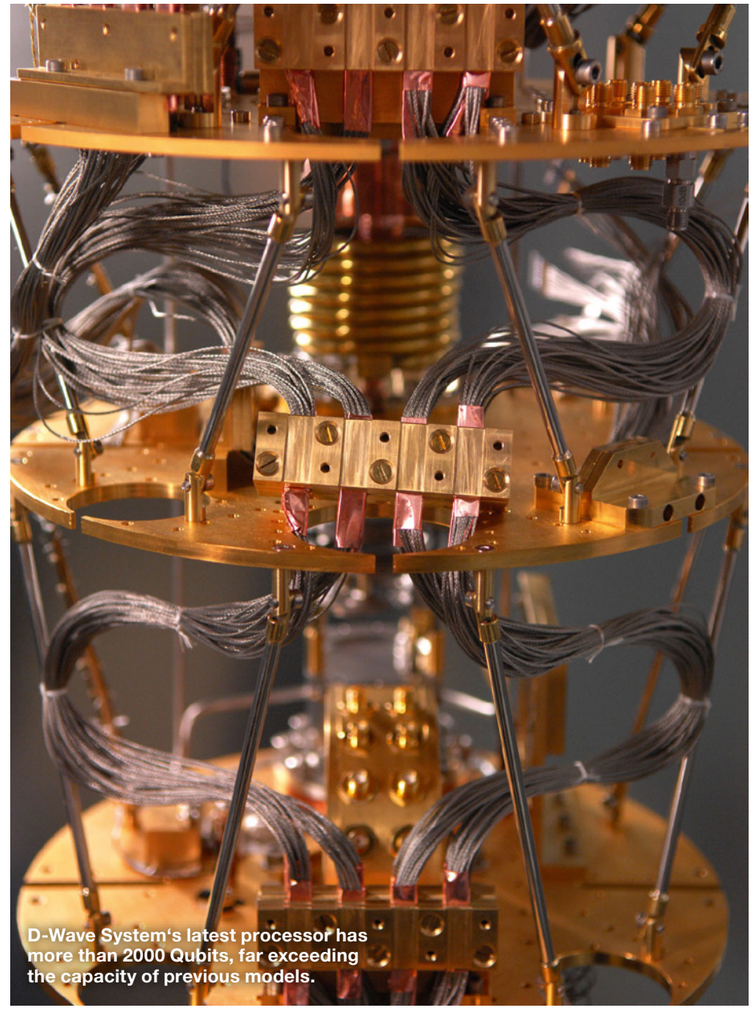
Today we have a little over 25 cloud customers. Like Volkswagen or DLR. In rough numbers: About half of those are in Japan. Usually the customers are big Japanese companies, Toyota being one of them. That is interesting because Japan is usually very conservative when it comes to applying new technologies. Europe has maybe one quarter of them and the rest are in the U.S.

How much does a quantum computer cost?

A machine costs around ten million U.S. dollars if someone just buys it out right.

How big is a quantum computer?

The computer itself is only a chip as big as your thumbnail. But the quantum mechanical state is fragile. So to get the chip into a quantum mechanical state, it has to be protected from radio frequency interference and from vibration. The superconducting circuits that we use operate very near absolute zero. There can´t be any moisture at that temperature and there has to be an extreme vacuum. So you end up putting one little chip in the heart of a big box. The box is about three meters by three meters by three meters. That box is a Faraday cage which keeps radio frequency interference from getting inside. Inside there is an apparatus that reminds of a Terminator´s arm, but it is a dilution refrigerator. And it gets colder and colder and colder the further down you go until you get to the actual chip. There, the temperature we run at is about ten to twelve millikelvin. Outer space is three to four kelvin. So our computers are hundreds of times colder than outer space. Another challenge is to keep the machine running for longer periods of time. So the longest we had a machine running was for 22 months.



D-Wave System's latest processor has more than 2000 Qubits, far exceeding the capacity of previous models.

In order to protect the computers from vibration our customers usually put them on the ground floor of a building and they'll cut a square, so that the concrete pad that our computer sits on is not connected to the rest of the concrete. That way it is vibration-isolated.

"The quantum model gave Donald Trump a thirty to forty percent chance of winning."

The computer uses only 25 Kilowatt maximum. So that's not so much power. And it needs some chilled water.

Do you upgrade the computers for your customers?

Yes, we upgrade the chips. But that can take between two and three months, because it takes time to warm the computer and the maintenance itself takes time as well. Then it takes the remaining time for the computer to cool down again.

How can quantum computers be used?

I think how we use quantum computers is how it must have been in 1955 at IBM. It was the time before Fortran was invented, so whenever you did something on a digital computer it was probably the first time it was ever done. So people were trying out different things and eventually that developed into applications.

The reality is that we are in a very early state of quantum computing still. There are no proven production applications for it yet. Most of the things people are looking at currently are experimental and research related. Our customers have worked with the computers in different ways and it is unbelievable which tasks for quantum computers have been figured out by smart

D-Wave System's huge patent collection. Exhibited at the headquarters in Vancouver, Canada.

people. What quantum computing really needs is more smart people who think about how to apply it. However it is unbelievable what people have done in the past two years.

Like Volkswagen's Beijing taxi project?

Exactly! In fact, this is one of the best examples of how quantum computers can be used. That was the first problem that was solved on a quantum computer that you could explain to your parents. So Volkswagen wanted to try quantum computing on a real problem and they chose traffic optimization in order to avoid big traffic jams. Since they had all the GPS data of all the 10,000 taxis in Beijing, they chose this problem for the quantum computer to solve. It wouldn't have been feasible to cover the entirety of 10,000 taxis in this mega city. This is why we decided to choose the route between Downtown Beijing and the airport, where there are 400 or 500 taxis. This was still too big for the hardware. So very much like we did in high performance computing we created software decomposition techniques. For that purpose we partitioned the route into smaller pieces, in order to solve it in chunks. In a hybrid computing manner we could solve it and it worked like this: The traditional computer broke the problem into pieces, sent those to the D-Wave to solve each piece, and then the classical computer glued the pieces back together to make the whole. It was also the classical computer which noticed when solutions didn't work out. If this was the case, the digital computer sent the problem back to the D-Wave.

"Our computers are hundreds of times colder than outer space."

Working with the team from Volkswagen it took us around three months to figure out how to map this two-dimensional and time-dependent GPS coordinates on a quantum computer. But once having done that, now, within a couple of seconds they'll get 5,000 good solutions. So I think this is a good example of how engineering will be in the future: The combination of classical and quantum computing.

When will this future begin?

I think in five to ten years the future will have arrived.

Did you verify the results of the Volkswagen project by using only a classical computer?

Volkswagen ran the same problem on one of their servers in Wolfsburg and it took many minutes. But when you are driving every few seconds you need to determine where to go, because every few seconds the conditions change. Multiply that by 10,000 taxis! You can´t wait minutes or hours to give them the best routing, because ten seconds later all the conditions are different. It is safe to say that with our quantum computers we probably get the best answer in a second or two, but we don't guarantee that we do.

What other problems were solved using the D-Wave computers?

Today we have 75 or 80 of what I call "proto-apps". I created this funny word "proto-apps", because I wouldn't call them full applications yet, but they are prototypes for future applications. And they are almost all done by customers. About half of them are optimization. About twenty percent are machine learning, about ten percent is material science. Volkswagen, for instance, started to work on battery chemistry in a small way. Originally people thought that this wasn't possible on a quantum annealing machine, but it is. In the customers' and so to speak the users' own words, about half of the times the performance is approaching, or even exceeding, that of conventional computers, however always on smaller problems.

Could you tell us some more about the different prototype applications your customers have created so far?

Don't forget, I call them prototypes, because I don't want to overstate what these applications are. However, Los Alamos is probably the flagship customer for trying different kinds of applications. In the first phase they ran 22 different projects. They made all of the results available and NASA, USRA and USC have done the same.

The U.S. tried to optimize a constellation of satellites, which have priority target stage. They showed that they could do that.

DLR on the other hand was working on air traffic routes over the North Atlantic. Apart from that, they also are working on a gate-scheduling application.

Denso wanted to outdo Volkswagen so they wanted to optimize the flow of all commercial vehicles in Bangkok. However, there are 100,000 commercial vehicles in Bangkok. Hence this project was way too big and they had to partition it further.

Then British Telecom has about five projects in the cell phone world.

There is another project in the U.K. of a company called Ocado, which has the world's largest online grocery store. Their business objective is to put all the items you want in a box fifteen minutes after you have placed your order online. So each of their warehouses has like 10,000 bins for different things and they have 1,000 robots. Optimizing the flow of those is their goal; so that the robots don't run into each other, so that they get the right things picked and also to make sure that they save time when they recharge. When you think about it: That's a huge combinatorial optimization problem. But they started to have some success in this.

A university in Japan is starting to use the D-Wave computer for evacuation optimization in the case of a tsunami.

The computers are also used on Cyber Security: For instance to explore the formation of global terrorism networks in Syria.

Another interesting project was from a man from a company in Washington D.C. As you remember in the last U.S. presidential elections all the polls said Hillary Clinton would defeat Donald Trump easily. That didn't happen. So that man wondered if he could create a model on the D-Wave to be able to look at the same data that they used, create a quantum model and see what it predicts. It took a lot of work, but he was able to do that. The quantum model gave Donald Trump a thirty to forty percent chance of winning. The D-Wave model noticed that there were hidden relationships in the data of political correlations between individual states and that the reactions in the different states corresponded to each other. Traditional techniques didn't see that. I would have never thought that our machines would be used for something like this. Overall they are most often used for more scientific problems.

"The thinking is different than in digital computing."

And many more. It is funny, because on the fictional side there are also a number of books written and TV-Shows being broadcasted now about quantum computing. The most prominent example is probably Dan Brown's new novel "Origin".

How do you predict the future of quantum computers in the next 25 years?

I think at least for the next ten years, if not longer than that, you won't have quantum computing without traditional computing side by side. It is really helpful to compare that with the development of GPUs: So twenty years ago GPUs were just good for one thing: graphic processing. But then they also started being added to high performance computers where you were doing lots of graphics. So you had a traditional computer and plugged into a GPU. Most of the applications ran on the traditional computer and then when you had a graphic´s application, the GPU ran it and then returned the result to the classical computer. Then over time the GPUs became more powerful and you could start doing some numeric calculations on them. And they started to do more and more calculations and eventually you could start making machine learning on them. However, that took twenty years. So at the moment you could compare that with quantum computing. If the computer detects that there are special problems which could be solved by the quantum computer, it will make it solve it. So we would be looking at quantum enhanced computing.

Do you think in twenty years my cell phone will have a quantum computer inside?

I don't think so. Not unless there is some breakthrough in the technology that enables us to create a protected quantum environment in a phone, which includes all the aspects about vibration, cold temperature and so on which I mentioned before. However there will be breakthroughs in the superconducting circuits. The reason why we have to run them so cold is because certain materials become superconducting only at certain temperatures.

Do you think in twenty years every cell phone will be connected to a quantum computer?

Yes. I believe that is going to happen and I don't think most people will even notice or know that this is happening.

Will you face a lack of skilled personnel in quantum computing in the future?

Yes we will. There are no applied quantum curricula so far in the universities, at least as far as I know. I think the application of quantum computing will move so fast that the universities will have difficulties producing course work and to get people trained quickly enough. The thinking is different than in digital computing.

Prof. Dr. Claudia Linnhoff-Popien and Dr. Sebastian Feld at the factory tour with D-Wave President Bo Ewald.

Interview geführt von:
Prof. Dr. Linnhoff-Popien und Dr. Sebastian Feld
Autorin: Florentina Hofbauer

Fotos: Privat, D-Wave Systems Media Resources

Machine learning in the quantum era

Niels Neumann, Frank Phillipson, Richard Versluis

Introduction

Everyday computers can be used to solve numerous tasks which are often too difficult for humans to do quickly. Whether it is finding the shortest route between your home and your work or automatically finding the solutions to puzzles such as sudoku's, computers can solve these problems faster and often better than humans can. On the other hand, there are problems that are easy for humans, but much harder for computers to do automatically, such as face identification or pattern recognition in images.

The state-of-the-art technique for solving these problems is machine learning. Different types of machine learning exist, most of them boiling down to supplying data to a computer, which then learns to produce a required outcome. The more data is given, the closer the outcome will be to the actual solution or the higher the probability will be that the correct solution is found.

Even though machine learning has solved numerous problems and improved approximate solutions of many others, it also has its limitations. Training machine learning models requires many data samples and models may require a long time to be trained or produce correct answers. Quantum computers may be able to improve the performance of machine learning algorithms by exploiting the power of quantum mechanics.

In this article we give a brief overview of machine learning techniques and explain how and where quantum machine learning is expected to deliver benefits. Next, we introduce quantum computing in general and the Quantum Inspire platform, an online quantum computing platform developed by QuTech in The Netherlands, in particular. After that, we show the results of implementing one of the quantum machine learning algorithms we propose in the second section. We tested a machine learning algorithm to classify and subsequently generate two by two-pixel images. The machine learning algorithm learned the probability distribution of the input and tried to replicate this in the generated images. This task is inherently difficult when the distribution of the input is unknown. We show how this algorithm was implemented on the Quantum Inspire platform and make a comparison with classical results.

Quantum Machine Learning

Machine learning is a potential interesting application for quantum computing. Current classical approaches ask huge computational resources and in many cases training costs a lot of time. In machine learning, the machine learns from experience, using data examples, without a user or programmer giving it explicit instructions; the machine builds its own logic. Looking at classical machine learning, one can distinguish various types:

- Supervised learning – here labeled data is used, e.g., for classification problems. This means that the data that is used for learning contains information about the class it belongs to.
- Unsupervised learning – here you use unlabeled data, e.g., for clustering problems. Here data points have to be assigned to a certain cluster of similar points, without prior information.
- Semi-supervised learning – here partially labeled data is available and models are investigated to improve classification using labeled data with additional unlabeled data. Many of these models use generative, probabilistic methods.
- Reinforcement learning – here no labeled data is available, but a method is used to quantify the machine's performance in the form of rewards. The machine tries many different options and learns which actions are best based on the feedback (rewards) it receives.

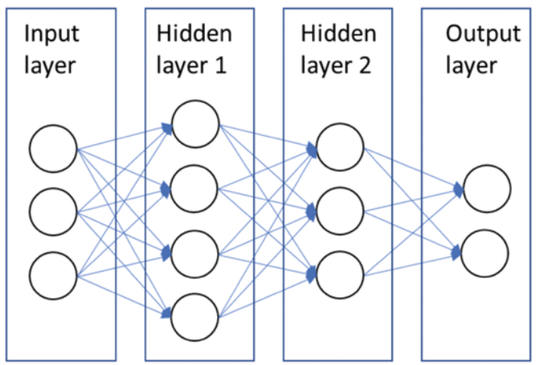


Figure 1: An artificial neural network with an input and an output layer and two hidden layers.

A common model used in machine learning is the artificial neural network. This is a model based on nodes connected by weighted edges, see for an example Figure 1. Commonly, the nodes are clustered in layers, and information is transported from the input layer to the output layer, traversing intermediate layers. These intermediate layers are the so-called hidden layers. The number of nodes per hidden layer can be chosen freely. For the input and output layer this will be determined by the preferred output and the number of inputs. At each node, the information is modified, based on a certain activation formula, for example a linear function or the sigmoid function, and the weights of the connecting edges. In the learning stage the weights or parameters are tuned such that the difference between the output data generated by the system and the desired output data is minimized.

The purpose of such a network can be classification and clustering of objects. It can also serve as a decision maker or as an associative or content-addressable memory, where a system recognizes specific patterns. This has applications in error correction where unwanted errors are automatically corrected, and anomaly detection, where suspicious behavior of parties in a network can be detected.

If we think how quantum computing and machine learning meet, we could think of both the input and the processing part being classical or quantum (Schuld & Petruccione, 2018). If both are classical, we have classical machine learning. Classical machine learning can be used to support quantum computing, for example in quantum error correction. Quantum processes can also be used as an inspiration for classical algorithms, such as tensor networks, simulated annealing and in optimization. If the input is a quantum-mechanical state and the computing is classical, the machine learning routine is used to translate quantum information into classical information. If both the input and computing are quantum, this will be real quantum machine learning, however, only a few results in this direction are published yet. In this article however, we look at classical input information and quantum processing.

One of the main benefits of quantum computers is the potential improvement in computational speed. Depending on the type of problem and algorithm, quantum algorithms can have a polynomial or exponential speed-up compared to classical algorithms. There are also other benefits relevant in the near future. Quantum computers could possibly learn from less data, deal with more complex structures or could be better in coping with noisy data. In short, the three main benefits of quantum machine learning are (interpretation based on (Dunjko & Briegel, 2018)):

- Improvements in run-time: obtaining faster results;
- Learning capacity improvements: increase of the capacity of associative or content-addressable memories;
- Learning efficiency improvements: less training information or simpler models needed to produce the same results or more complex relations can be learned from the same data.

For each of these benefits we show some examples further on in this article.

The improvement in run-time can be realized in various ways. Machine learning consists of optimization tasks that can be done faster by quantum annealers, like the D-Wave machine. Another way of getting a speed-up is the use of quantum sampling in generative models. Sampling is one of the tasks on which a quantum computer is expected to outperform classical computers already in the near future. Hybrid quantum-classical algorithms are expected to be among the first to outperform classical algorithms. Hybrid algorithms perform a part of the algorithm classically and a part on a quantum machine, using the specific benefits such as for example efficient sampling. The last way to realize the speed-up is via specific quantum machine learning algorithms using amplitude amplification and amplitude encoding. Amplitude amplification is a technique in quantum computing and is known to give a quadratic speed-up in comparison with classical approaches. In amplitude encoding, amplitudes of qubits are used to store data vectors exponentially efficiently, enabling exponential speed-up. However, this exponential speed-up is not obvious and the assumptions made to come to this theoretical speed-up have some technological challenges, (see e.g. (Aaronson, 2015)). Those quantum algorithms

- assume preloaded databases in quantum states, for example using quantum RAM (QRAM);
- assume data to be 'relatively uniform', meaning no big differences in value; and
- produce a quantum state as output, meaning this has to be transferred efficiently to a meaningful result.

As stated by (Aaronson, 2015): 'To maintain the potential exponential speedups of the quantum algorithms, this conversion needs to be efficient. If this is not the case, then one ends up in a situation in which the quantum algorithm can solve the problem very efficiently, but only after a lengthy preprocessing of the data has been performed, therefore killing the whole point of using the quantum algorithm.' Otherwise one might be able to find a classical algorithm having similar performance. These issues, and the fact that the number of qubits is still small, make that this class of specific quantum machine learning algorithms is still far away.

However, next to the mentioned improvements in run time, also capacity and efficiency improvements are benefits of quantum computing. In order to quantify the potential of both in improving machine learning, we implemented some examples from literature on the Quantum Inspire platform of QuTech, a joint venture of the Delft University of Technology and TNO, The Netherlands Organisation for applied scientific research. Each of those examples falls within a different combination of machine learning and expected benefit:

- Classification with Hybrid Helmholtz Machine (Benedetti, Realpe-Gómez, & Perdomo-Ortiz, 2018) – a generative semi-supervised learning model, expected to result in an improvement in run time using quantum sampling;
- Classification with Quantum Neural Networks (Fahri & Neven, 2018) – a supervised learning case, expected to result in an efficiency gain;
- Anomaly detection with Quantum Hopfield Networks (Rebentrost, Bromley, Weedbrook, & Lloyd, 2018) – a supervised learning case, expected to result in a capacity gain.

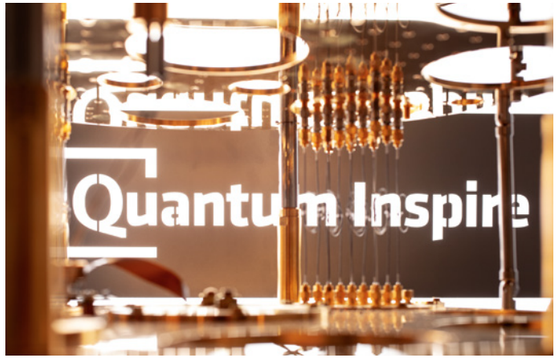
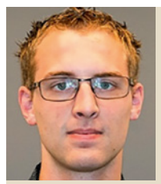


Figure 2 Quantum Inspire logo and dilution refrigerator (Copyright Marieke de Lorijn).

Figure 3 Thermal stages and wiring of a quantum computer prototype inside a dilution refrigerator at QuTech (Copyright Marieke de Lorijn).



Niels Neumann MSc

Niels Neumann MSc is a scientist at TNO. He works on (near term) applications of quantum computers and quantum networks. He studied mathematics and physics.

Dr. Frank Phillipson

Dr. Frank Phillipson is senior scientist at TNO. He leads the project team within TNO that studies applications and algorithms for near future use on quantum computers and quantum simulators. He studied econometrics and mathematics and has a PhD in applied mathematics.

Ir. Richard Versluis

Ir. Richard Versluis is principal systems engineer and lead scientist quantum technology at TNO. He is the system architect of Quantum Inspire, an online open access quantum computing platform.

In this article we will elaborate on the first example, a gate-based hybrid Helmholtz machine, whereas the original paper showed an implementation on the D-Wave annealer. This is the first time that a gate-based hybrid Helmholtz machine has been implemented.

The Quantum Inspire platform

Though building a quantum computer is one of the hardest quantum applications to reach, a lot of resources are put into its development throughout the world. Exploiting quantum mechanical effects such as quantum tunneling, superposition and entanglement, a quantum computer can be regarded as a massive parallel computation system capable of solving specific types of problems more efficiently than the classical computers. In general, two types of quantum computers are being developed: quantum annealing computers and gate-based quantum computers. The quantum annealing computers are sometimes referred to as analog quantum computers, where gate-based quantum computers are also called digital quantum computers.

Quantum annealing computers exploit the effect of quantum tunneling. Very simplified, this means that quantum mechanics allows very small particles such as electrons to go to the other side of a potential barrier by tunneling through that barrier, which is not possible classically. If you imagine a landscape full of hills and valleys and you are trying to find the lowest valley in this landscape, you can imagine that you can find this lowest valley faster, if you could tunnel through the hills instead of climbing all the hills. The best known example of a quantum annealing machine is the D-Wave quantum computer. By controlling the potential landscape, annealing machines are capable of finding (approximate) solutions of various minimization problems.

Gate-based quantum computers can solve more general problems than annealing machines, but are more difficult to build and control. Gate-based quantum computers work by executing a quantum algorithm, which is a sequence of single-qubit and multi-qubit gates. A quantum gate is an operation on one or more qubits. Gate-based quantum computers exploit the quantum-mechanical properties of superposition and entanglement to create quantum algorithms potentially outperforming classical computers for various problems, such as big data analysis, machine learning, code breaking and even to assist in the quest for improved medicines or new materials with special properties. Qubits are the fundament of a gate-based quantum computer. Unlike classical bits, qubits can be in a superposition of 0 and 1. Qubits can also be entangled, meaning that the state of these qubits can no longer be described as separate qubits. The easiest way to think of this, is by an extension of the superposition principle: one qubit can be in the state 0 and 1 at the same time, two qubits can be in the states 00, 01, 10 and 11 at the same time, three qubits can be in the states 000, 001, 010, 011, 100, 101, 110 and 111 at the same time, etc. This means that an N qubit system can be in 2 to the power N possible states at the same time. When you do calculations with these entangled qubits, it is like you are operating on a massive parallel computer, performing operations on many bits at the same time. The finer details of quantum computing are much more complex than explained here. For the interested reader there is many literature online about the concept of quantum computing.

Quantum Inspire (QuTech, 2018) is an online quantum computing platform designed and built by QuTech (https://www.quantum-inspire.com/) and is a gate-based quantum computing system. The goal of Quantum Inspire is to provide users access to various technologies to perform quantum computations and to provide insights in the principles of quantum computing. Quantum Inspire is a full stack system consisting of:

- a web portal with a GUI to program quantum algorithms in cQASM;
- a software development kit (SDK) that provides a Python interface to Quantum Inspire, a backend for the ProjectQ framework and a backend for the Qiskit framework;
- control software for scheduling and queueing jobs and for connecting the control hardware;
- software for data processing and automated tuning and calibration of quantum chips;
- different instances of the QX simulator for simulating up to 26 fully entangled qubits on a commodity server, or up to 37 fully entangled qubits on Cartesius, the Dutch national supercomputer.

Quantum Inspire is designed to be connected to both quantum simulators and quantum hardware.

At QuTech different qubit hardware technologies are being developed, such as superconducting charge qubits (transmons), semiconducting electron spin qubits and NV center qubits that are based on the spin properties of nitrogen-vacancy centers. Another line of development are qubits based on Majorana fermions. One or more of these quantum chips will be integrated in Quantum Inspire in the future, but they are not available for online access yet.

All work published in this paper has been executed on the QX simulator of Quantum Inspire. QX is a quantum computing simulator using vector state representation of qubit states and can be used to execute gate-based quantum algorithms. A primitive noise model for simulating depolarizing noise can be included in the simulation. The native gate set of cQASM contains single-qubit rotations of arbitrary angle around the 3 axes of rotation, standard two- and three-qubit operations (CNOT, CZ, Swap, Toffoli), but also binary controlled qubit operations.

What is a hybrid Helmholtz machine

Finding structure in data is hard. Humans are able to find structure, such as recognizing a handwritten digit, only because we have done it a thousand times. Even if the task seems naturally, everybody has had (and maybe even still has) a period in which he or she learned what all these writings mean. Computers can do similar things, but also have to learn first.

Often when information has to be obtained from data, specific machine learning tasks are used. Also for pattern recognition, machine learning algorithms are used to recognize and classify patterns. However, it is not true that every machine learning algorithm can be used to solve arbitrary tasks. In fact, specific tasks often require dedicated machine learning algorithms to find the answer.

A special class of machine learning algorithms are neural networks, where information is fed to a network or different nodes connected by weighted edges. A special neural network, which inspired the research on this topic, is the human brain. Also here, information that is obtained, for instance a sound we hear, activates some neurons. These neurons might activate other neurons, enabling us to recognize a sound as speech, music or noise.

Often, data fed to a neural network (either the human brain or artificial neural networks) are corrupted. Think for instance about an image of a pig with a crate partially in front of it. We do not see the full pig, however, we can still recognize it as being one. This task is harder for artificial neural networks. A special type of neural network suited for this specific task is a Helmholtz machine. Apart from trying to recognize patterns, a Helmholtz machine also tries to find probable explanations for certain patterns by means of pattern generation.

A Helmholtz machine consists of two neural networks. The first is a bottom-up recognition network, the second neural network is a top-down generative network. Data can only be given to the very first layer of the recognition network, and output is extracted from the last layer of the generative network. These layers, with which interaction is possible, are called visible. All layers with which no interaction is possible, are said to be hidden. Note that the first layer of the generative network is also hidden, as it gets input from the last layer of the recognition network (called sampling), meaning that users cannot interact with it. See also Figure 4 for an example of a Helmholtz machine with a visible layer of four nodes and a hidden layer with two nodes. Note that neural networks in general can have more than four nodes per layer, as well as more than one hidden layer. Data can be fed into the Helmholtz machine in the recognition network, and from the generative network data can be extracted.

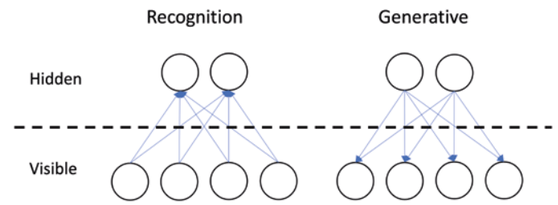


Figure 4 A Helmholtz machine with a visible layer of four nodes and one hidden layer with two nodes.

Each link has a weight assigned to it and based on the input and on the weight of links, other nodes can be activated. The hardest part that has to be executed in most neural networks, including the Helmholtz machine, is assigning the correct weight to each link.

This assignment of weights, which is also called learning, is performed iteratively. In general, data samples are presented to the neural network, after which the weights are updated

to better fit all the data presented so far. For the Helmholtz machine, learning is slightly different as we have two neural networks working together instead of a single one. A special algorithm is used to train a Helmholtz machine and thus learn the weights of the links: the wake-sleep algorithm.

In the wake-sleep algorithm, the weights of both neural networks are learned alternately. A single iteration of learning consists of two phases. Firstly, the weights in the recognition network are fixed and the weights of the generative network are learned. The Helmholtz machine is in the wake-phase, as samples from the data set are used as input, this is also called sensing. Secondly, the weights in the generative network are fixed, and the weights of the recognition network are learned. The Helmholtz machine is in the sleep-phase and gets its input by sampling from the probability distribution of the recognition network. This process is called dreaming.

Once the wake-sleep algorithm is finished, the Helmholtz machine is trained. It has learned an efficient representation of the data, often in the form of an approximate probability distribution, describing how often each pattern or event occurs.

Quantum computing can be used in multiple ways to enhance the Helmholtz machine. One way is by replacing the sampling in the first hidden layer of the generative network, by quantum sampling, as done by (Benedetti, Realpe-Gómez, & Perdomo-Ortiz, 2018). This approach gives a speed-up in running time, however uses a different computer paradigm, quantum annealing as explained in the previous section, than we use in this article. We consider a quantum-classical hybrid Helmholtz machine, where the neural networks are replaced by quantum gate-based neural network implementations, with classical pre- and postprocessing.

For this implementation, parameters used in the quantum circuit are learned instead of the weights of the links. Again, learning is done using the wake-sleep-algorithm. Theoretically, this approach requires less data samples and less training to achieve similar performance results.

Implementation of a hybrid Helmholtz machine on Quantum Inspire

A gate-based hybrid Helmholtz machine has been implemented on the Quantum Inspire platform, based on the work done in (Lopez-Chagoya, 2018). Every node in the classical network corresponds to a single qubit and the learned parameters, instead of weights, are used as input for operations on the qubits.

A gate-based quantum implementation of the recognition and generative network of Figure 4 is shown below in Figure 5 and Figure 6. Each line in these figures corresponds with a single qubit and each block corresponds with operations on that qubit. The parameters $\alpha\_i,\beta\_i,\gamma\_i,\delta\_i,\phi\_i,\omega\_i$ are learned during the learning phase of the algorithm. This means that these parameters are similar to the weights in the classical Helmholtz machine.

The measurement results of the recognition circuit are used as input in the generative circuit. The operations connecting two qubits in the figures below correspond to the edges connecting two nodes in the classical neural network.

With perfect training, and thus optimal parameters, the measurement results of the generative circuit match the probability distribution of the input data set.

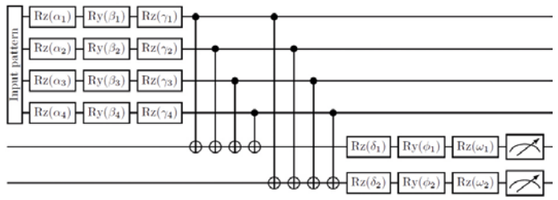


Figure 5 Quantum implementation of the recognition network of the hybrid Helmholtz machine.

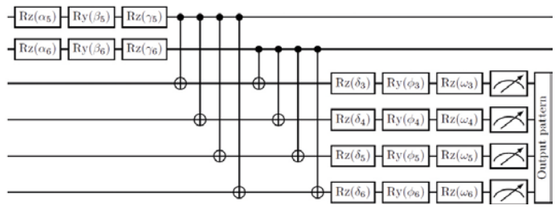


Figure 6 Quantum implementation of the generative network of the hybrid Helmholtz machine.

Both the recognition circuit and the generative circuit of the hybrid Helmholtz machine are implemented on the Quantum Inspire platform, based on the work done in (Lopez-Chagoya, 2018). As input for the recognition circuit, the BAS_22-dataset is used (MacKay, 2003). The BAS_22-dataset, short for Bars and Stripes-dataset, consists of 2-by-2 pixel images. In total there are sixteen possible 2-by-2 pixel images as shown in Figure 7, with the BAS_22-dataset shown on the left only containing six of those.

The input of the hybrid Helmholtz machine are random samples from the BAS_22-dataset. Each sample is transformed from a 2-by-2 pixel image to a binary string of length four, where a one represents a blue square and a zero a white square. The probability distribution for this dataset, describing how often each sample is chosen, is a discrete uniform distribution, meaning that each of the six images is equally likely to be chosen at random.

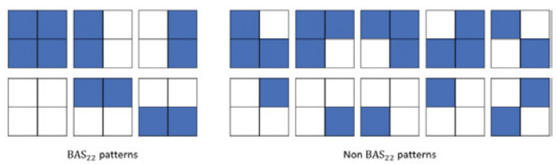


Figure 7 The Bars and Stripes-dataset. Patterns in the dataset are shown on the left, all other patterns are shown on the right and are not in the dataset.

The hybrid Helmholtz machine tries to learn the probability distribution of the input set, meaning the hybrid Helmholtz machine tries to learn how often a 2-by-2 pixel image is likely to occur. This learning of the parameters by the hybrid Helmholtz machine happens in an iterative fashion. Each iteration consists of first learning the probability distribution of the input by trying to replicate the (fixed) output, and second, the other way around for the probability distribution of the output.

After learning the hybrid Helmholtz machine, it can be used to represent the input data efficiently. The performance of the machine is measured in terms of how good the output probability distribution matches that of the input. That is, how often each of the samples above occurs in the output. Note that the ten patterns that originally were not in the BAS_22-dataset may still appear as output, given a suboptimal training of the parameters. Performance of both the classical and the hybrid Helmholtz machine is defined by the so-called Kullback-Leibler divergence, which indicates how well the probability distributions of the input and output match. The larger the Kullback-Leibler divergence is, the worse the two probability distributions match and the worse the performance is. When the output probability distribution is the same as the input, the Kullback-Liebler divergence equals zero and the Helmholtz machine has learned to reproduce the output with 100% accuracy.

Quantum hardware is still in development and running the hybrid Helmholtz machine requires too much resources. More qubits and more stable qubits are required, together with a link to a classical interface in order to train the hybrid Helmholtz machine. The hybrid Helmholtz machine can be simulated on a conventional computer, however at the cost of an increase in running time. Therefore, the number of learning cycles of the hybrid Helmholtz machine is limited.

In Figure 8 we see results of both the classical Helmholtz machine and the hybrid Helmholtz machine in terms of the Kullback-Leibler divergence. On the horizontal axis the number of samples used is stated. Naturally, this number is larger for the classical Helmholtz machine than for the hybrid Helmholtz machine.

Based on these results we can conclude two things. The first being that it is indeed possible to implement a hybrid Helmholtz machine on a gate-based quantum computer. The second that more training cycles of the hybrid Helmholtz machine will probably also lead to better results, comparable to that of the classical Helmholtz machine.

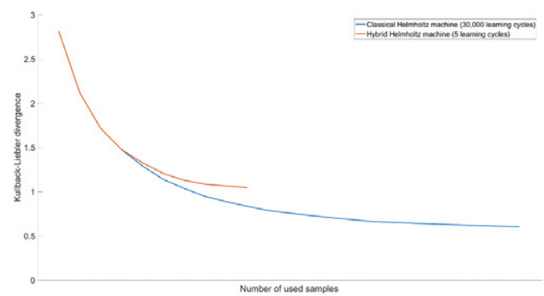


Figure 8 Kullback-Leibler divergence of both the classical Helmholtz machine for 30,000 learning cycles and the hybrid Helmholtz machine for only five learning cycles.

Conclusion

In this article we discussed the possible effects of quantum computing on machine learning. Machine learning is applied in various areas: from pattern recognition to anomaly detection and from marketing to gaming. However, machine learning also has its limitations, such as the long running times and the restricted capacity. Using quantum computing, some of these challenges can be overcome.

Three ways can be identified in which machine learning can benefit from quantum computing. The first is run-time improvements. The second advantage is an increase in the capacity of associative or content-addressable memories. The third is more efficient learning. This means that quantum machine learning requires less data samples or less learning cycles to obtain similar or even better results.

In this article we focused on a specific machine learning algorithm: the Helmholtz machine. With both a recognition and a generative neural network, the Helmholtz machine is used to recognize patterns and to find explanations for corrupted input data. The Helmholtz machine learns iteratively an (unknown) probability distribution by trying to recognize patterns and generating new samples.

A Helmholtz machine benefits from quantum computing as it allows for more efficient learning. A hybrid classical-quantum Helmholtz machine was implemented on the Quantum Inspire platform, developed by QuTech in the Netherlands. This implementation is the first gate-based implementation of a hybrid Helmholtz machine. However, in this phase of the development of the quantum computer, a simulation of a quantum computer on a conventional (super) computer is used.

The Helmholtz machine was also implemented in a classical manner on a digital computer. Simulating the hybrid Helmholtz machine led to an increase in the running time, hence both implementations are not compared in terms of running time. Instead, the results are used to show that it is indeed possible to implement a hybrid Helmholtz machine in a gate-based manner. Performance was evaluated using the Kullbach-Leibler divergence, indicating how well the learned probability distribution matches that of the input.

We saw that the Kullbach-Leibler divergence decreased as the number of samples and the number of iterations increased for the classical Helmholtz machine. We also saw that the performance for the hybrid Helmholtz machine roughly followed that of the classical version for much less training iterations. We expect that with more iterations and improved quantum hardware the performance of the hybrid Helmholtz machine will improve and probably surpass that of the classical Helmholtz machine.

References **Aaronson, S. (2015).** Read the fine print. Nature Physics 11.4, 291. **Benedetti, M., Realpe-Gómez, J., & Perdomo-Ortiz, A. (2018).** Quantum-assisted helmholtz machines: a quantum–classical deep learning framework for industrial datasets in near-term devices. Quantum Science and Technology 3.3. **Dunjko, V., & Briegel, H. J. (2018).** Machine learning & artificial intelligence in the quantum domain: a review of recent progress. Reports on Progress in Physics 81.7. **Fahri, E., & Neven, H. (2018).** Classification with quantum neural networks on near term processors. arXiv preprint. **Lopez-Chagoya, T. J. (2018).** Hybrid Helmholtz machine: A gate-based quantum circuit implementation. Maastricht, The Netherlands: Maastricht University: Master's thesis. **MacKay, D. J. (2003).** Information Theory, Inference, and Learning Algorithms. Cambridge University Press. **QuTech. (2018).** Quantum Inspire Home. Retrieved from Quantum Inspire: https://www.quantum-inspire.com/ **Rebentrost, P., Bromley, T. R., Weedbrook, C., & Lloyd, S. (2018).** Quantum Hopfield neural network. Physical Review A. **Schuld, M., & Petruccione, F. (2018).** Supervised Learning with Quantum Computers. Springer.

Fotos: Privat

The Capacitated Vehicle Routing Problem – A hybrid solution method using a quantum annealer

Christoph Roch, Stefan Langer

Quantum computing is one of the hottest topics in computer science. With D-Wave Systems releasing the first commercially available quantum annealer in 2011[1], there is now the possibility to develop practical quantum algorithms for solving complex optimization problems. In this article a hybrid quantum solution method for the Capacitated Vehicle Routing Problem is presented.

Introduction

Optimization problems can be found in many application domains, be it economics and finance [1], logistics [2], or healthcare [3]. Their high complexity engaged researchers to develop efficient methods for solving these problems [4].

This article regards the Capacitated Vehicle Routing Problem (CVRP), an NP-hard optimization problem that plays a major role in common operations research and is excessively studied since its proposal in 1959 [5]. It generalizes and combines many important research scenarios like intelligent transportation, autonomous driving or automation and optimization.

The classic CVRP (see Figure 1) can be described as the problem of designing optimal routes from one depot to a number of geographically scattered customers subject to some side constraints. It can be formulated as follows:

Let $G = (V, E)$ be a graph with $V = \{1, \ldots, n\}$ being a set of vertices representing n customer locations with the depot located at vertex 1 and E being a set of undirected edges. With every edge $(i, j) \in E$, $i \neq j$ a non-negative cost c_{ij} is associated. This cost may, for instance, represent the (geographical) distance between two customers i and j. Furthermore, assume there are m vehicles stationed at the depot that have the same capacity Q. In addition, every customer has a certain demand q [6]. The CVRP consists of finding a set of vehicle routes such that

- each customer in $V \setminus \{1\}$ is visited exactly once by exactly one vehicle;
- all routes start and end at the depot;
- the sum of customer demand within a route does not exceed the vehicles' capacity;
- the sum of costs of all routes is minimal given the constraints above;

[1] https://www.dwavesys.com/news/d-wave-systems-sells-its-first-quantum-computing-system-lockheedmartin-corporation

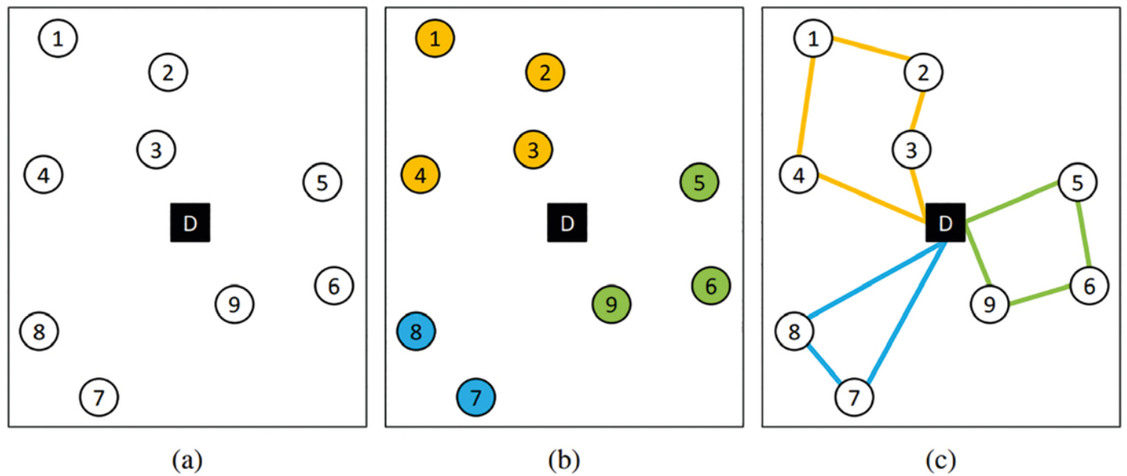


Figure 1: Overview of the CVRP and the 2-phase-heuristic. (a) Initial state with 9 customers and 1 depot. (b) Clustering phase results in three clusters found. (c) Routing phase determines shortest path inside each cluster [14].

With D-Wave Systems releasing the first commercially available quantum annealer in 2011[2], there is now the possibility to find solutions for such a problem in a completely different way than classical computation does. However, quantum computation compared to classical computation is still in its infancy and one of the major problems is that quantum hardware is limited regarding the number of quantum bits (qubits) and their connectivity on the chip. Generally, this leads to difficulties in solving large (real-world) optimization problem instances on the hardware. Therefore hybrid methods will be increasingly used for solving complex problems with quantum annealing algorithms. It can be useful to split these problems into sub-problems and thus outsource the complex part to a quantum annealing hardware.

In this article an intuitive way to split the CVRP into smaller optimization problems by taking advantage of a classical 2-phase-heuristic [7] is presented (see Figure 1). The heuristic divides the CVRP into two phases, the clustering phase and the routing phase. The clustering phase itself can easily be computed by a classical clustering algorithm (e.g. modified k-means algorithm), which tries to group the customers into capacity restricted clusters. Doing this, the Euclidean distance between customers assigned to a cluster should be minimized. The routing phase can be represented by the well-known NP-hard Traveling Salesman Problem (TSP) [8]. Thus, the minimal tour in which all customers of a cluster are visited once is sought. Doing this, the tour starts and ends in one place, i.e. the depot. In Figure 1 a CVRP example with the 2-phase-heuristic is visualized. First the customers are grouped into clusters (b) before efficient vehicle routes in each cluster are calculated (c).

D-Wave's quantum annealing hardware is known to solve a specific optimization problem called a quadratic unconstrained binary optimization (QUBO) problem [9]. QUBO is a unifying model which can be used for representing a wide range of other combinatorial optimization problems, to which also the TSP belongs.

In this article a hybrid method based on the 2-phase-heuristic to solve the CVRP using a quantum annealer is proposed. While the clustering phase is computed classically, the routing phase, i.e. the TSP, is solved on the quantum hardware.

Quantum annealing on D-Wave processor

The most obvious difference between quantum and classical informatics is the so called state principle. Quantum particles can reside in multiple states, such as having different locations, energies, or move in different speeds. Additionally, in quantum mechanics, such particles adopt not only one, but multiple states at the same time. This behavior can be illustrated by thinking of quantum particles as waves that can overlap, extinguish or amplify one another, just as known from classical physics.

One property of quantum bits (qubits) is called superposition and describes the ability to reside in two states simultaneously, hence be in the state 0 and 1 at the same time [10].

The difference between the two computing systems gets even more clear with multiple (qu)bits: A classical computer can represent 2^n different numbers with n bits, but only save one of them at a time. A quantum computer, however, can represent the same amount of numbers with an equally amount of quantum bits, all at the same time [11].

Another property that is not consistent with our classical view on physics is called entanglement. The manipulation of one entangled bit can affect the measurement of another bit. More interestingly, this behavior does not require the two qubits to be in direct contact, and is therefore the basis of research concerning quantum teleportation [11].

Using these fundamental quantum effects, one hopes for solving complex problems in a faster way than classical computation does. However, for solving optimization problems like the TSP on D-Wave's quantum annealing hardware the problem has to be formulated as a quadratic unconstrained binary optimization (QUBO) problem [9], which is one of two input types acceptable by the machine (alternative: the Ising model [12]). The functional form of the QUBO is:

$$\min x^t Q x \qquad \text{with } x \in \{0,1\}^n$$

with x being a vector of size n with binary variables, and Q being an $n \times n$ real-valued matrix describing the relationship between the variables. Given matrix Q, the annealing process tries to find binary variable assignments to minimize the objective function stated above.

The metaheuristic quantum annealing itself seeks for the minimum of the optimization function, which corresponds to the best solution of the defined optimization problem.

Hybrid solution method

The classical distance based clustering phase, in which every customer is assigned to a vehicle cluster considering the capacity constraint, is straight forward. Thus, the focus in this section is on the mapping of the TSP to the QUBO formulation.

The TSP tries to find the shortest tour (starting and ending at the depot) between the customers of a cluster.

In [13] the mathematical QUBO problem (respectively Ising Model, which is mathematically equivalent) for the TSP is stated:

$$H_A = A\sum_{i=1}^{n}\left(1-\sum_{j=1}^{n} x_{i,j}\right)^2 + A\sum_{j=1}^{n}\left(1-\sum_{i=1}^{n} x_{i,j}\right)^2$$

$$H_B = B\sum_{j=1}^{n} D_{ui}x_{u,j}x_{i,j+1}$$

H_A and H_B describe the energies of the underlying problem, for which the configuration with the lowest corresponding energy is sought. The binary variable $x_{i,j}$ is 1 if the customer with index i is located at position j in the tour. The first term (constraint) of H_A requires that each customer must occur only once in the cycle, while the second term of H_A enforces that each position in the cycle must be assigned to exactly one customer. This defines the order of the customers within the tour. The squared differences of these terms ensure that exactly one customer has a unique position in the tour. Otherwise, a high penalty value A would be added to the solution energy, which states the solution itself as suboptimal or rather invalid (see example below).

The term H_B represents the objective function of the TSP in which D_{ui} is the Euclidean distance between the customer u and i. Thus, the minimization function sums all costs of the edges between successive customers. The total solution for the TSP QUBO problem is then composed of the energies: $H = H_A + H_B$

Example (Regard first constraint of H_A):

$$A\left(1-\sum_{j=1}^{n} x_{1,j}\right)^2 = A\left(1-\left(x_{A,1}+x_{A,2}+x_{A,3}+x_{A,4}\right)\right)^2$$

Assume finding a tour between 4 customers. There are four possible positions of customer A in the tour (*A1, A2, A3, A4*). These position-to-customer-combinations are represented by the binary variable x_{ij} and states that customer i has the position j in the tour. If $x_{A1} = 1$, customer A was assigned position 1 in the tour.

Under the premise that customer A is fixed, sum up all binary variables x_{Aj}. This leads to various cases:

3. No position was assigned to customer A: $A(1-(0+0+0+0))^2=A$
3. Exactly one position (2) was assigned to customer A: $A(1-(0+1+0+0))^2=0$
3. Two positions (1, 3) were assigned to customer A: $A(1-(1+0+1+0))^2=A$

As one can see, the best case - with the lowest energy - is in case 2, where exactly one position is assigned to customer A. This is also the only valid solution. In the other cases (also in case 4 and 5, which were omitted) the penalty value A is added on top of the system energy, which defines a solution as invalid. The second constraint of H_A can be regarded analogously.

Conclusion

In this article, a hybrid approach for solving the capacitated vehicle routing problem (CVRP) using D-Wave's quantum annealing hardware was provided.

The most important step was to find an intuitive way to map this optimization problem to a QUBO problem that could then be embedded on the quantum annealer. Doing this, the classical 2-phase-heuristic has been used, which enables to divide the complex problem into a clustering phase as well as a routing phase. The solution method was tested and compared regarding the solution quality as well as the computational time. The results can be found in [14].

We showed that the hybrid approach was able to compete with other classical constructions and 2-phase-heuristics and in some cases even surpasses them with regard to solution quality. However, it should be mentioned that there are other solution methods like metaheuristics, which provide a better solution with regard to some of the used benchmark datasets.

The computational time of this solution method must be considered differentiated.

Due to the currently limited number of available qubits on the D-Wave processor, the tool QBSolv must be used for large QUBO problem instances. This tool makes it possible to split the QUBO into smaller subQUBOs and to place them one after the other on the quantum annealer. However, this hybrid solution option involves certain latency and waiting times which lacks the hoped acceleration of the computational time compared to the classical option. However, the real solution time for an embeddable QUBO problem on the D-Wave quantum annealer is located in the range of microseconds.

At the 2018 D-Wave Qubits Europe users conference D-Wave provided an outlook on the future hardware directions of quantum annealing. They stated that the connectivity and the number of qubits on D-Wave machines will immensely rise over the next years[2]. This news give hope that in the future D-Wave's quantum annealers are more suitable for this kind of optimization problems and a shorter total computation time can be achieved.

References: **[1]** Black, F. and Litterman, R. (1992). Global portfolio optimization. Financial analysts journal , 28–43 **[2]** Caunhye, A. M., Nie, X., and Pokharel, S. (2012). Optimization models in emergency logistics: A literature review. Socio-economic planning sciences 46, 4–13 **[3]** Cabrera, E., Taboada, M., Iglesias, M. L., Epelde, F., and Luque, E. (2011). Optimization of healthcare emergency departments by agent-based simulation. Procedia computer science 4, 1880–1889 **[4]** Papadimitriou, C. H. and Steiglitz, K. (1998). Combinatorial optimization: algorithms and complexity (Courier Corporation) **[5]** Dantzig, G. B. and Ramser, J. H. (1959). The truck dispatching problem. Management science 6, 80–91 [6] Laporte, G. (1992). The vehicle routing problem: An overview of exact and approximate algorithms. European journal of operational research 59, 345–358 **[7]** Laporte, G. and Semet, F. (2002). Classical Heuristics for the Capacitated VRP, chap. 5. 109–128. doi:10.1137/1.9780898718515.ch5 **[8]** Lawler, E. L. (1985). The traveling salesman problem: a guided tour of combinatorial optimization. Wiley-Interscience Series in Discrete Mathematics **[9]** Boros, E., Hammer, P. L., and Tavares, G. (2007). Local search heuristics for quadratic unconstrained binary optimization (qubo). Journal of Heuristics 13, 99–132 **[10]** McGeoch, C. C. (2014). Adiabatic quantum computation and quantum annealing: Theory and practice. Synthesis Lectures on Quantum Computing 5, 1–93 **[11]** Homeister, M. (2008). Quantum Computing verstehen. Friedr. Vieweg & Sohn Verlag, 2 **[12]** Glauber, R. J. (1963). Time-dependent statistics of the ising model. Journal of mathematical physics 4, 294–307 **[13]** Lucas, A. (2014). Ising formulations of many np problems. Frontiers in Physics 2, 5 **[14]** Feld, S., Roch, C., Gabor, T., Seidel, C., Neukart, F., Galter, I., ... & Linnhoff-Popien, C. (2018). A Hybrid Solution Method for the Capacitated Vehicle Routing Problem Using a Quantum Annealer. arXiv preprint arXiv:1811.07403.

[2]https://www.dwavesys.com/sites/default/files/mwj_dwave_qubits2018.pdf

Christoph Roch

Christoph Roch is doing his PhD at the LMU Munich at the Chair of Mobile and Distributed Systems with a focus on optimization problems and their solvability by quantum computing. Additionally the computer scientist is a member of the Quantum Applications and Research Lab (QAR-Lab) and contributes his knowledge to various industrial projects, research and teaching.

Stefan Langer

Stefan Langer is doing his PhD at the LMU Munich at the Chair of Mobile and Distributed Systems in the sector of quantum computing. In between his master's study in media informatics and his work as a researcher, Stefan has worked as a software engineer for a supplier of indoor positioning technologies for several years.

Fotos: Privat

Volkswagen and quantum computing:

An industrial perspective

Sheir Yarkoni, Martin Leib, Andrea Skolik, Michael Streif, Florian Neukart, David von Dollen

What is quantum computing at Volkswagen?
Quantum computing has gained serious mainstream attraction over the past couple of years. Decades of research from universities around the world have yielded industrial efforts in companies such as Google, IBM, D-Wave, Rigetti, and a host of start-ups rushing to create the next groundbreaking technology. The motivation behind quantum computing is promising, as Richard Feynman originally proposed: Nature is quantum ("dammit!") and the natural power of quantum mechanics could be used to create a sophisticated computer. Since then, various algorithms have been written for quantum computers in the fields of combinatorial optimization, machine learning, quantum materials simulations, and more. Quantum computers are similar to regular computers in the sense that they have processors that perform operations and calculations to produce a result. However, instead of being composed of many bits of information that can be changed from 1 to 0 and 0 to 1 in a controllable way, quantum computers are made of quantum bits (qubits) that can be 0 and 1 at the same time. These qubits have a property called entanglement, which means that all the qubits in the system are connected with each other in a fundamental way. When we change the conditions of one qubit in our computer, it could possibly affect all other qubits in our computer without any additional work. This makes quantum computers extremely powerful, provided that one can write an algorithm that exploits these quantum properties. Researchers around the world are constantly coming up with new ideas about how to use these novel devices.

But how is this relevant to Volkswagen? Volkswagen is much larger than just a car manufacturer, putting cars on the road. The challenges that need to be overcome to deliver our services span the entire technological spectrum: Physically building a car is an engineering problem. Scheduling deliveries of cars from factories to dealerships is a logistical problem. Designing better batteries in electric cars is a chemistry problem. Organizing warehouses for parts storage is an optimization problem. The list goes on endlessly, and the IT and R&D infrastructure in Volkswagen need to support all these different areas. And this is where quantum computing fits in Volkswagen, helping to solve these complicated problems with cutting edge technology. We aren't simply interested in theoretical questions about algorithms and complexity. We need to know how these computers work on a fundamental level, but we also look into the future and see which specific areas of our business they can impact. When researchers talk about a new quantum algorithm, we look at our business and ask ourselves: where can this help us? Can we use this to organize our factories better? Can we now simulate new materials we weren't able to before?

Historically, the focus has been on showing how quantum computers could use these algorithms to solve problems "faster" than traditional computers. A popular example for this is Shor's algorithm, which factors a number into its prime factors, a process used often in cryptography and cybersecurity. Imagine a hacker trying to decrypt a secure file: the hacker knows the key is composed of some combination of numbers multiplied together, but not which numbers. The time it takes a computer (or a hacker) to go through these combinations grows rapidly with the number of digits in the key, which is what makes these methods of encryption (like RSA) secure. However, for a big enough quantum computer, something entirely different happens. Instead of going through individual combinations of numbers, the hacker needs to apply a sequence of instructions (called quantum gates) and the quantum computer can determine on its own which combination of numbers produces the decryption key. And most important, the number of instructions for the quantum computer depends only on the number of digits in the key, making this algorithm extremely effective. Hence, many people are now looking for something called "post-quantum cryptography", the idea of creating new encryption algorithms that can withstand the processing power of a quantum computer. This example is a typical benchmark for quantum computing: what problem can we solve, or what algorithm can we write, where we know that quantum computers will always be better? Pursuing the answer to this question has led to the introduction of a term called "quantum supremacy"- a task performed by a quantum computer that beats every known classical approach. Over the last few years, researchers have been working hard to find cases of this, both in theory and in practice, with limited success. We now have a small collection of problems we think can be solved most efficiently with quantum computers (factoring and quantum chemistry simulations are most often used as examples), but building quantum computers that are big enough to run these algorithms is still a few years away. In the nearer future, a different benchmark is becoming popular, called "quantum advantage". As opposed to supremacy, quantum advantage has the relaxed condition that the quantum computer simply needs to provide a tangible gain by using it as opposed to a classical computer. This could be in terms of cost, runtime, or some other beneficial metric. There is considerable debate about what the correct benchmark should be, and what the best path is to viable quantum computing.

At Volkswagen, we see these two ideas as separate, but not necessarily competing, concepts. On the one hand, quantum supremacy can help us solve problems that previously couldn't be tackled. For example, simulating quantum properties of materials is notoriously difficult and requires significant computing power. This means that R&D in this area can involve painstaking hours of laboratory work developing a material, and taking careful measurements over and over again to get the necessary information. But quantum computers are inherently quantum materials themselves. If we had access to a large enough quantum computer, we could simply write a program that sets the conditions we want to test and let the quantum computer do the work. By measuring the results of this quantum program we could simulate the interactions and properties we are interested in before even producing the materials, allowing us to do research in a fundamentally new way. On the other hand, with quantum advantage, we can look to improve existing techniques to solve complicated problems. One field this is particularly suitable for is logistics. Every day at Volkswagen we ship things from one location to another. Whether we're sending car parts from storage to factories, or products from factories to dealerships, a variety of conditions needs to be taken into account when optimizing logistics. Weather or traffic conditions can change by the hour, and our systems in Volkswagen need to be able to deal with these unpredictable fluctuations, otherwise both our customers and the company suffer. With quantum computing, we could write complex programs that take such variables into account in real-time, allowing us to sort through endless combinations of solutions to these problems quickly, saving both time and money for the company and its workers. For this reason, we have worked hard over the past few years to build up our quantum computing expertise with people in San Francisco, Munich, and Wolfsburg, so we understand how to take cutting edge research and adapt it to help Volkswagen.

How Volkswagen is investing in quantum computing now
Innovation is the key to survival in business. Being able to adapt to a changing market, and staying ahead of the technology curve is imperative to company growth. Stagnation will quickly lead to falling behind the rest of industry, making it hard to compete. We see our quantum computing team at Volkswagen as an investment in the future. Our goal is always to put the best products on the market, and the easiest way to accomplish this is by leading the industry through research and development. This means staying up-to-date with the latest trends in technology, and developing the skills necessary to use them. In this aspect, quantum computing makes no difference. We cannot wait for quantum computers to impact the market before we learn how to use them. That is why we are constantly learning and developing internally, connecting quantum computing to different branches in Volkswagen, to assess where it can be most effective. To this end, we have ongoing collaborations with quantum computing leaders Google and D-Wave Systems, and together we work towards developing the tools and strategies needed to incorporate quantum computing into our existing infrastructure. The state of quantum computing now is similar to that of computers in the 1950s. There are no standard operating systems, no programming languages or compilers. The work being done now by quantum computing researchers, both on the hardware and software side, is laying the groundwork for future users of these devices. The industry of quantum computing is ripe for developers at the moment, people who are eager to understand the technology at low levels, and help build the stack on which future applications will sit on. The main challenge for the coming years is to come up with techniques that intelligently leverage the quantum resource that's

provided by these devices. At Volkswagen we are contributing to this in many different aspects.

Volkswagen's involvement in quantum computing started in late 2016 with a proof-of-concept project with D-Wave Systems to investigate the readiness of quantum computing for industry. The goal was to showcase a small prototype program at CeBIT 2017 to highlight why quantum computing was interesting for a company like Volkswagen. The result was a traffic-flow optimization program that used GPS coordinates of 418 taxis in Beijing to resolve traffic congestion. Through this project our researchers in San Francisco and Munich learned a fundamentally different paradigm of programming for quantum computers: instead of writing many lines of code for a computer to step through, we simply set the appropriate initial conditions and constraints for the quantum computer, and let it evolve naturally. When this process is performed correctly, reading out the solutions provided by the quantum computer resolved the traffic congestion. The importance of this work for Volkswagen was two-fold. Firstly, by doing the development work ourselves we retained the experience and knowledge required to work with quantum computers. Secondly, and most importantly, we were able to translate data taken from a real-world system (GPS coordinates) and use this to write a program that solved a difficult problem using a real quantum processor, what had never been done before. From an industrial perspective, this project proved vital in forming Volkswagen's path forward into quantum computing. After learning that it was indeed possible to use quantum computers for problems that are relevant to Volkswagen, and with the strong supsupport by Volkswagen CIO Martin Hofmann, we were able to expand our research and development efforts. Today, we focus on applying our knowledge to research areas where we see the best fit between quantum computing and Volkswagen.

One of the most promising applications of quantum computing is quantum machine learning. Machine learning algorithms are robust against noisy data by design, and often can use this noise to improve performance. Because near-term quantum devices aren't advanced enough to work in ideal conditions, this makes them perfect for quantum machine learning. Most recent proposals in the quantum machine learning community focus on taking existing classical algorithms and translating them to the realm of quantum computers. This can either mean extracting certain parts of an algorithm that can be sped up by executing them on a quantum device, or finding purely quantum analogs of existing algorithms. In between these two practices there are the so-called hybrid quantum classical algorithms, which jointly use both types of computers. One of our main research topics is implementing these machine learning networks directly on a quantum processor (called a "quantum neural network"). By doing this on a quantum processor instead of a regular computer, we can encode much more information in our quantum network, due to how the qubits interact with each other. In our work we research various methods of controlling the quantum gates which govern the interactions between the qubits to give us the best results for our quantum machine learning algorithms. Along with developing the algorithms themselves, we also look for tasks where quantum machine learning algorithms are more suitable than classical machine learning. This allows us to build solutions inside Volkswagen using current machine learning techniques, but including the power of quantum machine learning. These solutions can in turn be used for practical applications. Problems like predicting maintenance for machines in our factories, price changes in the automotive market, or prediction of traffic congestion are all still intractable even for current machine learning solutions, making them good candidates for quantum machine learning algorithms. Together with researchers from Google, we are working towards creating quantum machine learning algorithms that will enable us to do all these applications and more on the quantum computers of today and those that are still to come.

Applications of quantum computing are not all confined to theoretical subjects. A good example of this are optimization problems, another proposed sweet-spot for quantum computers. In business, as they say, time is money, and so everything can be boiled down to an optimization problem. Every decision in a company is weighed against resources, financial cost, and opportunity cost – and the longer it takes to make a decision the higher the cost. Anything from amending logistics schedules to mobility solutions to product pricing can be formulated as an optimization problem. For this reason we've been working with our partners at D-Wave and Google to learn how we can use their quantum processors to solve our internal optimization problems. We have already produced multiple prototypes of optimization solutions using quantum computing. At the Web Summit 2018, we showed how we can use a D-Wave quantum processor to assign taxis on-demand in Barcelona, and at CeBIT 2018 we showed how one could optimize a car mirror's shape to reduce acoustic noise with a hybrid quantum-classical algorithm. Recently we also published a first-of-its kind demonstration of quantum materials simulation of small molecules, which will allow us to investigate new materials and their properties. We showed how a D-Wave quantum processor could simulate properties of these molecules by translating the simulation to an optimization problem. With our collaborators at Google, we've been working on solving complex optimization problems with a significantly different approach. We are researching methods to compile quantum circuits in a way that exploits the inner structure of these optimization problems to compress the circuits. This will allow us to make even more efficient use of quantum computers when solving these problems, much like compilers work in regular computers today. We can then train these quantum circuits to solve problems like traffic flow, quantum machine learning, and high-dimensional optimization of car parts. While many of these projects are small relative to the size of our company, the knowledge and experience they provide help us prepare Volkswagen for the arrival of bigger quantum computers in the future.

Volkswagen's future in quantum computing

From Richard Feynman's proposal in the 1980s, to the device prototypes of the early 2000s, to the quantum processors of today, there is no doubt that quantum computing has advanced enormously over the years. The way this technology works is a fundamental shift in how we view computing, requiring a different approach to both designing and programming these computers. It seems unlikely that quantum computers will ever replace traditional computers in the workplace, but they are poised to be great companions to classical computers, accelerating the way we view computing and allowing us to perform tasks we were unable to before. The truth about quantum computing is that it's too early to know exactly what the first "killer application" will be. That the technology holds enormous potential has become clear over time, and at Volkswagen we have invested deeply in quantum computing to position ourselves for the future. We have to be ready today for the technology of tomorrow. No matter what field this "killer application" of quantum computing will come from, at Volkswagen we must find a way to use it to benefit everyone. We can use our optimization solutions for smart mobility platforms that will reduce traffic congestion in large cities. Quantum machine learning algorithms could revolutionize autonomous cars, making them safer and more reliable at a lower cost. With new material simulations we can research better components for our products, reducing our waste production and impact on the environment. After decades of research, we are finally reaching the point where quantum computers are leaving the research labs and become accessible to industrial early adopters. For us at Volkswagen it's not enough to be users of this technology, we need to become experts in it to help ourselves and others accelerate the growth of the quantum computing community. This is why we are constantly expanding our quantum computing efforts by partnering with industry leaders, attending conferences and events around the world. Internally within our company, we work closely with experts in related fields to understand what their needs are, and how we can help Volkswagen grow using quantum computing wherever possible. We know that these quantum devices, although small today, are capable of doing extraordinary things in a fundamentally different way. We will continue to showcase their use in industry applications like we've done with mobility optimization and materials research, while we prepare for the quantum computers of the future. Whichever path leads in the end to the quantum computing revolution, Volkswagen is committed to leading the way.

Sheir Yarkoni
Sheir is a quantum computing researcher at the Volkswagen Data:Lab in Munich. Before joining Volkswagen he worked for D-Wave Systems with a focus on benchmarking quantum processors for industry applications. His work includes doing a PhD in hybrid quantum-classical algorithms for applications at Volkswagen and Leiden University.

Martin Leib
Martin joined the Volkswagen Data:Lab quantum computing team after post-doctoral stints in Japan, Scotland, and Austria. He obtained his PhD in physics, developing superconducting processors at TU Munich. Martin leads the Data:Lab research in optimized quantum circuits for quantum machine learning and optimization.

Andrea Skolik
Andrea gained industry experience in many application areas before joining the Data:Lab including machine learning, e-commerce, and finance, and holds a Master's degree in computer science focusing on machine learning and robotics. She is currently a PhD student at LMU in Munich researching quantum machine learning.

Michael Streif
Michael is a physicist currently doing his PhD with University of Freiburg at Volkswagen. Before that he studied in Freiburg and Oxford. His current research involves understanding the physical effects governing quantum processors and their applications to optimization problems.

Florian Neukart
Florian is the principal quantum computing researcher for Volkswagen, based at the CODE:Lab in San Francisco. He holds a PhD and several Master's degrees in computer science. Before moving to the CODE:Lab, Florian brought quantum computing to Volkswagen as co-founder of the Data:Lab in Munich. Florian is also an Associate Professor at Leiden University for quantum computing.

David von Dollen
David is a Senior Data scientist in the Volkswagen CODE:Lab in San Francisco, holding a Master's degree in Computer Science and machine learning from Georgia Institute of Technology. His work involves accelerating machine learning algorithms with new techniques using quantum computers. And he is currently working towards a PhD at Leiden University.

Benchmarking in Quantum Algorithms:
A Case Study with Quantum Minimum Cut/Maximum Flow Algorithm for Network Analysis

Colleen M. Farrelly and Uchenna Chukwu

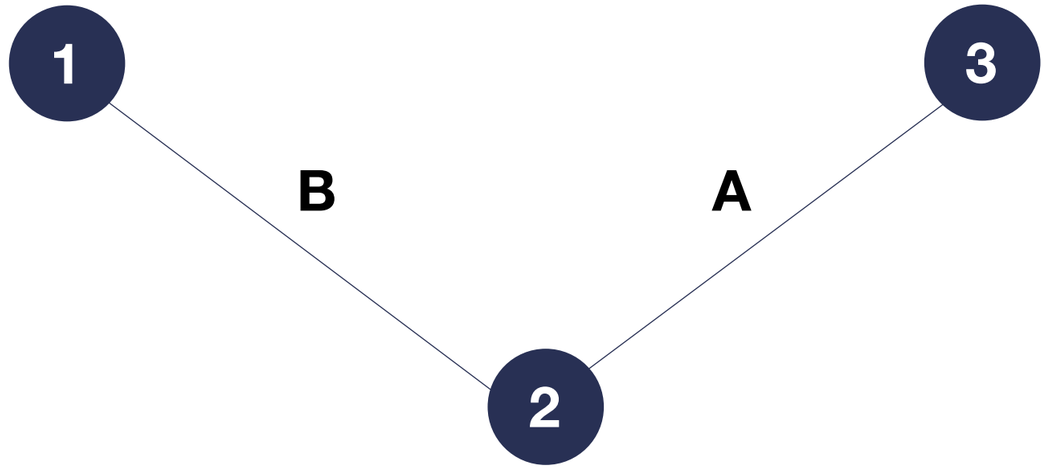


Fig. 1. Example graph used to explain parallel edges in the Forman-Ricci curvature formula for unweighted graphs.

1. Introduction

1.1 Network Analysis Overview

Network analysis is ubiquitous in many fields of science today, and one of the most-studied areas of network analysis involves centrality rankings of vertices and edges of a given graph [1]. Vertex-based centrality metrics abound and have found success in many applications [1]. Some examples of vertex-based centrality metrics include hub centrality [2], eigenvector centrality [3], degree centrality [4], and cross-clique centrality [5]. Important applications of these have included super-spreader identification in epidemic models [6], assessment of network infrastructure and vulnerability [8], and targeted disruption of terrorist communication networks [9].

Edge-based rankings are less common, and many focus on edges as a means to adjust vertex-based rankings (such as Katz centrality [9], PageRank centrality [10], or betweenness centrality [11]), rather than edge-based rankings as a goal [1]. However, recent studies suggest that metrics derived specifically to quantify edge importance can be useful tools and can provide additional information regarding network structure and can be used to derive vertex importance rankings that perform well in network disruption (such as the recently-developed Forman-Ricci curvature [12, 13]). Very few measures targeting edge properties currently exist, and new ways of measuring edge properties are likely to compliment existing metrics in network analysis. Benchmarking on a variety of graph structures can help establish new metrics as robust in network analysis or highlight their limitations on certain types of graphs, such as dense graphs.

Quantum computing offers several well-studied graph algorithms that can be adapted to derive edge importance metrics/rankings, including the minimum cut/maximum flow algorithm [14, 15]. Application of this algorithm on a given graph yields rankings of edges in terms of cut likelihood; cut likelihood reflects importance to flow disruption. Given the probabilistic nature of quantum graph analysis algorithms, a distribution of solutions at each step is given by the algorithm. Thus, edge 1 may be the most likely edge solution with a probability of 0.7, while edge 7 may be the least likely edge solution with a probability of 0.05. Vertex importance can then be derived by summing edge probabilities for edges connected to a given vertex, similar to how Forman-Ricci curvature is used to derive vertex importance scores. Minimum cut/maximum flow algorithms have been related to vertex and edge centrality previously, but no applications regarding quantum minimum cut/maximum flow approaches seem to exist. It is unknown how this type of algorithm might perform across types of network problems or how this metric might relate to Forman-Ricci curvature or other successful edge-based ranking metrics.

1.2 Contribution

This paper presents a novel edge importance scoring and subsequent derivation of vertex importance scoring based on a quantum minimum cut/maximum flow algorithm, which provides probabilistic solutions to the minimum cut/maximum flow problem. This yields a potentially useful edge-based centrality metric, which is explored in 3 small example graphs and compared with Forman-Ricci curvature edge and vertex rankings and betweenness centrality vertex ranking. Results suggest each edge-based metric yields different insight into the structure of the graph, and quantum minimum cut/maximum flow metrics provide another tool for network analysis.

This paper provides a case study on benchmarking quantum network analysis tools, as well as it introduces the new network analytics tool, such that other quantum network analysis tools can be developed and benchmarked effectively.

2. Methods

2.1 Overview of Forman-Ricci Curvature Centrality

One new tool that has been well-explored in the past few years is Forman-Ricci curvature, a discrete version of a central tool in differential geometry, Ricci curvature [12, 13]. Technically, Ricci curvature measures deviation from a standard sphere in Euclidean space, such that curvature on the manifold squishes, pulls, or compresses parts of the sphere [12]. This measures the distortion of Euclidean space at a given point on the manifold [12].

Forman derived a discrete version of Ricci curvature that could be applied to meshes, graphs, and other discrete geometric objects based on edge connectivity through vertices connected by that edge. For an unweighted graph, the formula for Forman-Ricci curvature simplifies to:

$$Ricci\ curvature = 2 - degree(vertex\ 1) - degree(vertex\ 2) \quad (1)$$

where vertex 1 and 2 are the vertices connected by the edge of interest. In figure 1 below, consider edge A, which connects vertices 2 and 3. A parallel edge would connect to either vertex 2 (such as edge B) or vertex 3 (none in this example). Thus, the Forman-Ricci curvature for edge A would be -1, where the Ricci curvature is calculated as 2-1-2= -1.

To derive vertex-based metrics from the edge values, one can sum the Forman-Ricci curvature values for each edge connected to a given vertex. In figure 1, edges A and B both have Forman-Ricci curvature of -1, in which the sum of the Forman-Ricci curvature value for edges connected to vertex 2 is -2.

2.2 Overview of Betweenness Centrality

Betweenness centrality relies on number of shortest paths between vertices in the network, such that edges and vertices involved in a large fraction of shortest paths present in the network will rank high in betweenness centrality [11]. In figure 1, vertex 2 would rank high in betweenness centrality, as it is involved in shortest paths between vertices 1 and 2, 2 and 3, and 1 and 3. Vertices 1 and 3 are only involved in 2 shortest paths. Were there an edge C connecting vertices 1 and 3, all vertices would have an equal ranking.

Technically, betweenness centrality is defined as:

$$Betweenness\ centrality = \sum_{s \neq t \neq v} \frac{\sigma(v)}{\sigma} \quad (2)$$

where s and t are arbitrary vertices in the graph, v is the vertex of interest with respect to number of shortest paths through vertex v, σ(v) is the number of shortest paths through vertex v, and σ is the total number of shortest paths [11].

2.3 Overview of Proposed Quantum Maximum Flow/Minimum Cut Centrality

The maximum flow/minimum cut problem has a dual solution using quantum approximate optimization algorithm solutions in Rigetti's pyquil language, specifically the pyQAOA package's max_cut function (dual of minimum cut) with Nelder-Mead optimization and maximum steps of 5, 10, and 15, so as to be

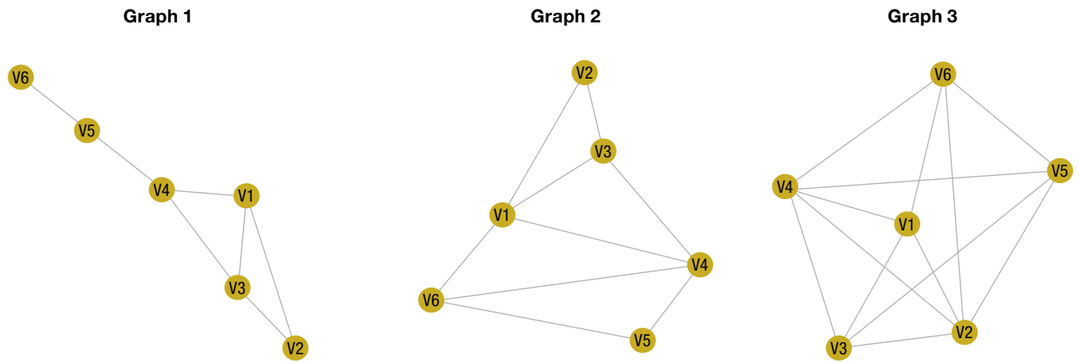


Fig. 2. Graphs used for the comparison of edge-based centrality metrics.

able to understand convergence properties on the 3 graphs. Convergence was defined as a solution with >67% probability of optimality.

One of the main advantages of using a quantum approach to this problem is the probabilistic nature of the solutions, such that all solutions are considered and can be ranked according to probability of optimality of a given solution. Thus, one can rank the cuts and, by extension, the links being cut by the solutions. This gives a weighting of edges, from which importance scores can be derived.

Edges were first ranked by converged solutions, including all solutions with >10% probability of solution optimality. Edge weights were assigned according to the sum of cut probabilities in solutions included in the converged solution. To obtain vertex importance scores, edge weights of edges connected to a given vertex were summed together, creating a final importance score for each vertex.

2.4 Overview of 3 Example Graphs and Ranking Comparison Methodology

This study focused on 3 graphs that were generated to illustrate the differences in these edge-based centrality metrics with simple graph structures that can be visualized to understand results (figure 2); these graphs vary density of graphs to explore functioning on both sparse and dense graphs. Vertex importance scores compared include Forman-Ricci curvature centrality, betweenness centrality, and quantum minimum cut/maximum flow centrality. Edge scores compared include Forman-Ricci curvature and quantum minimum cut/maximum flow centrality.

3. Results

3.1 Vertex Centrality Results

Results suggest that each type of vertex centrality yields slightly different rankings of vertex importance for the example graphs. However, there is some correspondence between different scores that suggests a relationship between Forman-Ricci curvature and betweenness centrality (correlation= -0.41 for graph 1), which has been found in previous papers [17]. Correlations of these different centralities scores with our proposed metric are -0.71 (Forman-Ricci curvature) and 0.71 (betweenness centrality), respectively for graph 1. These correlations are even stronger for graph 2: -0.88 (Forman-Ricci curvature and proposed metric), 0.96 (betweenness centrality and proposed metric), -0.79 (Forman-Ricci curvature and betweenness centrality). Given a standard deviation of 0 in graph 3's proposed metric results, correlations could not be obtained for comparison; however, a correlation of -0.52 is obtained for the comparison of Forman-Ricci curvature and betweenness centrality. While there is substantial correlation, results suggest that our proposed metric yields different information about vertex and edge importance to graph structure.

These results suggest that more work is needed to explore the efficacy of the new metric on dense graphs, as no variation in metric was noted for the new metric. By benchmarking on several types of graph structures, one is able to find potential pitfalls in new quantum algorithms and set the priority to understand these potential limitations.

3.2 Edge Metric Results

Edge metric results suggest that all three graphs have a hyperbolic geometry according to their generally negative Forman-Ricci curvature and confirm prior results of a moderate inverse relationship between Forman-Ricci curvature and betweenness centrality.

When considering edge importance in our proposed metric, most cut solutions yield many cuts in these 3 example graphs, giving most edges a high-probability cut value. Convergence to a solution took 10 steps for graphs 1 and 2; graph 3 required 15 steps for convergence. Below these values, probability was spread among many solutions, such that solutions were not informative about graph structure.

More work is needed to explore the new metric on dense graphs, such as graph 3. Results aren't sensitive enough to distinguish between edge or vertex importance, and convergence is slow. By comparing with several state-of-the-art classical methods across a variety of graph structures, it is possible to uncover potential problems with the quantum algorithm and how it compares to established network metrics.

Colleen M. Farrelly

Miss Colleen M. Farrelly is a machine learning researcher and data scientist whose industry experience spans healthcare, military logistics, biotech, finance, and education. Her research focuses mainly on classical and quantum algorithms in topological data analysis, manifold learning, and graph theory.

Uchenna Chukwu

Mr. Uchenna Chukwu is a software engineer and co-founder of Quantopo, LLC, whose work focuses on quantum machine learning algorithms and their applications in healthcare and supply chain logistics. His prior work includes quantum physics and string theory.

4. Conclusions

This paper presents a novel edge-based importance ranking of vertices and edges based on a quantum max flow/min cut algorithm, where cut probability at convergence is taken to be edge importance scoring. The proposed algorithm correlates well with extant edge-based important metrics, such as Forman-Ricci curvature and betweenness centrality. This suggests that the proposed importance ranking algorithm captures some underlying properties of the edges that are common among edge-based ranking metrics while providing additional information not captured by these extant edge-based ranking metrics. In addition, the limitations on this metric's use for dense graphs have been revealed, suggesting possible extensions of this benchmarking on larger dense graphs. This study also introduces a graph-based quantum algorithm and its benchmarking as a case study to a wider audience of network scientists, who may not be familiar with the tools of quantum computing or the methods needed to benchmark them.

References: **[1]** White, S., & Smyth, P. (2003, August). Algorithms for estimating relative importance in networks. In Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 266-275). **[2]** León, C. (2013). Authority centrality and hub centrality as metrics of systemic importance of financial market infrastructures. **[3]** Bonacich, P. (2007). Some unique properties of eigenvector centrality. Social networks, 29(4), 555-564. **[4]** Opsahl, T., Agneessens, F., & Skvoretz, J. (2010). Node centrality in weighted networks: Generalizing degree and shortest paths. Social networks, 32(3), 245-251. **[5]** Everett, M. G., & Borgatti, S. P. (1998). Analyzing clique overlap. Connections, 21(1), 49-61. **[6]** Fu, Y. H., Huang, C. Y., & Sun, C. T. (2015). Identifying super-spreader nodes in complex networks. Mathematical Problems in Engineering, 2015. **[7]** Hines, P., & Blumsack, S. (2008, January). A centrality measure for electrical networks. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual (pp. 185-185). IEEE. **[8]** Krebs, V. (2002). Uncloaking terrorist networks. First Monday, 7(4). **[9]** Zhao, J., Yang, T. H., Huang, Y., & Holme, P. (2011). Ranking candidate disease genes from gene expression and protein interaction: a Katz-centrality based approach. PloS one, 6(9), e24306. **[10]** Halu, A., Mondragón, R. J., Panzarasa, P., & Bianconi, G. (2013). Multiplex pagerank. PloS one, 8(10), e78293. **[11]** Brandes, U. (2001). A faster algorithm for betweenness centrality. Journal of mathematical sociology, 25(2), 163-177. **[12]** Weber, M., Saucan, E., & Jost, J. (2017). Characterizing complex networks with Forman-Ricci curvature and associated geometric flows. Journal of Complex Networks, 5(4), 527-550. **[13]** Sreejith, R. P., Mohanraj, K., Jost, J., Saucan, E., & Samal, A. (2016). Forman curvature for complex networks. Journal of Statistical Mechanics: Theory and Experiment, 2016(6), 063206. **[14]** Cui, S. X., Freedman, M. H., Sattath, O., Stong, R., & Minton, G. (2016). Quantum max-flow/min-cut. Journal of Mathematical Physics, 57(6), 062206. **[15]** Hastings, M. B. (2017). The asymptotics of quantum max-flow min-cut. Communications in Mathematical Physics, 351(1), 387-418. **[16]** Farhi, E., & Harrow, A. W. (2016). Quantum supremacy through the quantum approximate optimization algorithm. arXiv preprint arXiv:1602.07674. **[17]** Sreejith, R. P., Jost, J., Saucan, E., & Samal, A. (2017). Systematic evaluation of a new combinatorial curvature for complex networks. Chaos, Solitons & Fractals, 101, 50-67.

Table 1. Vertex centrality results for graph 1.

Vertex	Forman-Ricci Curvature	Betweenness Centrality	Quantum Minimum Cut/ Maximum Flow Centrality
1	-11	4	1.64
2	-6	0	1.64
3	-11	0	1.64
4	-11	6	2.46
5	-4	4	1.64
6	-1	0	0.82

Table 2. Vertex centrality results for graph 2.

Vertex	Forman-Ricci Curvature	Betweenness Centrality	Quantum Minimum Cut/ Maximum Flow Centrality
1	-20	3	2.46
2	-7	1	1.64
3	-13	0	1.64
4	-20	4	2.56
5	-4	0	1.64
6	-1	0	1.64

Table 3. Vertex centrality results for graph 3.

Vertex	Forman-Ricci Curvature	Betweenness Centrality	Quantum Minimum Cut/ Maximum Flow Centrality
1	-26	0	2.58
2	-36	2	2.58
3	-26	0	2.58
4	-36	4	2.58
5	-26	4	2.58
6	-26	0	2.58

Fotos: Privat

How Quantum got Gamed

Faisal Shah Khan and Nour Abura'ed

Since the 1960s, scientists have promised technologies working on the principles of quantum mechanics that can solve age-old problems facing the human civilization. For instance, consider the challenge of tamper-proof currency. Counterfeit currency can wreak havoc on an economy, most obviously in the form of uncontrollable inflation caused by large amounts of counterfeit currency circulating the economy. Uncontrolled inflation over-values the assets in a society or economy and negatively affects the cost and standard of living, and hence counterfeit currency is a relatively cheap but effective way to bring down a government from bottom-up. Much effort has therefore been put by central authorities throughout history into the development of tamper-proof currency, although prior to the 1960s all they could achieve in reality was tamper-resistant currency.

A common strategy adopted prior to the emergence of industry-based economics in the 18th century was to issue currency in the form of coins made of rare metals, typically gold or silver. This policy made counterfeiting a challenge simply because only the authorities had enough stores of these metals (due to their control over the police and armed forces). Unfortunately, this solution would consistently lead to economic deflation, making economic enterprise and growth difficult as only a limited amount of currency would circulate the vast majority of an economy (only those close to the authorities would get most of the gold and silver). Some authorities tried printing treasury-backed paper bills, such as the Tang dynasty in China in the 600s [1], but mostly for private bills of credit or exchange notes. And as this paper currency became more commonly used, inflation reared its ugly head, prompting a ban on paper currency in China till approx. 1455. Surely, counterfeiters got the best of this effort at easing deflation! More modern efforts in making tamper-resistant currency bills have of course been extremely successful; however, the prospect of a smart and dedicated counterfeiter finding a hack and reproducing even these currencies is ever present. Hence, the lynchpin that can hold the inflation-deflation dynamic in equilibrium is tamper-proof currency.

Until 1968, this lynchpin was beyond the reach of human knowledge and technological creativity. What was needed was a creative application of quantum physics, and Stephen Wiesner [2]. Wiesner, a quantum physicist, used the truly random nature of quantum physical systems as a solution to the problem of creating electronic tamper-proof currency. It is an often obfuscated fact that non-quantum physical systems only mimic randomness via chaotic properties (such as the number of wing flutters of a small group of humming birds) and their behavior may in fact be predicted with access to a suitably powerful computer and a careful enough analysis. On the other hand, certain physical properties of a quantum system are fundamentally inversely correlated, technically known as conjugate pairs, so that increasing the precision in acquiring information about one physical property, such as the momentum of an electron, decreases the precision with which information about the other property, such as the position of the electron, can be gained.

This feature of quantum physical systems is known as the Heisenberg uncertainty principle [3]. Wiesner's quantum money utilized the Heisenberg uncertainty system to ensure, in principle, that a counterfeiting attempt would always fail. This is made possible by assigning serial numbers to the electronic currency bills. The value of each digit in the serial number is generated by following a protocol to gain precise information about one physical property of a conjugate pair in a quantum system. This means that even if a counterfeiter knows what the protocol is, he still has to guess, with a (true) 50-50 chance, which one of the two physical properties in the conjugate pair was used to generate the digit's value in the serial number. If he attempts to learn the value of the digit, half the time he will learn the value with exact precision and half the time with no precision at all. It follows that the more often he guesses, the smaller his chance of guessing the entire serial number correctly becomes. In fact, even with a serial number of only 10 digits, the probability of counterfeiting a bill of quantum money is 0.00097, that is, 1 success out of every 1,024 attempts. For serial numbers of length 20, a successful outcome is once every 1,048,576 attempts, or 0.0095% of the time.

It is impossible to hack (by way of pattern recognition) this and other related tamper-proof quantum systems [4], and the best a would be counterfeiter can ever do to ascertain the value of a serial number is guess. Further, note that 99.9999% of the time, bankers will know that a counterfeiting attempt has been made! The security of quantum money can be further increased by replacing the protocol or the actual quantum physical system that generates the serial numbers frequently.

Unfortunately, while quantum money is tamper-proof in principle, engineering its implementation is fraught with challenges, though dramatic progress has been made in this area since the beginning of the 21st century. The most promising approach to implementing quantum money is via the quantum systems known as photons, or units of light (which are fundamentally also wave-like, as per the "weirdness" of quantum mechanics so talked about in media). Photons are already used in many electronic devices, especially smart phones. However, maintaining and manipulating their quantum physical properties essential to implementing quantum monetary protocols is not the main concern for the engineers of these devices. To this end, one needs to fine-tune the use of the photons with respect to the given practical constraints (such as the size of the smart phone or interference with its other functions). And this is where one gets to game the quantum.

Non-cooperative game theory [5] is a well-established field that has seen remarkable success in applications to different disciplines such as economics, politics, and evolutionary biology. Playing games as simple as tic-tac-toe or as complicated as poker or chess may appear to the uninitiated to be based on guess work or just luck. However, upon taking a closer look, all players taking part in a game, no matter how simple or complicated, exhibit a certain "rational" behavior. That is, the players look to maximize their payoffs, where the payoffs may simply be measured in monetary tokens, or more complex measures might be employed such as ideological satisfaction (a willing suicide bomber is completely rational when blowing himself up to achieve, as per his beliefs, instant salvation). Broadly speaking, games are categorized as zero-sum, which are strictly competitive in the sense that one player's "meat" is the other player's "poison", and non-zero-sum where players can benefit from a more relaxed notion of competition.

A standard example of a non-cooperative game and one of the most utilized in scientific literature is Prisoner's Dilemma, a non-zero-sum game. Initially transcribed by Merrill Flood and Melvin Dresher [6], this game demonstrates how rational behavior of the players can produce outcomes that are not the best possible ones for either of them. The narrative of the game is as follows: assume that there are two criminals, A and B, who get arrested on the same day at the same time, and have no opportunity to agree on a mutually beneficial alibi. The prosecutor offers A and B, separately, two options. The first option is to betray your partner, and if he doesn't betray you, then you are granted freedom. However, if he betrays you, then both of you spend 2 years in prison. The second option is to remain silent, and if your partner remains silent as well, both of you spend only one year in prison. However, if your partner betrays you, he will be able to walk free, and you will serve 3 years in prison. These options are summarized in Table 1, which demonstrates all possible payoffs for each player's actions as ordered pairs or numbers, with the first entry in a pair being the payoff to player A and the second being that to player B. In this game, each player wants to minimize the time he spends in prison with the best possible payoff being the one to walk away with no time in prison. But how likely is that to happen?

Table 1. Prisoner's Dilemma Payoffs

A | B	Silent	Betray
Silent	(-1, -1)	(-3, 0)
Betray	(0,-3)	(-2,-2)

Let's examine A's available strategies and find out the best course of action for him. If B stays silent, then A gets 1-year sentence if he stays silent as well. However, if A betrays, then he can walk free! Now let's assume B will betray. Then, if A stays silent, he gets a 3-year sentence. But if A betrays as well, then he gets 2 years, which is still a better outcome than a 3-year sentence. Thus, A concludes that he is better off betraying B in any case. If B follows a similar line of thinking, he will arrive at the same conclusion. Consequently, neither A nor B will unilaterally deviate from the decision to betray, a situation that in game theory is referred to as

Faisal Shah Khan

Faisal Shah Khan is an Assistant Professor of Mathematics and a principal investigator at the Center on Cyber-Physical Systems, Khalifa University. His research work is at the confluence of non-cooperative game theory and quantum information science, with special interest in optimizing quantum technologies under practical constraints.

Nour Abura'ed

Nour Abura'ed holds BSc degree in Computer Engineering and MSc degree that specializes in Quantum Image Processing. She is currently a research assistant at University of Dubai, interested in supervised deep learning, convolutional neural networks, object recognition, instance segmentation, quantum computing, and quantum games.

Nash equilibrium [4]. Hence, they both end up with a 2-year sentence. Of course, this is not the best option available to either player. It would have been ideal for B if A stayed silent and he betrayed A, and vice versa. Furthermore, if both of them remained silent, they would have gotten away with only 1-year sentences. All of these three options are referred to as being Pareto optimal [4], an outcome in a game deviating from which makes one player better but leaves at least one other player worse off. In game theory, a social optimum outcome is ideally desired, that is, an outcome that is both Pareto optimal and a Nash equilibrium. This is not the case in Prisoner's Dilemma. In fact, the only Nash equilibrium we see is the one that disagrees with all of the Pareto optimal outcomes. Hence the "dilemma".

Sometimes there is a natural way out of such dilemmas that has been employed since time immemorial: randomization. Including randomization into a game, via tossing of coins or rolling of dice, so long as the original game structure can be recovered when desired, is known as a game-extension. Not only does randomization allow possible resolution of dilemmas, it also guarantees that in the least, a Nash equilibrium will always exist in the extended mixed game [7]. This is the famous theorem of John Nash that earned him the Noble prize in economics. The importance of this theorem being evident when one imagines playing a game like Prisoner's Dilemma and permanently moving from outcome to outcome, much like the never ceasing warfare that marks the tribal culture from around the world. For Prisoner's Dilemma, it turns out to the case that the mixed version of the game does not solve the dilemma.

Once randomization links physical processes to the theory of non-cooperative games, one has the ability to apply game theory to any physical process so as to optimize it under constraints. The other point of view can be taken as well where one applies physics to the game at hand, that is, the game is implemented or played physically in the real world via a specific physical mechanism. While in most cases this distinction may be moot, there are cases, in particular when one considers the interplay between game theory and quantum physics, where delineating the two points of view can be crucial. For instance, for a given channel, there is a capacity limit to the amount of information that can be exchanged in a single transaction, and this limit is known as bandwidth. Each player (sender/receiver) needs to optimize the way the communication channel is utilized in order to guarantee maximum payoff. In this context, payoff refers to the amount of exchanged information. In computer security, there are further payoffs taken into account, such as the possibility of eavesdropping. This scenario can be modeled as a non-cooperative game, and it is not only applicable to classical communication, but also for communication channels processing information at the quantum level.

Let us return to the game Prisoner's dilemma. In 1999, Eisert et al. [8] presented a quantum physical implementation of this game and showed that the dilemma, while persisting in the mixed version of the game, vanishes in this quantum one. This is due to the fact that the randomization afforded by the strictly quantum realm is of a higher-order than that afforded by the "classical" physical realm. This remarkable feature is referred to as quantum entanglement, a physical characteristic that has no counterpart in the classical domain, and it allows to create correlations between quantum objects that are stronger and remain in place over cosmic time scales and distances. This means that two photons can be created in an entangled state on Earth and then one of them can be sent to Mars, but information gathered about the one on Earth instantaneously produces precise information about the photon on Mars. Aside from this dramatic property, quantum entanglement can clearly break dilemmas in non-cooperative games!

In addition to the dramatic feature of allowing players to break free of dilemmas, what are other benefits of gaming the quantum? Let us go back to the example of quantum money. While theoretically a perfect solution to the problem of tamper-proof currency, its practical implementation requires that the quantum physical system and the protocol used (to gain information about one of the conjugate pairs) should all perform optimally and therefore should interface with each other optimally under several natural constraints. A complete understanding of these constraints is possible in the form of Nash equilibrium or optimal outcomes in the game model for quantum money. Once achieved, stakeholders can choose the technology platform that comes closest to realizing these outcomes. From an investment in technology point of view, gaming the quantum is not an option but in fact, a necessity.

Finally, while much work has been done in gaming the quantum, or what has come to be known as the theory of quantum games [9] in the scientific literature, hard mathematical results in the spirit of Nash's work on the existence of equilibrium in games can be found in [10] for the case where randomization is utilized within a quantum system. For the case where purely quantum physical features are of interest, results pertaining to Nash equilibrium have only just appeared in [11]. Not only does much scientific work remain to be done in the theory on quantum games by up and coming scientific minds, but their applications to the emerging quantum technologies niche remains terra incognita.

References: **[1]** W. N. Goetzmann, K. Geert Rouwenhorst (1 August 2005). The Origins of Value: The Financial Innovations that Created Modern Capital Markets. Oxford University Press. p. 94. ISBN 978-0-19-517571-4. **[2]** S. Wiesner, Conjugate Coding, ACM SIGACT News - A special issue on cryptography, vol. 15, pp. 77–78, 1983. **[3]** Heisenberg, W. (1927), Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, Zeitschrift für Physik (in German), 43 (3–4): 172–198, Bibcode:1927ZPhy...43..172H. **[4]** B. P. Williams, K. A. Britt, and T. S. Humble, Tamper-Indicating Quantum Seal , Phys. Rev. Applied 5, 014001, 4 January 2016. **[5]** K. Binomre, Playing for Real, Oxford University Press; 1 edition, March 29, 2007. **[6]** Kuhn, Steven, Prisoner's Dilemma, The Stanford Encyclopedia of Philosophy (Spring 2017 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/spr2017/entries/prisoner-dilemma/>. **[7]** J. F. Nash, Equilibrium Points in n-Person Games, Proceedings of the National Academy of Sciences Jan 1950, 36 (1) 48-49; DOI:10.1073/pnas.36.1.48 **[8]** J. Eisert, M. Wilkens, M. Lewenstein, Quantum Games and Quantum Strategies Phys. Rev. Lett. 83 (1999) 3077–3080. **[9]** F. S. Khan, N. Solmeyer, R. Balu, T. S. Humble, Quantum Games: A Review of the History, Current State, and Interpretation, Quantum Information Processing (2018) 17: 309. https://doi.org/10.1007/s11128-018-2082-8. **[10]** D. A. Meyer, Quantum Strategies, Phys. Rev. Lett. 82, 1052 – Published 1 February 1999. **[11]** F. S. Khan, T. S. Humble, Nash Embedding and Equilibrium in Pure Quantum States, to appear in Springer Lecture Notes on Computer Science as Proceedings of the first Quantum Technology and Optimization Problems conference, 2019.

Fotos: Privat

Protection of Quantum Data Communications

Prof. Michel Barbeau

Quantum data communication protocols are theoretically secure, aren't they? But wait, they involve classical bits. Quantum nodes use classical hardware and software. Quantum storage is sensitive to environmental disturbances, that may have malicious origins. These reasons are good enough to motive the need to protect quantum data communications, in particular when quantum data disclosure or loss of integrity may have high impact on their owner. How can quantum data be protected during communications? This article examines this question and outlines some of the current answers.

Quantum data protection is an emerging area that has been a subject of recent attention by researchers. In this article, two key aspects are discussed in details: integrity and confidentiality. Authentication protects quantum data integrity, i.e., alteration by an adversary. Cryptographic techniques protect the confidentiality of information represented in quantum data from non-authorized access. We review the principal features of quantum cryptographic schemes that have been created to achieve authentication and confidentiality of quantum data. We discuss how they can be applied to protect quantum data communications and networking. Firstly, we introduce key quantum information concepts.

Quantum state

In the quantum information model, the unit of information is called the quantum bit, or qubit. In contrast to a classical bit, a qubit can be simultaneously in states zero and one. In fact, a qubit is in a superposition of states zero and one. This superposition condition can be interpreted as the association of a probability p of reading a qubit into value zero, and 1-p of reading it into a one (Fig. 1).

Probability	Reading outcome
p	0
$1-p$	1

Figure 1: A single qubit.

A qubit is in the zero-one superposition condition until it is read, which outcome is a zero or a one. In contrast to a classical bit that can be read several times, a qubit can be read only once. Reading is destructive. Furthermore, it is impossible to make a perfect copy of a qubit.

Qubits are interesting because they can be composed together to build complex quantum states. They can also interact together and be entangled. They can represent problems that involve an enormous amount of combinations in a very compact way, at least conceptually. This capability is exploited by the Shor's quantum algorithm for efficient integer factorization. A quantum state is a composition of n qubits. There are 2^n possible reading outcomes with respective probabilities $p_0, \ldots, p_{2^n-1}$ (Fig. 2).

Probability	Reading outcome
p_0	0
p_1	1
$\vdots$	$\vdots$
p_{2^n-1}	2^n-1

Figure 2: A quantum state made of n qubits (each reading outcome is interpreted as the numerical value represented by n bits).

As for a single qubit, a quantum state can be read only once. Reading is destructive. In addition, it is impossible to make a perfect copy of a quantum state.

Quantum entanglement

Qubits may be entangled, that is, related together such that they read in a coherent way. This means that some of the reading outcomes are made more probable than others. Besides, some reading outcomes can be made entirely non-probable. Entanglement is a key property of quantum distributed computing, communications and networking because the phenomenon works across distances. That is, two entangled qubits may be physically separated by an arbitrary long distance. However, despite their physical separation, the two individual qubits behave as if they were a single entity. The measurement of one qubit determines the outcome of the measurement of the other qubit.

Quantum transformation

Probability	Reading outcome
p_0	0
p_1	1
$\vdots$	$\vdots$
p_{2^n-1}	2^n-1

→

Probability	Reading outcome
p'_0	0
p'_1	1
$\vdots$	$\vdots$
p'_{2^n-1}	2^n-1

Figure 3: A quantum transformation on a n qubit state.

In the quantum world, computing takes the form of transformations of quantum states. The art of quantum programming consists of translating an idea into the right transformation(s). A transformation can be on a single qubit or on a whole quantum state. Not any transformation is permitted, which makes quantum programming a bit tricky. A transformation is valid solely if it reassigns new probabilities $p'_0, \ldots, p'_{2^n-1}$ to the reading outcomes of the quantum state (Fig. 3).

Quantum communications and networking

Quantum data communications and networking aim at supporting applications that need the transfer of quantum states from one network node to another, e.g., for the purpose of distributed quantum computing. It is foreseen that quantum teleportation and quantum repeaters will play key roles in future quantum networks.

Quantum teleportation. Teleportation is a point-to-point protocol devised to transfer a qubit from one location to another, i.e., a source and a destination. It builds upon pre-shared entanglement between the source and destination. It is assumed that they have the capability of long-term storage of pre-shared entangled qubits. The entangled qubits can be obtained at network setup time. The parties must also be able to exchange classical bits. The transfer of every qubit requires the transfer of two classical bits.

Quantum repeater. For quantum networking, the use of quantum repeaters is envisioned for the end-to-end transfer of quantum states. Quantum repeaters leverage entanglement swapping, possibly together with error correction, to achieve multi-hop communications. Using pre-established node-to-node entanglement, entanglement swapping establishes an entangled qubit between a source and a destination. This end-to-end entanglement is used to transfer a qubit from the source to the destination. Entanglement swapping is conceptually similar to teleportation. The swap of every qubit requires the transmission of two classical bits. A coordination protocol between participating nodes is also required. On a multi-hop network, routing of a quantum state requires several swaps and classical bit transmissions.

Need for quantum data protection

When alteration and disclosure have impact, integrity and confidentiality of quantum data need to be protected. Quantum computing, communications and networking use classical hardware and software. Classical hardware and software can be compromised. Hence, quantum hardware and software are vulnerable to all classical attacks. They may lead to disclosure of quantum data. An attack can disturb quantum states in a random way. The state loses its authenticity. Teleportation of quantum states and quantum repeaters use classical qubit communications to implement their logic. When they are attacked, teleported or swapped qubits may lose their integrity. Quantum data protection builds upon the science of quantum cryptography.

Quantum data integrity protection

Authentication is a data integrity protection mechanism. Authentication aims at demonstrating that quantum data has not been altered by an adversary during the transit between a source and a destination. Authentication is achieved using a data signature mechanism.

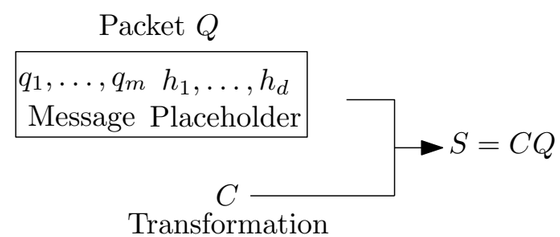


Figure 4: Sender procedure of quantum data authentication.

The quantum authentication procedure is based on a shared secret. The sender-side authentication procedure is schematically outlined in Fig. 4. A quantum packet Q comprises a m-qubit message $q_1, \ldots, q_m$ and a placeholder for a quantum signature made of d qubits $h_1, \ldots, h_d$. The number d is a security parameter. The larger the better. The shared secret is a quantum operator C used to transform the packet Q into a quantum state S. The transformation, $S=CQ$, computes the quantum signature and loads it into the placeholder.

There are important aspects to highlight. The transformation C is chosen with key mathematical properties. It has an inverse transformation $C^{\dagger}$. That means that when S is integrally forwarded to the destination, the application of $C^{\dagger}$ to the received content restores the original quantum state. An attack to the integrity of a quantum state translates to the application of some quantum transformation P. The transformation C is selected such that P is mapped to a transformation that has an effect on the qubits in the signature. Hence, the attack is detectable.

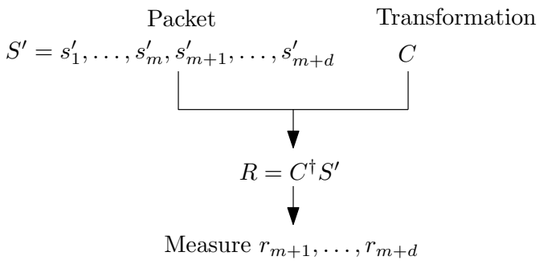


Figure 5: Receiver procedure of quantum data authentication.

The quantum packet S is forwarded to the destination, using teleportation or a network of quantum repeaters. There is a risk that the quantum packet is altered by an adversary because quantum communications and networking require as well the transmission of auxiliary classical bits and classical control software, such as operating systems. At the destination, the receiver gets a quantum S' that may or may not correspond to S. When the quantum state has not been altered, S' is equal to S. This is verified by an inspection of the signature. Fig. 5, the receiver gets a quantum packet S' consisting of a $m+d$-qubit state $s'_1, \ldots, s'_m, s'_{m+1}, \ldots, s'_{m+d}$. It applies to S' the inverse transformation $C^{\dagger}$ to obtain the quantum state R, i.e., R is equal to $C^{\dagger} S'$. The d rightmost qubits of R are $r_{m+1}, \ldots, r_{m+d}$. Measurement of qubits $r_{m+1}, \ldots, r_{m+d}$ should yield d zeros. The original quantum message $q_1, \ldots, q_m$ is in qubits $r_1, \ldots, r_m$. Otherwise, the quantum authentication procedure failed and the message has been compromised and should be rejected.

Quantum data confidentiality protection

The goal of confidentiality is to insure the secrecy of data during the transport from a source to a destination. Confidentiality is achieved by encrypting data. Quantum cryptographers have developed encryption techniques specifically for quantum data that may be used to protect the confidentiality of information during communication and transit over a network. There are two forms of encryption: asymmetric and symmetric. We discuss the symmetric form first.

Symmetric quantum data encryption

Symmetric encryption means that the sender and receiver share a common secret key. The symmetric encryption procedure is based on a shared n-bit classical key k and a one-way hash function f. An output of f does not reveal any information about its input. The hash function takes as arguments the key k and a random index i. It returns a value used as an index to select a transformation. The value i plays the role of initialization vector. A repeated usage of key k does not allow an adversary to infer a relationship between encrypted messages. The symmetric key k is a secret shared by the sender and receiver.

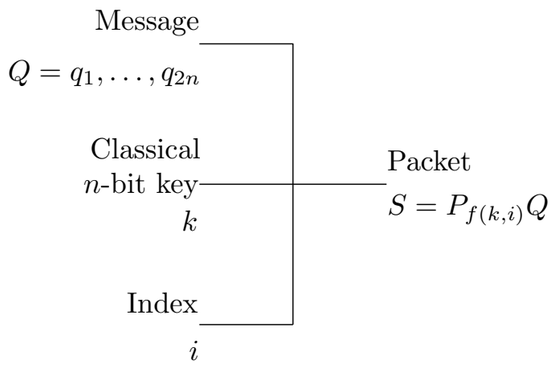


Figure 6: Symmetric quantum data encryption by the sender.

Fig. 6 pictures the encryption procedure performed by the sender. The sender has a message consisting of $2n$ qubits $q_1, \ldots, q_{2n}$. Given key k and index i, the result of the evaluation of the hash function $f(k,i)$ is used as an index to determine a quantum transformation $P_{f(k,i)}$. The source computes S equal to the product $P_{f(k,i)}\, Q$ and sends S and i.

In this scheme, when an adversary succeeds reading the quantum state S, before it reaches its destination, information is concealed due to the presence of transformation $P_{f(k,i)}$. The adversary may try to guess what $f(k,i)$ is. In contrast to classical cryptanalysis, due to the fact that quantum state reading is destructive and the impossibility to copy, the adversary has only one trial. Hence, a brute-force attack cannot be perpetrated directly on the quantum state representation. The transformation $P_{f(k,i)}$ is chosen such that it has the self-inverse property. Assuming that S and i are correctly delivered to the final destination, a second application of transformation $P_{f(k,i)}$ to S restores the initial state Q.

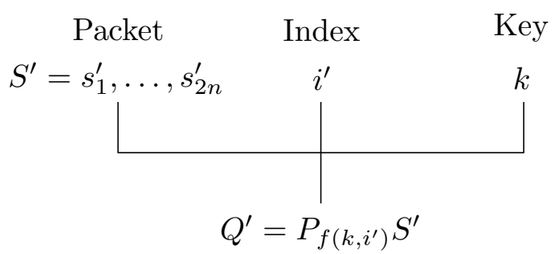


Figure 7: Symmetric quantum data decryption by the receiver.

Fig. 7 pictures how cipher text is decrypted. The destination owns the secret key k and receives a quantum state S' consisting of the qubits $s'_1, \ldots, s'_{2n}$ and index i'. Let $P_{f(k,i')}$ be the transformation determined by the index $f(k,i')$. To obtain the plain text, the transformation $P_{f(k,i')}$ is applied to S', that is, the received plaintext Q' is equal to $P_{f(k,i')}\, S$'.

Asymmetric quantum data encryption

Asymmetric encryption means that the sender uses a public encryption key and the receiver uses the corresponding private decryption key. The asymmetric key encryption procedure uses a n-bit classical public key i. The public key determines an indexed permutation function f_i. The indexed function f_i is chosen such that it has the one-way and trapdoor properties. The latter means that, given an output $f_i(x)$ and a trapdoor value t, the input x can be determined easily. Using function f_i, a function h that has the hard-core property is constructed to generate pseudo-random values. The value returned by an invocation of function h is used to determine the index of a transformation. The hardcore property means that given the result of $f_i(x)$, it is difficult to determine $h(x)$. The trapdoor value t plays the role of private key. It is used to resolve the inverse permutation of $f_i(x)$, denoted by $g_i(x)$.

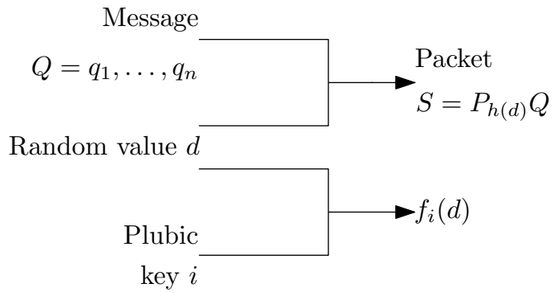


Figure 8: Asymmetric quantum data encryption by the sender.

Asymmetric key quantum data encryption is outlined in Fig. 7. Let Q be a quantum state representing a message consisting of the n qubits $q_1, \ldots, q_n$. A value d is selected at random such that $f_i(d)$ is not null. The hardcore of d, i.e., $h(d)$ is used as an index to determine a transformation $P_{h(d)}$. The source sends the quantum state S equal to the product $P_{h(d)}\, Q$ together with the hash value $f_i(d)$.

We have conditions similar to quantum symmetric encryption, but not exactly the same. When an adversary succeeds reading the quantum state S before it reaches its destination, information is concealed due to the presence of transformation $P_{h(d)}$. Using the hash value $f_i(d)$, the adversary may try to guess what the random value d is and calculate the hard-core value $h(d)$, perpetrating a brute-force attack, i.e., a search for the trapdoor value t. Because it is single read and impossible to copy, a chosen transformation $P_{h(d)}$ can be tried only once on a quantum state. The transformation $P_{h(d)}$ is chosen such that it has the self-inverse property. Assuming that S and $f_i(d)$ are correctly delivered to the final destination, a second application of transformation $P_{h(d)}$ to S restores the initial state Q.

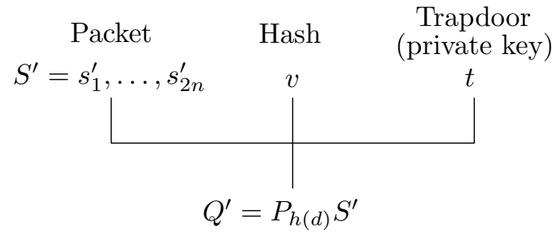


Figure 9: Asymmetric quantum data decryption by the receiver.

The decryption procedure uses a n-bit classical private key, i.e., the trapdoor value t (Fig. 9). The destination receives a quantum state S' made of $2n$ qubits $s'_1, \ldots, s'_{2n}$, representing an encrypted message, and a hash value v. Using the trapdoor value t, the inverse permutation function g_i of function f_i is used to determine d equal to $g_i(v)$ and calculate the hardcore $h(d)$. The receiver applies the transformation $P_{h(d)}$ to S' to obtain the n-qubit plain text quantum state Q'.

Further readings

Quantum data communication protection and encryption are relatively news topics. The goal of this article was to demonstrate their relevance and outline some of the main ideas developed by researchers. Visit the web page of the author for more readings and relevant reference material (carleton.ca/scs/people/michel-barbeau).

Michel Barbeau

Michel Barbeau is a professor of Computer Science. He got a Bachelor (Université de Sherbrooke, Canada '85), a Master's and a PhD in Computer Science (Université de Montreal, Canada '87 & '91). From '91 to '99, he was a professor at Université de Sherbrooke. During the '98-'99 academic year, he was a visiting researcher at the University of Aizu, Japan. Since 2000, he works at Carleton University, School of Computer Science, Canada. His current research interests are wide area ad hoc networks, underwater communications and networks, quantum communications and networks, and cyber-physical systems security.

Fotos: Privat

Quantum Computing. Applied Now.

Starting the Quantum Incubation Journey with Business Experiments

Matthias Ziegler, Tim Leonhardt

Recent developments in quantum hardware for optimization and general purpose quantum computing prototypes as well as application software have propelled quantum computing from a theoretical concept into a tangible computing option for enterprises – one with the potential to deliver business value by solving difficult subsets of problems based on a fundamentally different set of rules.

This year on January 8th 2019 IBM announced the first commercially available universal quantum computer on-premise solution housing 20 qubits[1]. This provides a major step in releasing complex prototype systems, which use chambers as cold as outer space, microwave frequency control electronics and high-tech nano-fabricated chips from their flat-size laboratories, which require extensively trained physicists for maintenance and operation, towards an on-premise solution in your data center. Specific hardware for optimization purposes known as quantum annealers have been announced already in 2011 by D-Wave Systems and reached 2000 qubits today.

At the current stage the gate quantum computer solutions with high quality qubit operations do not provide the capability of solving practical problems but yield the potential of surpassing supercomputers in processing power for a class of sampling problems, that describe the outcomes of random processes in nature. Reaching this milestone is an important step in this era of noisy intermediate scale quantum computation, which is characterized by having access to a few dozen to hundred qubits running hundreds to thousands of operations without errors. This sets the stage for finding approximate solutions to a variety of hard problems. This process is driven by initiatives of global companies and scientific institutes like Google and NASA[2]. Quantum annealers on the other hand trade-off a larger number of qubits at the cost of lower operation quality and a more granular control of the system parameters to solve intermediate scale instances of a specific problem class (so called quadratic binary optimization problems or QUBO) with hundreds to thousands of variables.

These developments raise vast discussions contrasting enormous theoretical potential with uncertainties in predictions of the developments in technology maturity. It is imperative to prepare for different possible outcomes of this Hilbert-space race[1].

The first step towards a quantum strategy is a sound introduction to the capabilities, potential advantages and tools in quantum computing. The next step is the identification of business areas, where quantum could yield a business advantage and the assignment of an employee to monitor the trends reporting monthly to hold up with the developments in the field. The quantum potential may only be leveraged, when there is expertise in understanding the structure of the problems that limit business activities in the identified areas and finding quantum approaches that could tackle those limits. Only after this ideation and analysis endeavors the next step of running business experiments enables to build know how in quantum application development and supports predictions on the impact of future hardware developments by using quantum simulators or typical cloud access solutions. With these experiences the strategic roadmap can be funneled into a more specific timeline for how the use cases scale with quantum computing improvements and selecting the most promising.

A large ecosystem has already formed to support this incubation journey in providing hard- and software for quantum computing applications. Quantum computer mainframe providers typically provide an interface including instructions sets that define qubit specific electrical control signals and higher-level programming languages that accumulate operations on qubit registers to subroutines (e.g. addition circuits) as well as high level optimization algorithms like solvers for QUBO problems, while giving cloud access to the quantum hardware backend via web protocols. At the highest level modern web frontends allow for an intuitive user interface that enables the usage by end users without the necessity of understanding the underlying rules of quantum mechanics or programming.

A survey[3] of more than 5,400 business and IT executives established that 40 percent of respondents are taking proactive steps to prepare for quantum computing, with 36 percent planning to invest in quantum capabilities in the next two years.

In several fields first proof of concept applications emerge from a sea of use case ideas, that point out promising directions driven by partnership initiatives between business-end-users, hard- and software-providers as well as research institutes. In this article we will focus on the financial services, life sciences and supply chain applications.

Financial services

"Banks and financial institutions like hedge funds now appear to be mostly interested in quantum computing to help minimize risk and maximize gains from dynamic portfolios of instruments," said Dr. Bob Sutor, vice president, IBM Q Strategy and Ecosystem. "The most advanced organizations are looking at how early development of proprietary mixed classical-quantum algorithms will provide competitive advantage."

Choosing assets from a portfolio of 60 assets already yields a higher number of options than there are atoms in the known universe. Significant competitive advantages could be achieved if the value of those portfolios could be efficiently calculated and the best combination of assets identified. Algorithm concepts exist that predict advantages for portfolio valuation and optimization yielding a competitive advantage, when a larger amount of possible next-day scenarios can be covered to yield precise predictions or intra-day valuations finish before the competitor establishes his numbers. As one example IBM provides software development kits to build algorithms on the quantum register level and functions for the valuation of a series of payments. First movers as the Royal Bank of Scotland, Goldman Sachs, and Citigroup have funded quantum computing startups directly. Barclays and JPMorgan Chase have been experimenting with IBM's quantum computing technology and joined the IBM Q Network. Morgan Stanley articulated the bank's hope of speeding up portfolio optimizations like Monte Carlo simulations with the help of quantum computing.

Life sciences

"At Biogen, we're always looking to harness cutting-edge technologies that push the boundaries of traditional pharmaceutical research to discover new treatments and cures for complex neuroinflammatory and neurodegenerative conditions," said Govinda Bhisetti, Head of Computational Chemistry, Biogen. "Collaborating with researchers at Accenture Labs and 1QBit made it possible to rapidly pilot and deploy a quantum-enabled application that has the potential to enable us to bring medicines to people faster."

The idea to build a quantum computer coined by Richard Feynman originally resides on the pain that physicists had with efficiently simulating quantum systems. A prime example is the prediction of material properties be it a slice of silicon or a molecule. Pharma companies invest billions for trials, which would be drastically reduced if one could predict the chemical properties in advance and estimate the influence on the human physiology. As a leading biotech company, Biogen is seeking to advance the development of new drugs for neurological and neurodegenerative diseases. With the price reductions chances would increase to find a live saving drug. Biogen has teamed up with Accenture Labs and 1QBit, a quantum software startup, to speed up the discovery of new drugs. The quantum molecular similarity method is a repeatable solution which can be further customized to a specific client's need. Amgen, a biopharmaceutical company, is using

Matthias Ziegler

Matthias Ziegler leads Accenture's Emerging & Growth group in Austria, Switzerland, Germany and Russia which helps bring emerging technologies to the business world. Current focus areas include Artificial Intelligence, Blockchain, Extended Reality, Application Security and Quantum Computing. He graduated in Computer Science at the University of Würzburg and completed his PhD at the Technical University of Munich in Geographical Databases.

Tim Leonhardt

Tim Leonhardt works as Quantum Computing Lead for Accenture within the Emerging & Growth group to identify and consult on go-to-market strategies and deliver quantum computing applications. Previous to his time at Accenture, he gained 5 years of experience in silicon gate quantum computing as research assistant and educator. He holds a double major in physics (M.Sc.) and economics, business and management (M.Sc.) from RWTH Aachen.

quantum computers for molecular simulations. IBM has recently shown the potential of quantum-based computational chemistry with the simulation of a BeH_2 molecule (beryllium hydride)[4] paving the way for simulations of more complex molecules that could help in reducing energy consumption by discovering new catalysts for fertilizer production (3% of the world energy consumption).

Supply chain

The ultimate goal of a driverless supply chain, where all aspects of end-to-end activities – planning, sourcing, production, logistics, services, and the ability to respond to risks with rapid replanning – are optimized for a single global objective across an organization frees disruptive potential to shift the automotive industry further towards mobility services and drives innovation initiatives: The Volkswagen Group is the world's first automaker which publicly used quantum computers, further expanding its digital competence for the future. In this context, Volkswagen Group IT is cooperating successfully with leading quantum computing company D-Wave Systems on a research project for traffic flow optimization[5].

VW CIO Martin Hofmann said in a recent interview with automotiveIT that quantum computers have "reached a stage where it becomes interesting to start developing use cases." He cited one project involving publicly available data from Beijing taxis that were used to plot optimal routes. "We were trying to prove that a particular traffic optimization problem could be addressed with a quantum computer," he said.

These are a few examples on building quantum-ready applications, which show how businesses can start innovating now by accessing existing commercial quantum computing capabilities through newly available quantum hardware platforms and software applications by leveraging teams with industry experts, advanced analytics and quantum computing specialists. Several more industry prototypes will be presented at IBM Think (February 12th–15th). In tight cooperation this low fidelity proof of concepts can be established on the time-scale of weeks to months limiting the investment and yielding insights on the execution of further quantum programs. Companies that join these first movers and start their quantum computing incubation journey now will be best positioned when the emerging technology reaches maturity.

[1] The mathematical description of quantum computers relies on matrices with entries that include real and imaginary numbers together with operations like multiplication, which transform these mathematical objects. It defines a concept known as Hilbert space within the physics and mathematics community

References: [1] https://www.hpcwire.com/2019/01/10/ibm-quantum-update-q-system-one-launch-new-collaborators-and-qc-center-plans/ [2] https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/ [3] Accenture Technology Vision 2017 [4] https://arxiv.org/pdf/1704.05018.pdf [5] https://guce.oath.com/collectConsent?brandType=nonEu&.done=https%3A%2F%2Fwww.engadget.com%2F2018%2F11%2F05%2Fvolkswagen-quantum-computer-traffic-management%2F%3F-guccounter%3D1&sessionId=3_cc-session_86232dcc-f07a-450e-ab74-b7e451dbb972&lang=en-US&inline=false

Fotos: Privat

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

Führung im Wandel – Augenhöhe statt Unterordnung

Im Übergang vom Industriezeitalter in das Zeitalter der Wissensarbeit ändert sich auch und gerade das Verhältnis von Mitarbeitern zur Organisation grundlegend. Aus abhängigen Arbeitern werden zunehmend unabhängige Wissensarbeiter, die ihre Produktionsmittel in ihrem Kopf tragen. Die Organisation ist deshalb mehr auf die Wissensarbeiter angewiesen als umgekehrt die Wissensarbeiter auf die Organisation. Das Netzwerk löst in diesem Übergang die Hierarchie als führendes Organisationsprinzip ab. Und Führung basiert nicht länger auf Unterordnung und Gehorsam, sondern muss die Selbstführung der ihr anvertrauten Menschen zum Ziel haben.

Lange und vielleicht zu lange zielte Führung auf Gehorsam ab. Kinder wurden (und werden leider immer noch) schon im Elternhaus und spätestens in der Schule zur Einordnung in die Gesellschaft und ihre Organisationen erzogen. Und diese Einordnung bedeutete und bedeutet im Kern Unterordnung. Die undurchlässige ständische Ordnung des Mittelalters gehört glücklicherweise der Vergangenheit an, aber das Organisationsprinzip der Hierarchie blieb gerade durch die mit der Aufklärung einhergehende Möglichkeit des eigenen Aufstiegs grundsätzlich erhalten. Ohne hierarchische Ordnung kein Aufstieg. Im Zuge der Industrialisierung mit ihren großen Konzernstrukturen erlebte dieses Prinzip sogar eine deutliche Ausweitung und Differenzierung. Die Hierarchie war und ist das bestimmende Organisationsprinzip des Industriezeitalters.

Bereits 1959 prägte Peter F. Drucker den Begriff des Wissensarbeiters, dessen Arbeit im Wesentlichen im Erdenken und Erschaffen von Neuem besteht. Dazu arbeiten Wissensarbeiter mit ihrem Wissen und erzeugen dabei neue Erkenntnisse und neues Wissen. Diese Arbeiter tragen ihre Produktionsmittel in ihrem Kopf. Deshalb ist die Organisation mehr auf sie angewiesen als umgekehrt die Wissensarbeiter auf die Organisation. Zu Zeiten von Frederick Winslow Taylor waren die Arbeiter ungelernte Arbeitskräfte und der Manager der Experte, der ihre Arbeitskraft möglichst produktiv einsetzte. Die heutigen Wissensarbeiter sind nun aber selbst die Experten und sie erwarten zu Recht eine „artgerechte" Führung auf Augenhöhe.

Das Verhältnis von Führungskraft und Wissensarbeiter ähnelt eher dem zwischen Dirigent und Musiker in einem Orchester. Nicht nur hinsichtlich der unterschiedlichen Fähigkeiten, denn sowohl der Dirigent als auch die Musiker sind Experten ihrer Domäne, sondern auch hinsichtlich der Macht- und Abhängigkeitsverhältnisse: Die Machtposition von Wissensarbeitern gegenüber ihrer Führungskraft ist eine völlig andere als die des prinzipiell leicht austauschbaren Arbeiters zu seinem Chef in tayloristischen Strukturen. Ein Wissensarbeiter kann seinen Vorgesetzten ebenso leicht und effektiv sabotieren wie ein Musiker einen autokratischen Dirigenten.

Zwar hat sich das Verhältnis von Führungskraft und Mitarbeiter in den letzten Jahrzehnten schon deutlich zum Positiven verändert. Viele Führungskräfte haben mittlerweile eine eher elterliche und fürsorgliche Haltung zu ihren Mitarbeitern eingenommen. Die Richtung stimmt also, aber das Abhängigkeitsverhältnis wurde nicht angetastet. Die Mitarbeiter bleiben abhängig von ihrem paternalistischen Chef. Und während Kinder in verschiedenen Phasen mehr oder weniger vehement ihre Selbstständigkeit und Gleichwürdigkeit einfordern und erkämpfen, bleiben diese Mitarbeiter für immer überbehütete Kinder.

Dem Prinzip der Hierarchie im Industriezeitalter folgt nun das Prinzip des Netzwerks im Wissenszeitalter. Führung basiert nicht länger auf Unterordnung und Gehorsam, sondern zielt auf die Selbstführung der ihr anvertrauten Menschen. Führung gibt der Wissensarbeit und den Wissensarbeitern Orientierung. Führung auf Augenhöhe jenseits von Unterordnung und Gehorsam ist deshalb notwendiger denn je. Der Schachmeister aber hat ausgedient, gefragt ist heute der Gärtner. Gute Führung schafft einen Rahmen, in dem sich die Menschen und ihre Ideen im Sinne eines gemeinsamen Zwecks entfalten können.

Dr. Marcus Raitner

Foto: Privat

1. CYBER SECURITY

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

Cyber Security ist ein so kompliziertes und eben auch interessantes Thema, weil es auf so vielen unterschiedlichen Ebenen behandelt werden kann. So ist Cyber Security selbstverständlich technischer Natur, aber ebenso hat es eine organisatorische Dimension: Nur wenn eine Maßnahme auch wirklich in einen Prozess integriert werden kann, wird diese verwendet. Darüber hinaus gibt es eine politische Ebene („wessen“

Datenschutzgesetze werden beispielsweise beim Surfen im Internet angewendet) und eben auch eine menschlich-soziale: Der Anwender muss die Maßnahmen wollen, keine Berührungsängste haben und sie insbesondere auch verstehen.

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

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

MEIST GEKLICKT – Unsere erfolgreichsten Blog-Beiträge

Unsere Beiträge wurden insgesamt **430.000 Mal** geklickt*

Beiträge zum Thema **CYBER SECURITY** erhielten **90.000** Klicks.

	Autor	Thema
#1	**Werner Thalmeier**	Schutz der Marke sorgt für Sicherheit der Kunden und Mitarbeiter **Seite 64**
#2	**Amy Baker**	Millennials und die Cyberrisiken **Seite 71**
#3	**Frank Limberger**	Der Mensch im Mittelpunkt – wie etabliert man ein Insider-Threat-System? **Seite 56**
#4	**Karl-Otto Feger**	Hacker in der „Honigfalle“ **Seite 65**
#5	**Dirk Rosenau**	Kryptografische Verfahren bei Frankiermaschinen **Seite 66**

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 04. Februar 2019.**

INHALT

1.1 ALLGEMEIN

Steve Wainwright, Managing Director EMEA, Skillsoft Gruppe

Unternehmenssicherheit muss in die Köpfe der Mitarbeiter

Obwohl Unternehmen verstärkt in IT- und Datenschutz investieren, bleibt der Erfolg häufig aus, weil viele Belegschaften weder potenzielle Gefahren noch die gravierenden Folgen (er)kennen. Können digitale Lernkurse das Sicherheitsbewusstsein bei Mitarbeitern nachhaltig verbessern?

Mit der rasanten Verbreitung digitaler, Cloud-basierter und mobiler Anwendungen im Unternehmen steigen die Risiken für IT-Sicherheit und Datenschutz erheblich. Die Ursachen hierfür sind allerdings weniger technisch bedingt. Denn der größte Risikofaktor ist nicht der Computer, sondern sitzt davor! Ein im Zug vergessenes Smartphone, das im Konferenzraum unbeaufsichtigte Laptop, die Weitergabe von Kundendaten, unbedachtes Öffnen eines eMail-Anhangs oder das vertrauensselige Überlassen persönlicher Zugangsdaten an einen Kollegen können weitreichende Konsequenzen haben.

Wie diese Beispiele zeigen, liegt beim Verursachen von Compliance- und IT Sicherheitsverletzungen meist noch nicht einmal böse Absicht vor: Einer aktuellen Studie des Branchenverbands BITKOM e.V. zufolge sind über 80% deutscher Arbeitnehmer nach eigenen Angaben schlicht „not ready“ für die digitale Transformation. Entsprechend gering ausgeprägt ist das Verständnis für die im Zuge der Digitalisierung deutlich gestiegenen Anforderungen an IT-, Daten- und Unternehmenssicherheit.

Schwaches Sicherheitsbewusstsein, wenig Verantwortung

Auch die beste Security-Strategie und der engagierteste Datenschutzbeauftragte sind gegen die Risikofaktoren „Unwissenheit“ und „Arglosigkeit“ machtlos. Es ist daher umso essenzieller, die gesamte Mitarbeiterbasis für die Brisanz dieser durchaus komplexen Themen zu sensibilisieren und sie viel stärker als bisher in regelkonforme Umsetzungsprozesse einzubinden.

Dies ist jedoch leichter gesagt als getan. Zwar führen Unternehmen mittlerweile Compliance- und IT-Sicherheitstrainings verstärkt über digitale Lernformen durch, um im Vergleich zu den sogenannten Präsenzschulungen mehr Mitarbeiter in kürzerer Zeit und zu geringeren Kosten zu schulen. Der Erfolg bleibt jedoch mäßig: viele eLearning-Programme erweisen sich als ungeeignet, um in der Belegschaft ein nachhaltiges Sicherheits-Bewusstsein zu generieren.

Dafür gibt es zwei Ursachen: zum einen werden Schulungsinhalte zu Sicherheitsthemen häufig als trockene, rechtlich verklausulierte Theorie und wenig praxisorientiert empfunden. Zum anderen mangelt es auf breiter Ebene an Verständnis und Einsicht: So hielten laut der erwähnten BITKOM-Studie 62 Prozent der Arbeitnehmer das Thema Datenschutz im Internet für nicht relevant. Das Grundlagenwissen für Firewalls und IT Security-Programme wurde gar von 66 Prozent der Befragten als unwichtig für den eigenen Job abgetan. Die weit verbreitete Ansicht „Warum soll ich auf IT-Sicherheit achten? – Dafür gibt es doch die IT-Abteilung!“ belegt, dass Mitarbeiter weder die globale Bedeutung von Unternehmenssicherheit noch die thematische Relevanz für ihren eigenen Arbeitsbereich oder ihr privates Umfeld erfasst haben.

Lernen mit Erfolg – darauf kommt es an!

Aktuelle Ergebnisse der modernen Hirnforschung zeigen, dass im Bereich der Erwachsenenbildung insbesondere drei Faktoren adressiert werden müssen, um eine optimale Lernerfahrung zu erzielen: Bedeutung, Relevanz und Emotion. Genau hier müssen eLearning-Programme ansetzen und diese Schlüsselbegriffe mit ‚Leben‘ füllen: Lernkurse müssen Mitarbeiter in die Lage versetzen, die Wichtigkeit von Sicherheitsthemen für das Unternehmen (und für sich selbst) zu erkennen, um ein Verständnis für den bewussten Umgang mit IT, Kommunikation und sensiblen Daten zu entwickeln.

Die emotionale Ansprache spielt dabei eine maßgebliche Rolle im Hinblick auf Lernmotivation, Sensibilisierung und nicht zuletzt eine nachhaltige Veränderung des Handelns. Die Verknüpfung der Aspekte „kognitives Lernen“ und „emotionales Erleben“ kann das Lernverhalten nachhaltig verbessern.

Praxisnahe, attraktive Inhalte:

Compliance-Kursprogramme sollten neben IT- & Datensicherheit natürlich auch die Themenfelder Recht, Arbeitssicherheit, Gesundheit und Umwelt umfassen. Um Kontinuität zu gewährleisten, müssen verschiedene Wissens-Aufbaustufen abgedeckt werden – vom Anfänger über den fortgeschrittenen Lerner bis zum Expertentraining als Vorbereitung auf eine Industriezertifizierung. Zusätzlich sollten sämtliche Lerninhalte kontinuierlich vom Content-Anbieter aktualisiert werden. Wie „up-to-date“ ein Kursprogramm tatsächlich ist, zeigt sich daran, dass auch verhältnismäßig neue Inhalte, zum Beispiel die EU-DSGVO 2018, aktuelle Cyber-Bedrohungen oder Themen wie Mobbing-Prävention, zu finden sind. Eine gut sortierte Compliance eLearning-Bibliothek umfasst gut und gerne mehrere tausend Kurse und Videos zu allen Rechts- und Sicherheitsthemen.

Die von renommierten Anwaltskanzleien und spezialisierten Partnern entwickelten Inhalte werden mithilfe erstklassiger Schriftsteller, Animationszeichner, Schauspieler und Moderatoren ansprechend präsentiert. Dabei bestehen die Lernkurse aus einer Vielzahl kompakter Micro-Learning Videos. Diese „Lernhäppchen“ von 5- bis 10-minütiger Dauer stellen beispielsweise sicherheitskritische Szenen aus dem täglichen Arbeitsleben nach und geben Handlungsempfehlungen zur Risikovermeidung. Auch spielerische Elemente (auf neudeutsch: Gamification), zum Beispiel Scorer-Punktesysteme und Learning Contests, schaffen Anreize, um die Lernmotivation zu erhöhen.

Gezielte Ansprache:

Leistungsstarke Lernprogramme sind diversifiziert. Das heißt, sie berücksichtigen die Zielgruppenvielfalt im Unternehmen – Basispersonal, Führungskräfte, junge Talente, gestandene Mitarbeiter – und die damit verbundenen Lernbelange jedes Einzelnen. Auch die Lernmethoden Erwachsener sind völlig unterschiedlich: Der Eine bevorzugt das Anschauen von Videos, ein Anderer Lernspiele. eBooks erfreuen sich in einem multimodalen Lernportfolio ebenfalls einer ungebrochen hohen Beliebtheit.

International aufgestellte Unternehmen sollten zudem auf die Mehrsprachigkeit des Kursangebots achten. Sie gewährleistet nicht nur eine einheitliche Qualifizierung aller Mitarbeiter über die gesamte Organisation hinweg, sondern berücksichtigt auch kulturelle Unterschiede und landesspezifische Gesetze.

Freie Nutzung:

Im Gegensatz zu einem Trainer-geführten Seminar lassen sich kompakte Micro Learning-Einheiten ideal in den Arbeitsalltag integrieren. Darüber hinaus bieten moderne Lernsysteme die Möglichkeit, praktisch jederzeit, an jedem Ort und über jedes mobile Endgerät auf die Inhalte zuzugreifen. Diese Art „Weiterbildung to go“ wird mittlerweile von jedem zweiten Arbeitnehmer in Deutschland genutzt.

Trotz aller Leistungsstärke und Themenvielfalt sollten Lernmanagement-Systeme vor allem eines sein: intuitiv! In der digitalen Arbeitswelt muss jeder Mitarbeiter – ob 25 oder 52, Basis- oder Führungskraft – die gleichen Chancen auf Weiterbildung haben. Dabei sollten etwaige Berührungsängste mit Digitaltechnologie abgebaut werden, anstatt neue Barrieren aufzubauen.

Moderne Lernplattformen sind deshalb in Gestaltung und Funktionalität einer Social Media-Plattform sehr ähnlich. Sie liefern nicht nur individuell zugeschnittene Lernangebote, sondern ermöglichen auch, Wissen zu teilen, Feedbacks und den Austausch innerhalb der Learning Community. In den nächsten Jahren werden so genannte Lern-Agenten, die auf künstlicher Intelligenz basieren, die individuellen Lerngewohnheiten jedes Anwenders erkennen, maßgeschneiderte Lernangebote zusammenstellen und zunehmend in die Rolle individueller Digital-Coaches und Mentoren schlüpfen.

Gezielte Investition in Weiterbildung zahlt sich aus

Massive Kosteneinsparmaßnahmen und zunehmender Fachkräftemangel haben über Jahre das interne Sicherheits-Knowhow vieler Unternehmen deutlich schrumpfen lassen. Digitale Lernsysteme können die entstandene Lücke kompensieren. HR- und Sicherheitsverantwortliche sollten zunächst eine konsistente Weiterbildungsstrategie für Compliance entwickeln und auf dieser Grundlage auswählen, welches Technologie- und Lernangebot am besten zu den eigenen Anforderungen passt. Ein leistungsstarkes Learning Management System kann zu einem nachhaltigen Sicherheitsbewusstsein auf breiter Ebene führen, Sicherheitsrisiken deutlich eindämmen und nicht zuletzt den digitalen Wandel im Unternehmen enorm voranbringen.

Steve Wainwright

Pascal Cronauer, Country Manager DACH, LogPoint

SIEM und Machine Learning – Automatisierung braucht Spezialisten für die Interpretation von verhaltensbasierten Log-Analysen

In der Branche wird aktuell viel über Automatisierung und die Auswirkungen der künstlichen Intelligenz auf IT-Sicherheitssoftware diskutiert. Dabei wird gerade im Hinblick auf Lösungen für das Security Information und Event Management (SIEM) oft der Eindruck erzeugt, als würden Sicherheitsverantwortliche in den Unternehmen durch Software ersetzt. Das Gegenteil ist der Fall. Vielmehr geht es darum, dass es geschulte und entsprechend erfahrene Experten braucht, um die Ergebnisse aus den Analysen richtig zu interpretieren und die erforderlichen Schlüsse und Maßnahmen daraus abzuleiten. Das Stichwort in diesem Zusammenhang ist das maschinelle Lernen der Sicherheitssoftware, die laufend aus unterschiedlichsten Quellen Logs sammelt, normalisiert, korreliert und auswertet. Gleichwohl es dem Nutzer einfach gemacht wird, in dem die Ergebnisse graphisch über verschiedene Diagramme aufbereitet werden können, bedarf es dennoch einer Einordnung der laufend automatisch generierten Alarm- und Warnmeldungen und dies kann nur ein Spezialist, der mit der Software und ihrem Output vertraut ist.

Besonders im Hinblick auf die zunehmende Komplexität dieser Software und der Aufgaben, die

sie mit den Big Data-Analysemöglichkeiten leisten kann, hängt immer mehr von den handelnden Personen ab; der Art und Weise, wie sie die gewonnenen Erkenntnisse nutzen, um ihre Unternehmen vor Hackerangriffen zu schützen, sowie davon, wann die Verantwortlichen bei einem Sicherheitsvorfall beispielsweise weitere externe Unterstützung in Form von Forensikspezialisten, Penetration Testern etc. hinzuziehen.

Analyse des Nutzerverhaltens
Eine Auswertung des Nutzerverhaltens in Echtzeit, im Englischen als „User Behavioral Analytics" bezeichnet, bietet die Möglichkeit mit SIEM-Software Daten Exfiltrierungen aufzudecken, kompromittierte Login-Daten zu finden, herauszufinden, ob und wie privilegierte Accounts ausgenutzt wurden und welche unbekannten Bedrohungen aktuell im Netzwerk ihr Unwesen treiben. Mit der Einbindung in SIEM, Intrusion Detection-Systeme und Firewalls können Protokollinformationen eingelesen werden, die für eine verhaltensbasierte Analyse die entscheidende Grundlage darstellen. Durch die Korrelation dieser Informationen können die Experten herausfinden, welches Verhalten für ihre jeweiligen Nutzer und IT-Systeme „normal" ist und welches Verhalten davon abweicht.

Darüber hinaus, und hier kommt die praktische Erfahrung mit solchen Systemen ins Spiel, ist es wichtig für die Effizienz der Auswertungen, dass harmlose Verhaltensabweichungen von Bedrohungen unterschieden werden. Hier hilft der Ansatz des maschinellen Lernens weiter, denn durch die automatischen Lerneffekte der Software entfällt ein hoher administrativer Aufwand, jede Abweichung manuell unter die Lupe nehmen zu müssen. Diese Reduktion der False Positive-Meldungen über den Faktor Zeit ist nicht zu unterschätzen. Wer wirkliche Bedrohungen von eher unwichtigen Fehlermeldungen trennen kann, der kann auch besser priorisieren und sich schneller um die Lösung der wirklich wichtigen Probleme kümmern. Anstatt mehreren hundert Falschmeldungen nachzugehen, sind es vielleicht lediglich zwei bis drei wirklich gefährliche Warnungen, die beachtet werden müssen. Dies ermöglicht eine schnellere Entscheidungsfindung und bessere Ressourcenausnutzung der eingesetzten Experten.

Insider-Attacken – das unterschätzte Übel
Wichtiger als die Erkennung, Analyse und Begegnung externer Angriffe sind interne Angriffe, denn interne Angreifer wissen in der Regel besser, wo sie welche Daten finden, und müssen nicht lange suchen. Mit selbstlernenden verhaltensbasierten Analysen und Sicherheitsmonitoring-Software können solche Insider-Angriffe frühzeitig erkannt werden. Besonders die Aufzeichnung des Nutzerverhaltens in Echtzeit verbessert die Identifikation dieser Attacken deutlich. Daneben werden ebenfalls in Echtzeit Risikoprofile erstellt, anhand derer die Attacken eingestuft und bewertet werden, um die möglichen Auswirkungen eines Sicherheitsvorfalls vorab bewerten zu können. Durch das maschinelle Lernen der Software verbessert sich die Bewertung der Alarme stetig und die Granularität lässt sich stetig steigern, um eine neue Ebene der Security zu erreichen. Diese Möglichkeiten verhaltensbasierter Software-Lösungen erlauben eine bessere Gefahrenerkennung und dadurch auch die schnellere Einleitung von Gegenmaßnahmen und Analyse des Vorfalls.

Fazit
Künstliche Intelligenz wird in vielen Branchen im Rahmen der Digitalisierung derzeit unter anderem als Job-Killer diskutiert. In der IT-Sicherheitsbranche, eine Branche, die stetig wächst und immer mehr Beschäftigung generiert, kann von einer Reduktion durch KI und maschinelles Lernen von Sicherheitssoftware eigentlich keine Rede sein. Zu komplex und vielschichtig sind die Anforderungen. Zu viele zusätzliche Aufgaben wie die Absicherung von mobilen Geräten, IoT-Geräten, Cloud Umgebungen und Services wie auch organisatorische Aufgaben sowie das große und immer wichtigere Thema Security Awareness mit entsprechenden Maßnahmen und Trainings der Mitarbeiter sind in den letzten Jahren hinzugetreten.

Darüber hinaus müssen die Auswertungen, die durch selbstlernende Sicherheitssoftware generiert werden richtig interpretiert und die Ergebnisse aufbereitet werden, dies ist ohne erfahrene und gut geschulte Sicherheitsverantwortliche gar nicht möglich. Expertensoftware benötigt entsprechende Mitarbeiter, die diese auch für das Unternehmen gewinnbringend einsetzen können. Letztlich profitieren Unternehmen von beidem, Experten und moderner Sicherheitssoftware mit der Unternehmen sich vor Attacken von innen wie außen besser schützen können. Intelligente Software unterstützt Fachleute u.a. bei der Aufklärung von Sicherheitsvorfällen dabei mehr Licht ins Dunkel zu bringen, und den Unternehmen ihre Kronjuwelen vor Cyberkriminellen zu schützen.

Pascal Cronauer

Der Mensch im Mittelpunkt – wie etabliert man ein Insider-Threat-System?

Wie schütz man die Zero-Perimeter-World, eine digitale Welt ohne klare Grenzen? Die Unternehmen sehen sich mit der Aufgabe konfrontiert, ein stetig im Wandel befindliches, hybrides Konstrukt aus öffentlichen, privaten und Unternehmensnetzwerken zu schützen, auf das rund um die Uhr unkontrolliert zugegriffen wird. Verschiedene Cloud-Applikationen, Private-Cloud- und Storage-Lösungen oder auch andere Services, die oft nicht vom Unternehmen gemanagt werden, machen heutige IT-Landschaften überkomplex. Die Strategie über reinen Infrastrukturschutz für Cybersicherheit zu sorgen, hat dadurch ausgedient.

Neue Bedrohungen
Insider Threats oder auch die Gefahren von innen rücken mehr und mehr ins Bewusstsein der Sicherheitsverantwortlichen. Warum sind diese Bedrohungen so gefährlich?

Erstens, wer erst einmal im Unternehmensnetzwerk ist, kann dort beinahe ungestört agieren, ohne dass er große Gefahr läuft, entdeckt zu werden. Zweitens, ein Großteil dieser Bedrohungen kommt ohne Schadcode aus und wird deswegen von gängigen Tools nicht entdeckt. Eine Welt ohne klare Netzwerk-Perimeter verlangt einen ganzheitlichen Sicherheitsansatz. Den Umgang mit und die Bewegungen von Daten im Unternehmen zu verstehen, ist der Schlüssel zu einem solchen. Welche Daten sind schützenswert und welche Compliance-Vergehen gilt es zu verhindern? Das sind die Fragen, die sich Unternehmen zu allererst stellen müssen. Dazu ist es auch allerhöchste Zeit, denn im Hinblick auf die Datenschutz-Grundverordnung (DSGVO) werden Unternehmen Fragen beantworten müssen, zum Umgang mit sensiblen Daten. Ohne Transparenz über vorhandene Datenströme ist das nicht zu schaffen.

Was schützen?
Welche Daten müssen geschützt werden, wo befinden sich diese und wer greift auf diese wann und wie zu? Neben der örtlichen Zuordnung der Daten, also ob diese sich im Unternehmensnetzwerk, in Rechenzentren, bei Dienstleistern oder in Cloud-Anwendungen befinden, gilt es auch festzustellen, in welchem Zustand die Daten sind. Also Data at Rest (gespeichert), Data in Use (von Mitarbeitern benutzt) oder Data in Motion (in den oben beschriebenen Netzwerken unterwegs). Moderne Data-Leakage-Prevention-Lösungen (DLP) können hier aufwändige Datenklassifizierungen weitgehend ersetzen und die sensiblen Daten automatisiert identifizieren sowie erfassen.

Transparenz schaffen
Ein Monitoring-Tool mit User Behavior Baselining lernt automatisiert das Normalverhalten im Umgang mit schützenswerten Daten und kann in Abgleich mit vorher erstellten Compliance-Regeln entscheiden, welche riskanten Aktionen überprüft werden müssen. Administratoren bekommen wesentlich weniger falsche Benachrichtigungen, denen sie nachgehen müssen und können sich auf wirklich relevante Vorfälle konzentrieren. Über ein Dashboard sieht der Sicherheitsverantwortliche einen Risk-Score, der anzeigt, wo es im Netzwerk riskantes Verhalten im Umgang mit sensiblen Daten gibt. Um den Datenschutz zu gewährleisten, funktioniert ein User Behavior Monitoring (UBM) etwa wie ein Flugschreiber. Informationen zum Nutzerverhalten werden pseudonymisiert erfasst. Diese Daten sind mehrstufig verschlüsselt, sie können nur dekodiert und einem Mitarbeiter zugeordnet werden, wenn ein konkreter Verdacht vorliegt. Ein autorisiertes Gremium aus IT-Leiter, Geschäftsführung und Betriebsrat muss dazu eine Freigabe erteilen.

Analysieren und gegensteuern
User and Entity Behavior Analytics (UEBA) analysieren „out of the box" das riskante Verhalten und setzt dieses in Zusammenhang mit Informationen aus dem gesamten Netzwerk. So entsteht ein umfassendes Bild, das auch Aufschluss über eine Zielsetzung oder Motive geben kann. Moderne Lösungen kombinieren UEBA mit DLP und stellen dadurch sicher, dass keine sensiblen Daten das Unternehmen verlassen. Mit dieser Kombination lässt sich das forensische Potenzial eines Insider-Threat-Systems voll ausschöpfen und Vorfälle vom ersten bis zum letzten Moment verfolgen. Die forensischen Erkenntnisse sind außerdem auch vor Gericht ein gültiges Beweismaterial. Ein durchgängiges Insider-Threat-Programm mit den genannten Komponenten gewährleistet umfassenden Schutz vor Infiltration, vor unbeabsichtigtem Fehlverhalten von Mitarbeitern sowie vor Datendiebstahl. Nur so lassen sich Mitarbeiter und Daten in der Zero-Perimeter-World effektiv schützen.

Frank Limberger

Frank Limberger, Data & Insider Threat Security Specialist, Forcepoint Deutschland GmbH

1.2 DATEN-SICHERHEIT

Sind mobile Endgeräte eine Schwachstelle – oder eher Ihre Security-Strategie?

Ich höre immer wieder von Unternehmen, denen Endpoint-Backup-Lösungen zu komplex wurden – und die sich darum darauf beschränkten, manuell Kopien anzufertigen. Dass das nicht nur aufwändig, ineffizient und fehleranfällig, sondern auch in zunehmenden Maße unsicher ist, brauche ich kaum zu erwähnen. Die Ursachen für dieses Handeln liegen tiefer: Viele Organisationen tun sich immer noch schwer damit, moderne und dennoch bereits erprobte Technologien anzunehmen, ihre Mitarbeiter in deren Nutzung zu

Newsletter und mehr Beiträge: www.digitaleweltmagazin.de/blog

Robert Romanski, Systems Engineer bei Commvault, Commvault

schulen und natürlich auch zu beobachten, welche Prozesse sinnigerweise beizubehalten, zu ersetzen oder völlig über den Haufen zu werfen sind. Weil mir die Absicherung von Endgeräten tatsächlich eine Herzensangelegenheit ist, möchte ich auf die Komplexität eingehen, die sich doch relativ gut vereinfachen lässt:

Mobilität ist Selbstverständlichkeit. Oder bloß ein teurer Spaß?
Wenn es darum geht, modernes Arbeiten zu definieren, dann gehört Mobilität ganz definitiv ins Glossar: Mit Notebooks, Tablet-PCs und Smartphones nutzen wir unsere Zeit am belebten Flughafen, in einsamen Lobbys und entspannt im Café mehr aus. Wenn nun eines dieser Endgeräte verloren geht, ist der Verlust eines vielleicht 1.000-Euro-teuren Gadgets wirklich so dramatisch? Nun, den Verlust der Buchhaltung zu erklären, ist kein Spaß. Den Verlust vor dem IT-Sicherheitsbeauftragten zu rechtfertigen noch weniger. Die Chancen stehen ziemlich gut, dass das mehr oder weniger lieb gewonnene Gerät wertvolles geistiges Eigentum enthält oder dass das Unternehmen nach dem Verlust von Daten nicht mehr Compliance-konform agiert. Das Problem: Der Schutz mobiler IT ist vielschichtig. Ist er nicht schnell, effizient, verlässlich und transparent, werden mobile Nutzer ihn nicht einsetzen.

Anders als im Fall von Servern, die stets mit einer Hochgeschwindigkeits-Netzwerk-Backplane verbunden sind, werden Laptops häufig ausgeschaltet oder möglicherweise mit Netzwerken mit niedrigen Bandbreiten verbunden. Dies erschwert die Planung und Ausführung automatisierter Backups. Gleichzeitig speichern viele Mitarbeiter tätigkeitsbezogene Daten in persönlichen Freigabediensten in der Cloud, die nicht von Ihrem IT-Team kontrolliert werden, wie Dropbox und Google Drive.

Ich würde dies nicht erwähnen, meine Kollegen und ich selbige Schichten des Problems nicht unzählige Male durchkämmt hätten – und es eine Lösung gibt. Datenspezialisten arbeiten sogar an „Endpoint Data Protection as a Service“. Das bedeutet, dass keine eigene Infrastruktur gekauft, installiert und gewartet werden muss.

Das beinhaltet dann zum Beispiel dass,

- kritische Unternehmensdaten auf Laptops und Desktop-Computern mit einem automatisierten Backup-Service geschützt und gesichert werden, ohne die Benutzerproduktivität zu behindern.
- integrierte Sicherheitseinstellungen den Datenverlust minimieren, indem Nutzer Dateien und Ordner verschlüsseln, Geolokalisierung nutzen und Daten sicher von verlorenen oder gestohlenen Notebooks löschen können.
- Sichtbarkeit und Kontrolle über Endpunkt-Daten im Fall von Compliance- oder Rechtsstreitigkeiten gewährleistet sind.

Zuwenig Bandbreite ist keine Ausrede mehr
Zwar wird das Internet in Deutschland immer besser, aber wer ist schon permanent online und mit dem Firmennetzwerk verbunden? Der W-LAN-Zugang am Flughafen etwa stellt nicht das Gelbe vom Ei dar. Aber glücklicherweise lassen sich Endgeräte mittlerweile sehr viel effizienter abdecken. Backup-Programme helfen bei der Bewältigung dieser Herausforderung durch automatische Planung, Bandbreitenbegrenzung und Backup-Ausführung, was den zusätzlichen Vorteil hat, dass Nutzer so wenig wie möglich gestört werden. Während die IT-Abteilung immer noch darauf angewiesen ist, regelmäßig Updates von den Business-Geräten zu bekommen, sollen Mitarbeiter weiterhin flexibel arbeiten können, ohne dass Backup-Prozesse sie ausbremsen oder gar völlig am Arbeiten hindern.

Funktionen wie die quellseitige Deduplizierung mit inkrementellem Backup halten den Bandbreitenbedarf des Netzwerks gering, indem die Datenmenge, die über das Netzwerk gesendet wird, reduziert wird, während die IT-Abteilung dennoch den gewünschten Datenzugriff erhält. Außerdem wird die Gesamtdatenmenge im Vergleich zu einem Voll-Backup reduziert, da die inkrementellen Sicherungen nur die geänderten Daten enthalten. Darüber hinaus bietet eine integrierte Client-seitige Verschlüsselung schnelle und effiziente Sicherheit ohne der IT weiter zu belasten.

IT-Mitarbeiter sind mehr denn je mit Datenmanagement beschäftigt. Sie müssen in der Lage sein, Daten von Endgeräten zu sammeln und zu sichern – ohne Auswirkungen auf die Anwender. Wie kürzlich eine Studie von Commvault ergeben hat, stecken IT-Experten durch diese und viele andere Routineaufgaben fest, gerade einmal 6 Prozent ihrer Zeit können sie auf strategische Entwicklungen verwenden. Ein valider Weg, dies zu ändern, ist, den Nutzern Autonomie zu geben. Mit den passenden Self-Service-Tools und Rollen ausgestattet, können sie ihre eigenen Backups durchführen – und Daten selbst wiederherstellen. Sie können selbst den Zeitrahmen festlegen, wann wichtige Prozesse ablaufen sollen und sind nicht von der Planung der IT abhängig. Außerdem lassen sich Workflows automatisch festlegen.

IT-Mitarbeiter wiederum können auch verlorene oder gestohlene Laptops beziehungsweise Remote-Dateien orten, um sicherzustellen, dass das Unternehmen im Falle eines Verlustes des Geräts geschützt ist.

Punktlösung versus Enterprise Data Protection
Wenn es darum geht, Unternehmensdaten zu schützen, bringt eine ganzheitliche Lösung mehr als immer wieder nur einzelne Pain Points zu behandeln. Eine „Endpoint Data Protection System“, das in die komplette Backup- und Recovery-Strategie integriert ist, hat gegenüber einer Punktlösung einige Vorteile:

- Zentrale Verwaltung und Integration
- Einfache Oberfläche für Benutzer und Administratoren
- Weniger isolierte Software und Plattformen für die Wartung
- Überlegene Skalierbarkeit
- Geringere Betriebskosten

Zu guter Letzt
Letztendlich will jeder eine Software, die die Anforderungen des Unternehmens an die Datenhaltung und das Reporting erfüllt, die Produktivität nicht beeinträchtigt und den Anwendern Selbstbedienungs-Tools an die Hand gibt. Und das Schöne: Das ist nicht zu viel verlangt. Aber das gilt noch gar nicht so lange. Schließlich sind noch jede Menge schwerfälliger und klobiger Lösungen in Betrieb, die so gar nicht zum agilen Arbeiten und dem digitalen Business passen, das vom Management gefordert wird. Es ist an der Zeit, nicht länger Endgeräte oder deren Nutzer zu beschuldigen, wenn etwas schiefgeht, sondern sich des Risikos bewusst zu werden, das mit der heutigen Arbeitsweise und dem datenbasierten Business verbunden ist, und die Auswirkungen zu minimieren. Gewinnen Sie die Kontrolle über Unternehmensdaten auf Laptops, Desktops und in letztlich der Cloud zurück.

Robert Romanski

Das Wertversprechen und Sicherheitsrisiko von Daten steuern

Der Datensteuervorschlag von Bundekanzlerin Angela Merkel wirft grundsätzliche Fragen zum Datenwert, zur Regulierung und Chancengleichheit auf. So sollen auch kleine Firmen aus Daten Werte entwickeln können. In den Daten stecken neben Geschäftsaussichten aber auch Sicherheitsrisiken, die sich senken lassen – mit dem DataOps-Ansatz.

Die Konferenz „Global Solution“ in Berlin Ende Mai hat Bundeskanzlerin Angela Merkel genutzt, um eine Datensteuer ins Spiel zu bringen. Diese soll nach ihrer Ansicht für mehr Gerechtigkeit im Umgang mit den Konsumentendaten sorgen. Nicht der Staat, sondern der Nutzer soll Geld bekommen, sagen hingegen fünf Forscher, die sich mit Künstlicher Intelligenz (KI) beschäftigen. In ihrem Papier „Should We Treat Data As Labor? Moving Beyond ‚Free’“ schlagen die KI-Experten vor, den Nutzer, der Daten liefert, zu bezahlen. Dagegen hält unter anderem die Werbebranche, dass Konsumenten für ihre Daten doch bereits eine Gegenleistungen erhielten: personalisierte Angebote. Reicht das als Gegenwert?

Der kleine Ausschnitt an Reaktionen zeigt: Der Vorstoß der Regierungschefin setzt eine wichtige Diskussion in Gang, die sich vor allem mit der Frage beschäftigen muss: Was sind Daten wert? Der Zeitpunkt im Datenprozess ist entscheidend. Beim Erfassen sind Daten eigentlich noch wertlos. Erst Algorithmen veredeln die Informationen und schaffen Werte, wofür ein Datenexperte ein Datenmodel erstellen muss. Eine Datensteuer benötigt also eine exakte Bemessungsgrundlage, die den unbearbeiteten Rohstoff taxiert. Als „einfache Messgröße“ kann sich Michael Clasen, Professor und Wirtschaftsinformatiker an der Hochschule Hannover, die Zahl der Nutzer bei einer Plattform wie Facebook vorstellen. Auf die Wertschöpfung zielt die schon länger diskutierte Änderung der Körperschaftssteuer ab, nach der Amazon, Google, Facebook & Co ihre Gewinne dort versteuern müssten, wo sie diese erwirtschaften. Die ebenso auf EU-Ebene geplante „Digital Service Tax“ würde die digitalen Umsätze besteuern. Alle drei Steuervorschläge in einer großen Steuerreform zu vereinen, birgt die Gefahr, dass ein komplexes Regelwerk entsteht, welches einseitig in den Wettbewerb eingreift. Eine solche Wirkung entfaltet die EU-Datenschutzgrundverordnung (DSGVO).

Minas Botzoglou, Regional Director, Delphix Corp.

Voraussetzungen für die Wertschöpfung
Die digitale Wettbewerbsfähigkeit hängt entscheidend von drei Faktoren ab: der Technologiebasis, der Unternehmens-Konsumentenbeziehung und dem Datenzugang. Das Implementieren moderner Technologien wie maschinelles Lernen und Künstlicher Intelligenz befähigt dazu, Datenströme zu managen, in Echtzeit zu analysieren, neu zu kombinieren und erneut auszuwerten. Ohne Investitionen in die IT gelingt es Unternehmen nicht, Werte aus Daten zu erzeugen, was heute vor allem auf das Personalisieren von Produkten und Services hinausläuft. Das zielgruppengenaue Programmieren einer solchen App muss jetzt die Vorgaben der DSGVO einhalten. Das Regelwerk bietet ausdrücklich die Möglichkeit, über das „Maskieren“ personenbezogener Informationen Daten irreversibel zu anonymisieren. Unter dieser Voraussetzung fallen die Daten nicht mehr unter die DSGVO. Die Datenmaskierung für die Softwareentwicklung lässt sich relativ einfach realisieren – mit der DataOps-Technologie. Wie das funktioniert, darüber habe ich in einem früheren Post berichtet.

Wie bereitwillig Konsumenten bisher ihre Daten für ein individualisierten Service herausgegeben haben, zeigen Plattformökonomien von Facebook,

Google, Amazon & Co.. Im Prinzip appelliert die DSGVO an die Konsumenten, künftig aus Datenschutzgründen auf ein besseres Angebot zu verzichten. Ob diese Botschaft ankommt oder der mögliche Gegenwert für die Daten mehr zieht, bleibt die spannende Frage, die jeder für sich beantworten muss. In der besten Position im Wettstreit um Kunden befinden sich die Big Tech Player. Ihr Geschäftsmodell funktioniert und skaliert.

IT-Konzerne zur Datenfreigabe verpflichten?
Vor dieser Herausforderung stehen kleinere Tech-Firmen noch. Vor ihnen bauen sich jedoch zusätzliche Hürden auf, weil sie ihre IT zum Teil radikal umbauen müssen, um DSGVO-konform zu agieren. Während die einen wegen der hohen Investitionen aufgegeben, kapitulieren andere kleine Anbieter vor der Komplexität, welche die Regulierung mit sich bringt. Die Tech-Konzerne geraten hingegen nicht in die Bredouille. Im Gegenteil, denn die DSGVO stärkt ihre Marktmacht, die ihnen noch einen wesentlichen Vorteil beschert: Sie verfügen über die größte Datenmenge. Nur wer Zugang zu den Daten hat, kann aus ihnen innovativ Werte entwickeln. Wirtschaftsinformatiker Clasen gehört zu den Experten, die sich vorstellen können, Unternehmen zur Datenfreigabe zu verpflichten. Diese würde für ihn greifen, wenn ein Konzern 99 Prozent aller Daten eines Marktes beherrscht.

Die Diskussion über den Wert von Daten muss daher auch ausloten, wie sich Chancengleichheit für datenzentrierte Geschäftsmodelle herstellen lässt. Ein fairer Wettbewerb findet noch nicht statt. Gefahren drohen Unternehmen jedoch nicht nur durch überschnelle und komplizierte Regulierungen, die Innovationen (aus)bremsen, sondern durch auch durch die Daten selbst.

Datenfragmentierung und die Folgen
Ständig entstehen in einem Unternehmen neue Daten. Diese verteilen sich meist über mehrere Orte. Zugleich entwickeln sich Struktur und Form der Daten kontinuierlich weiter. Daten werden fragmentiert, was wiederum die Basis liefert, agil und flexibel mit digitalen Service auf Nutzerwünsche einzugehen. Die Chance auf Neugeschäft, auf das Wertversprechen der Daten, bildete nur einen der Teil der sogenannten Datenfriktion ab. Denn der firmeninterne Datenfluss birgt auch Risiken und führt zu Beschränkungen. Die Aufgabe besteht also darin, den Datenfluss im Unternehmen sicher und effektiv zu beherrschen. Dazu sind Sicherheitsmaßnahmen nötig, die jedoch nicht allzu stark zu Lasten der Innovationsfähigkeit gehen dürfen.

Die Datenfriktion verlangt von Unternehmen, dass sie wissen, wie sich ihre produktiven und nicht-produktiven Systeme zu einem Daten-Workflow verbinden. Die DataOps-Technologie stellt genau das in Aussicht und deckt zudem mögliche Risiken auf. Ein Unternehmen installiert seine DataOps-Software auf dem Hypervisor. Dadurch entsteht eine Plattform, die sich mit den geschäftskritischen Systemen verbindet. Die Technologie stellt virtuelle Datenkopien von den betreffenden Datenbanken, Applikationen und Dateisystemen schnell und sicher für Entwicklung, Tests, Reporting, Analysen und Backups bereit. Die Daten werden bei Änderung in der Originalquelle synchronisiert. Zur Verfügung stehen zudem Datenprofilierungstechniken, mit denen sich vertrauliche Informationen wie Namen, Adressen und Sozialversicherungsnummern schnell identifizieren lassen. Auf die Weise können Unternehme schnell Prozesse aufsetzen, um Risiken aufzudecken und zu minimieren. Das schließt insbesondere eine automatisierte Datenmaskierung ein.

Steuerungsmodell für die Daten
Der Umgang von strukturierten und unstrukturierten Daten in immer heterogener werdenden Umgebungen entscheidet künftig mit über den Geschäftserfolg, den eine Daten- oder wie auch immer geartete Digitalsteuer beeinflussen kann. Die Diskussion über eine mögliche Regulierung läuft. Ob in die Richtung für fairen Wettbewerb, bleibt abzuwarten. Mit der Ungewissheit muss die Wirtschaft leben, jedoch nicht mit Risiko, das in der Natur der Daten liegt. Beispielsweise darf ein unkontrolliertes Kopieren von Produktivdaten für andere Anwendungen nicht passieren. Ein Unternehmen muss jederzeit wissen, welche Daten wie durch seine Systeme fließen. Dieser Anspruch lässt sich leicht und effektiv mit einer DataOps-Plattform erfüllen, die zudem die Geschäftsmöglichkeiten erweitert. Minas Botzoglou

Data Leakage Prevention – Datendieben auf der Spur!

Nie waren sie so wertvoll wie heute: unsere persönlichen Daten. Seien es personenbezogene Daten oder geschäftsrelevante Informationen, die in all den täglichen Kundenanfragen, internen E-Mail-Korrespondenz oder in digitalen Personalakten schlummern. Für Hacker und Datendiebe sind diese Inhalte das Gold des 21. Jahrhunderts. Das belegen auch die aktuellen Zahlen der Bitkom: Laut der im Juli dieses Jahres veröffentlichten Studie „Wirtschaftsschutz in der digitalen Welt“ war in den letzten beiden Jahren jedes zweite Unternehmen in Deutschland von Datendiebstahl, Industriespionage oder Sabotage betroffen. Im Fokus der Angreifer standen dabei meist Kommunikationsdaten wie E-Mails (41 Prozent), Finanzdaten (36 Prozent) und Kundendaten (17 Prozent).

Mit der Zunahme der digitalen Kommunikation in allen Lebensbereichen muss deshalb davon

ausgegangen werden, dass sich dieser Trend weiter verstärkt. Etablierte Schutzmaßnahmen wie beispielsweise Virenscanner, Spamschutz oder Firewalls reichen dann nicht mehr aus. Denn Angreifer, die es auf geschäftskritische Daten abgesehen haben, gehen bereits jetzt sehr viel gewiefter vor. Denken Sie nur an beliebte Einfallstore wie täuschend echt aufgemachte Phishing E-Mails, mit Trojanern verseuchte Webseiten oder auch die personalisierte Manipulation durch Social Engineering. Um an Firmeninterna zu kommen, nutzen Betrüger unter Vortäuschung eines Vertrauensverhältnisses menschliche Eigenschaften, insbesondere Hilfsbereitschaft oder Respekt vor Autoritäten, aus, um sensible Daten zu erlangen.

Probleme, den Datenklau zu erkennen
Dabei stehen viele Unternehmen vor der Herausforderung, Datendiebstahl und Compliance-Verstöße überhaupt zu erkennen – insbesondere dann, wenn die Datendiebe bereits im Haus sind, weil sie die Firewall überwunden haben oder es sich bei ihnen sogar um Mitarbeiter des Unternehmens handelt. Tatsächlich belegt der Bitkom in seiner bereits eingangs zitierten Studie, dass immer mehr Mitarbeiter zum Datenleck in Unternehmen werden – ob nun beabsichtigt oder ungewollt: In 62 Prozent aller Datenvorfälle der letzten zwei Jahre waren aktuelle oder ehemalige Mitarbeiter involviert. Warum es so viele Mitarbeiter sind? Nun, denken Sie zum Beispiel an die täglich hunderte E-Mails, die gesendet werden: Sie können sich also vorstellen, dass es gerade in großen Organisationen ein sehr komplexes Unterfangen ist, potentiellen Datenabfluss frühzeitig zu erkennen. Stellen Sie sich doch einfach einmal diese Fragen: Wissen Sie, welche Daten ihr Unternehmen per E-Mail verlassen? Können sie ausschließen, dass schützenswertes Know-how dabei ist? Sind Mechanismen etabliert, die den illegalen Versand – ob beabsichtigt oder versehentlich – von Kundendaten blockieren? Und: Gibt es ein Notfallplan, der im Falle einer Datenpanne genau regelt, was wann von wem zu tun ist?

Ausgehende Korrespondenz zu wenig beachtet
Unternehmen achten meist sehr umfänglich und mit mehrstufigen Sicherheitsmechanismen auf ihre eingehende Kommunikation, schenken aber ihrer ausgehenden zu oft zu wenig Beachtung. Wer an E-Mail Sicherheit denkt, verbindet damit häufig nur Viren- und Spamschutz. Generell liegt in vielen Unternehmen der Fokus auf der eingehenden Kommunikation. Risiken, die bei unkontrollierter Kommunikation von innen nach außen lauern, werden nur selten wahrgenommen. Die Praxis zeigt aber, dass gerade der Verlust von sensiblen Informationen, das arglose Versenden von personenbezogenen Daten und die Missachtung von Vorschriften, beispielsweise zum Schutz von Kundendaten, immer größere Probleme bereitet. Wo früher der Diebstahl von Kundendaten noch via USB-Stick oder selbst gebrannten DVDs stattfand, haben es Datendiebe heute dank E-Mail leider sehr viel leichter. Kundendaten mit einem sehr viel größeren Umfang lassen sich mit nur einem Klick als Anhang an eine E-Mail anfügen und versenden.

Vertrauen ist gut, Kontrolle ist besser
Regelmäßig enthalten E-Mails samt ihrer Dateianhänge sensible Informationen und Unternehmenswissen – seien es Angebote, Verträge oder beispielsweise Spezifikationen. Um den unkontrollierte Versand dieser Daten zu verhindern brauchen Unternehmen Mechanismen, die solch einen Datenabfluss entdecken und unterbinden. Das beginnt mit der Kontrolle der zu versendenden Dateianhänge, geht über die Kontrolle ausgehender Textinhalte bis hin zur umfassenden Echtzeit-Analyse des E-Mail-Verkehrs für das gesamte Unternehmen oder einzelne Abteilungen.

Eine zeitgemäße DLP-Lösung (Data Leakage Prevention) erkennt beispielsweise Schlüsselbegriffe, die den branchenspezifischen Sprachgebrauch im Unternehmen prägen und die sich im E-Mail-Text oder Anhang befinden können. Das können bei Unternehmen aus dem Finanzsektor oder bei Online Shops Finanzdaten, Kreditkarteninformationen und Kundennummern sein, bei Unternehmen aus der Gesundheitsbranche Versicherungsdaten und definierte Patientendaten. Zudem kann eine auf elektronischen „Fingerprints“ basierende Technologie Dateiformate unabhängig von ihrer Benennung oder Dateiendung zuverlässig erkennen. So sind beispielsweise Office-Formate eindeutig identifizierbar. Im Rahmen einer automatisierten Prüfung lässt sich der Versand solcher E-Mails vereiteln.

Schon diese Maßnahmen können eine erste Hürde sein, den Versand vertraulicher Daten zu verhindern, können aber im Zweifel nicht alle Schlupflöcher abdecken. Deshalb gehen einige DLP-Lösungen noch einen Schritt weiter, indem innovative Erkennungstechnologien sogenannte Anomalien im E-Mail-Fluss aufdecken. Oder anders ausgedrückt: Abweichungen vom Standard-Verhalten beim E-Mail-Versand sollen erkannt und entsprechend darauf reagiert werden. Dazu können Informationen, wie E-Mail-Anzahl oder -Größe, über einen definierten Zeitraum gesammelt und mit dem aktuellen Verhalten der Anwender abgeglichen werden. Im Ergebnis ist beispielsweise der plötzliche Versand großer Datenmengen oder ein überproportionaler Anstieg des E-Mail-Volumens ersichtlich. Dies können mögliche Anzeichen für den Versand vertraulicher Inhalte sein.

Andreas Richter, Mitglied der Geschäftsleitung, Director Marketing & Product Management, GBS Europa GmbH

Verdächtige E-Mails blockieren
Die erfassten Daten können auf verschiedene Art und Weise ausgewertet werden. Bereits die Visualisierung gibt einen detaillierten Einblick in die ausgehende E-Mail-Kommunikation. Darüber hinaus sind durch Einführung bestimmter Regeln und Grenzwerte verschiedene Aktionen möglich, wie mit potentiell vertraulichen Inhalten umgegangen wird. Denkbar ist beispielsweise, den Versand anzuhalten und die E-Mail in einem geschützten Bereich abzulegen oder die IT-Verantwortlichen zu benachrichtigen. Sollten Zweifel über die Legitimität des Versandes oder Vertrauenswürdigkeit der Daten bestehen, kann auch das 4-Augen-Prinzip helfen: Eine E-Mail wird in der Quarantäne geparkt und der Absender informiert. Es folgt die 4-Augen-Prüfung durch eine zweite Instanz, zum Beispiel den Datenschutzbeauftragten oder Compliance-Verantwortlichen, und damit die Entscheidung über die endgültige Blockade oder den Versand der E-Mail.

In jedem Fall ist es aufgrund der steigenden Datenmengen entscheidend, dass die eben skizzierten Szenarien zu einem Großteil automatisiert ablaufen, da sich sonst ein solcher DLP-Prozess nicht wirtschaftlich umsetzen lässt. Im Zusammenspiel mit organisatorischen Maßnahmen wie der Sensibilisierung der Mitarbeiter durch Schulungen oder konkrete Betriebsanweisungen sowie unter Berücksichtigung geltender Datenschutzbestimmungen lässt sich auf diese Weise Datenklau nicht nur erkennen, sondern auch wirkungsvoll verhindern.

Andreas Richter

Security-Regeln: Bei Daten-GAU plötzlich außer Kraft

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

Größere Unternehmen verfügen über ausgefeilte Security-Policies und Prozessbeschreibungen vom Backup bis zur Datenwiederherstellung. Auch tiefgreifende Audits und umfangreiche Datenschutzerklärungen für Dienstleister aus der Hard- und Softwarebranche sind Usus. Was dabei aber häufig unter den Tisch fällt, sind Notfallpläne für den Fall der Fälle: nämlich wenn sich defekte Datenträger nicht hausintern wiederherstellen lassen und der Gang zu einem Datenretter erforderlich wird. Bei kritischen Systemausfällen werden oft plötzlich zentrale Security-Regeln außer Acht gelassen und in Windeseile Server, RAID-Systeme oder Festplatten mit hochsensiblen Informationen an externe Dienstleister übergeben – ohne dass diese im Vorfeld auf Sicherheit geprüft wurden.

Datendiebe zapfen Dritte an
Die Gefahr dabei: Einige Datenrettungsanbieter schicken defekte Medien an Recovery-Labore ins – bestenfalls – benachbarte Ausland, ohne ihre Kunden explizit darüber zu informieren. Organisierte Datendiebe zapfen Quellen über Dritte in Insider-Branchen an. Wenn auf diesem Weg Daten verloren gehen oder entwendet werden, hat das Unternehmen den doppelten Schaden, denn es kommt auch noch das Haftungsrisiko hinzu: Laut Datenschutzgesetz haftet der Eigentümer dann voll für seine Informationen, wenn er es verabsäumt, die 'sichere Datenverarbeitung' durch seinen Dienstleister vorab zu prüfen. De facto fordert das Datenschutzgesetz damit die Durchführung von Dienstleister-Audits.

Notfallplan für Datenrettung
Vor allem Banken, Healthcare- und Forschungsunternehmen mit sensiblen Daten nutzen verstärkt die Möglichkeit, eigene Notfallpläne für die Datenrettung auszuarbeiten. Ein wesentlicher Punkt dabei ist, dass der Datenrettungspartner schon auditiert wird bevor eine Katastrophe eintritt. Die Auswahl des Datenrettungspartners gehört konsequenterweise in die Security-Policy integriert.

Weitere Gefahrenquelle: Gebrauchte Datenträger
Alte Hardware wird von Unternehmen häufig an den IT-Dienstleister zurückgegeben oder an die eigenen Mitarbeiter verkauft oder verschenkt. Die Datenvernichtung ist somit in vielen Fällen unzureichend, wie Testkäufe von Festplatten auf Tauschplattformen zeigen. So landen Datenträger mit hochsensiblen Daten bei neuen Besitzern. Oft wurden die Datenträger nur gelöscht oder formatiert – selbst für einen semiprofessionellen Datenretter ist es inzwischen kein Problem, diese Daten sogar vollständig wiederherzustellen. Auch einzelne Festplatten oder SSDs aus RAID-Verbunden können noch viele brisante Daten enthalten. Daher ist es empfehlenswert, die internen Löschprozesse von einem professionellen Datenretter regelmäßig mit Stichproben verifizieren zu lassen.

Dipl. Ing. Nicolas Ehrschwendner

1.3 ANGEWANDTE SICHERHEIT

Biometrie 2.0 – Sicherheit durch kontinuierliche Authentifizierung

Cyberkriminelle betreiben für Social Engineering-Angriffe einen immer größeren Aufwand, um ihre Opfer zu verunsichern und sie zur Vernachlässigung von Sicherheitsstandards zu überreden, was hohe Schäden verursachen kann. Beim Microsoft Fraud geben sie sich beispielsweise als Supportmitarbeiter des Unternehmens aus. Üblicherweise kontaktieren sie ihre Zielperson telefonisch und bieten zu Beginn kostenfrei einige Tricks und Tipps, die bei der Optimierung des Geräts helfen, um Vertrauen aufzubauen. Später bieten sie dann für kleines Geld Zusatzfunktionen an, für die sie ihr Opfer dazu bringen, eine Software für den Fernzugriff zu installieren. Sobald sich ihr Gesprächspartner dann in seinen Bankaccount einloggt, manipulieren sie die Eingaben, um mit möglichst viel Geld zu verschwinden.

Gängige Sicherheitsmechanismen versagen beim Microsoft Fraud
Das Problem in einem solchen Angriffsszenario ist, dass gängige Sicherheitsmechanismen umgangen werden. Üblich sind Login-Daten, die aus Benutzername oder Kundennummer sowie einem Passwort bestehen, und eine TAN-Nummer, um Überweisungen und andere Transaktionen zu legitimieren. Die Angreifer manipulieren allerdings über die Remotesoftware, die sie dem Opfer kostenlos zur Verfügung stellen, die eingegebenen Werte.

Der Kunde loggt sich wie gewohnt in seinen Bankaccount ein und es wird eine legitime Sitzung aufgebaut, bei der er sich an seine gewohnten Abläufe hält. Auf Anweisung des angeblichen Supportmitarbeiters wird ein Überweisungsformular ausgefüllt, um eine scheinbar angemessene, kleine Summe für die Serviceleistung zu bezahlen. Zum Abschluss gibt der Kunde die korrekte TAN-Nummer ein, erst dann wird der Kriminelle aktiv: Über das manipulierte Fernzugriff-Programm kann er die Überweisungssumme verändern, ehe der Auftrag an die Bank weitergeleitet wird. Da für den Kunden alles normal verläuft und er den falschen Betrag nicht sieht, wird der Betrug in der Regel erst später auf dem Kontoauszug auffallen, wenn das Geld bereits verschwunden ist.

Verhaltensbasierte Biometrie als Schutz vor Betrügern
Das Problem der gängigen Sicherheitsmechanismen ist, dass sie den Nutzer lediglich zu einem bestimmten Zeitpunkt authentifizieren, nämlich nach Eingabe seiner Benutzerdaten. Sobald eine legitime Sitzung einmal aufgebaut wurde, können die Angreifer diese Sitzung dann ohne aufzufallen manipulieren. Dieses Problem löst eine kontinuierliche Authentifizierung, die während der gesamten Sitzung die Identität des Nutzers prüft und nachweist.

Eine sehr effektive Lösung ist die verhaltensbasierte Biometrie, die auf dem Tippverhalten basiert. Wie ein Nutzer tippt, ist eine individuelle Eigenschaft, die sich selbst unter besten Bedingungen nicht glaubwürdig nachahmen lässt. Dazu werden beispielsweise an Laptops und Desktop-PCs Merkmale wie die individuelle Tippgeschwindigkeit, Pausen zwischen den Eingaben und die Bewegung der Maus oder bei Mobilgeräten die Bewegung des Geräts während der Eingabe, Lage in der Hand und Trefferzonen der Tasten und viele andere Eigenschaften gemessen, um ein unverwechselbares Tippprofil des Nutzers zu erstellen. Dieses wird dann mit dem Tippverhalten während der laufenden Session verglichen, um den Kunden während der gesamten Sitzung zu authentifizieren.

Der Microsoft Fraud fällt mit einer solchen Sicherheitsmaßnahme aus zwei Gründen sofort auf: Erstens kann die Software erkennen, wenn ein Remotezugriff eingerichtet wurde und eine entsprechende Warnung ausgeben. Zweitens, und das ist der entscheidende Vorteil, erkennt die Sicherheitssoftware sowohl den Betrüger, wenn er eine Eingabe tätigen will, als auch einen Bot, der die Eingabe automatisch manipuliert.

Ein Betrüger wird immer ein anderes Tippverhalten als der legitime Nutzer haben und einen Bot erkennt die Software leicht daran, dass die geänderten Daten nicht manuell eingegeben, sondern lediglich eingefügt werden. Selbst fortgeschrittene Bots, die versucht, einen Nutzer zu imitieren, indem sie künstliche Pausen zwischen der Eingabe der Zeichen einbauen und sogar eine Mausbewegung simuliert, können zuverlässig von dem Eingabeverhalten eines Menschen unterschieden werden.

Sebastian Mayer, Director Sales DACH/CEE, BehavioSec

Transparenz und Komfort für den Nutzer
Der Vorteil der Verhaltensbiometrie ist neben der hohen Sicherheit die Benutzererfahrung. Für übliche TAN-Verfahren werden zusätzliche Geräte benötigt, ebenso für Sicherheitscodes per SMS und ähnliche Lösungen. Das Nutzerverhalten, die biometrische Identität als zweiter Faktor, ist für den Kunden hingegen transparent, das heißt, es gibt keinen zusätzlichen Aufwand für den Kunden, sodass ihn die zusätzliche Sicherheitskontrolle während seiner Finanztransaktionen nicht einschränkt.

Damit das unverwechselbare Profil des Kunden selbst geschützt wird, misst die biometrische Sicherheitssoftware das Verhalten des Nutzers nur in der Banking-App der Bank oder per Java Script während der Sitzung im Webbrowser. Aus diesen Messgrößen wird anschließend ein Hash berechnet, der von dem Gerät zur Datenbank des Finanzinstitutes geschickt und dort mit dem Hash aus seinem bisherigen Verhalten verglichen wird. In Millisekunden erfolgt die Bestätigung, ob der Nutzer sich authentifizieren konnte. Der Vorgang ist so schnell, dass die Nutzererfahrung nicht gestört wird.

Fazit
Banken investieren viel in die Sicherheit ihrer Kundenkonten, denn einerseits haften sie finanziell für die entstandenen Schäden beim Endkunden, andererseits werden im Schadensfall knappe Res-

sourcen für die Aufarbeitung des Vorfalls und die Identifizierung der Sicherheitslücke gebunden und zuletzt bedeutet jeder Vorfall einen Vertrauensverlust beim Kunden. Bisher setzen die meisten Banken in Deutschland dennoch auf Authentifizierungslösungen, die die Identität eines Kunden nur zu einem fixen Zeitpunkt bestätigen. Das macht sie anfällig für aktuelle Bedrohungsszenarien wie z. B. Microsoft Fraud, während in Skandinavien die verhaltensbasierte Biometrie als Sicherheitslösung bereits weit verbreitet und bei einem großen Teil der Banken sowie Versicherungen im Einsatz ist. Die Vorteile einer kontinuierlichen Identifizierung über das Tippverhalten des Kunden haben sich dort durchgesetzt.

Sebastian Mayer

Schutz der Marke sorgt für Sicherheit der Kunden und Mitarbeiter

Der Aufstieg der sozialen Medien sorgt für bis vor wenigen Jahren unvorstellbare Möglichkeiten der Kommunikation. Diese Netzwerke bestimmen aber keineswegs nur das private Kommunikationsverhalten, sondern nimmt auch massiven Einfluss auf unser Einkaufsverhalten. Wir folgen den Vorschlägen von Freunden und lesen in den Blogs der Influencer, was heute und morgen State-of-the-Art ist. Diese Veränderung kommt auch immer mehr in den Unternehmen an, die unterschiedlichste Dienste, beispielsweise den Kundenservice, auch über Social Media abwickeln. Kaum überraschend, dass sich auch Kriminelle dieser neuen Möglichkeiten bedienen wollen, um andere um ihr Hab und Gut zu bringen.

Werner Thalmeier, Director Sales Engineering EMEA, Proofpoint

Gefahren für Kunden und Mitarbeiter

Eine wachsende Zahl von Unternehmen nutzt den eigenen Social-Media-Auftritt nicht mehr nur als Kanal, um ihre Werbebotschaft mit potenziellen Kunden zu teilen. Firmen treten durch soziale Netzwerke immer stärker mit ihren Kunden in direkten Kontakt und tauschen sich mit Hilfe dieser Plattformen aus. Dabei geht es immer stärker um wirkliche Interaktion mit dem Kunden, nicht nur um Marketingaktionen oder das Beschwerdemanagement. Und genau diese Interaktion machen sich Cyberkriminelle immer häufiger zunutze.

Hierbei setzen die Täter auf so genanntes „Angler-Phishing“. Das heißt, sie legen gefälschte Social-Media-Profile an, die denen der tatsächlichen Marke zum Verwechseln ähnlichsehen. Oftmals lassen sich solche gefälschten Profile nur an Kleinigkeiten erkennen. Mal ist es ein hinzugefügter oder entfernter Buchstabe, zwei vertauschte Buchstaben wie „BEISPEIL“ oder ein der Optik nach ähnliches Symbol wie „BEISPIEL“ und „ßEISPIEL“. Im Zeitalter von immer höher getakteter Kommunikation wird ein derartiger Betrugsversuch einfach übersehen. Dies geschieht insbesondere deshalb, weil – im Gegensatz zur Kommunikation via E-Mail, wo die Absender-Adresse als primäre Verifikation genutzt wird – lediglich ein Profilbild genutzt wird, mit oftmals erheblichen Folgen für Betroffene.

Die Erstellung eines Fake-Profils ist für die Cyberkriminellen meist nur der erste Schritt. Der Zweck solch gefälschter Social-Media-Profile ist in vielen Fällen, Support-Anfragen oder Reklamationen argloser Kunden abzugreifen, um an vertrauliche Daten zu gelangen. Zu diesem Zweck geben die Betrüger beispielsweise vor, die Rückabwicklung eines Kaufs in die Wege zu leiten und bitten ihre potenziellen Opfer um ihre Bankverbindung. Sehr beliebt sind auch die Bitten nach den Zugangsdaten zu Online-Portalen der betreffenden Firma, um über diesen Umweg an weitere vertrauliche Daten zu gelangen.

Social-Media-Nachricht vom Chef

Eine weitere Form des digitalen Betrugs via Social Media ist eine Nachricht vom vermeintlichen Chef. Bei dieser Vorgehensweise handelt es sich zwar um klassisches Phishing, jedoch in einem neuen (Social-Media-) Gewand. Analog zu bereits genutzten Betrugsmethoden via E-Mail verwenden Internetbetrüger gefälschte Profile auf sozialen Netzwerken aber auch für eine weitere perfide Angriffsart, die CEO-Betrugsmasche, auch bekannt als Business-Email-Compromise (BEC). Dabei geben sich Online-Kriminelle als Vorgesetzte aus, oftmals CEOs oder CFOs, und versuchen auf diese Weise Mitarbeiter aus den Finanzabteilungen dazu zu bewegen, einen Geldbetrag zu überweisen. Dies selbstverständlich auf ein von den Betrügern verwaltetes Konto, von dem aus das ergaunerte Geld oftmals in Steueroasen verschoben wird und somit unwiederbringlich verloren ist. Bekannte Fälle sind hier beispielsweise der italienische Erstligist Lazio Rom [1] oder der deutsche Automobilzulieferer Leonie [2]. Während diese Vorgehensweise durch gefälschte E-Mails seit längerem bekannt ist und Mitarbeiter in Finanzabteilungen im besten Fall regelmäßig für derartige Betrugsversuche sensibilisiert werden, ist die Vorsicht beim Umgang mit sozialen Medien oftmals weit weniger stark ausgeprägt. Genau das machen sich Kriminelle zunutze.

Zudem sind besonders große Firmen und international bekannte Marken von einer weiteren bei Cyberkriminellen sehr beliebten Vorgehensweise bedroht. Immer häufiger lässt sich die betrügerische Registrierung von Internet-Domains beobachten, deren Domainnamen einen Bezug zu bekannten Firmen oder Marken aufweisen. Ähnlich der gefälschten Social-Media-Profile wandeln Online-Kriminelle die Schreibweise lediglich um Nuancen ab. Auf diese Weise wird der Eindruck erweckt, es handle sich um eine offizielle Domain. Dabei kann die Anzahl von betrügerischen Domains die Anzahl der tatsächlich mit dem Unternehmen in Verbindung stehenden Domains um das 20-fache übersteigen. Diese Beobachtung wird auch durch die Studie „The Human Factor 2018“ des US-amerikanischen Cybersecurity-Unternehmens Proofpoint bestätigt [3].

Mitunter werden aber nicht nur Domains in Verbindung mit großen Firmen oder bekannten Marken registriert. Selbst die Betreiber von illegalen Streaming-Portalen wie Kino.to sind von diesem Phänomen betroffen. Hier spielt besonders das gesteigerte Interesse an Krypto-Währungen wie Monero, Ethereum oder Bitcoin. Die starken Kursschwankungen des Cybergeldes gegen harte Währungen sind dabei kein Hindernis. Denn für Cyberkriminelle wird das Mining, also das Erzeugen von Krypto-Geld, auf jeden Fall ein lukratives Geschäft. Speziell entwickelter Schadcode erlaubt es Kriminellen, das Mining direkt im Browser der Opfer auszuführen, solange diese auf einer präparierten Webseite verweilen. Daher werden oftmals raubkopierte Inhalte angeboten, vorwiegend Video-Streams, damit mögliche Opfer diese Webseite besonders lange im Browser geöffnet lassen.

Cyberkriminelle gehen mit der Zeit

Die Erfahrungen der letzten Jahre zeigen, dass Betrüger und sonstige Kriminelle sich sehr schnell an neueste Trends und Entwicklungen der digitalen Welt und des dortigen Anwenderverhaltens anpassen. Viele dieser neuen Bedrohungen zielen auf den Nutzer mit seinen natürlichen Schwächen als Einfallstor für den Angriff ab, anstatt mit viel Aufwand und vor allem großem technischen Know-how neue Sicherheitslücken zu finden. Was liegt da für Kriminelle näher, als die Gutgläubigkeit von Menschen auszunutzen?

Entsprechend sind neben Software-basierten Schutzmechanismen auch regelmäßige Mitarbeiterschulungen und Informationen über die neuesten Cyberbedrohungen für Unternehmen von elementarer Bedeutung, wenn es darum geht, Kunden und Mitarbeiter vor Kriminellen zu schützen. Damit werden nicht nur finanzielle Risiken für die Organisation abgewendet, sondern auch ein möglicherweise drohender Reputationsverlust.

Werner Thalmeier

Referenzen: **[1]** https://www.thesun.co.uk/sport/football/5921587/lazio-email-scam-hackers-stefan-de-vrij/ **[2]** http://www.manager-magazin.de/unternehmen/autoindustrie/autozulieferer-leoni-um-40-millionen-betrogen-a-1107998.html **[3]** https://www.proofpoint.com/us/human-factor-2018

Karl-Otto Feger, Referatsleiter, CISO

Karl-Otto Feger, Referatsleiter für Informations- und Cybersicherheit im Sächsischen Staatsministerium des Innern, das Projekt „HoneySens“ initiiert.

Mit zunehmender Digitalisierung nimmt auch die Cyberkriminalität neue Ausmaße an. Nicht nur die Menge der Attacken steigt an, auch einzelne Cyberangriffe häufen sich und haben oft weitreichendere Auswirkungen wie Systemausfälle, Datenverluste und Datendiebstähle zur Folge. Behörden wie die Sächsische Landesverwaltung stellen als Ziel von Cyberattacken hier keine Ausnahme dar. So hat sich die Anzahl der Hacker-Angriffe auf das Sächsische Verwaltungsnetz 2017 im Vergleich zum Vorjahr um fast 30 Prozent auf über 1.800 erhöht. Gleiches gilt für die per E-Mail versandten Schadprogramme: Denn in 31 Millionen angenommenen E-Mails wurden mehr als 36.000 Malware-Programme gefunden.

Um Hacker künftig schneller aufzuspüren und unschädlich zu machen, baute der Freistaat Sachsen eine leistungsfähige Infrastruktur für die Informationssicherheit auf. Dabei verfügt das Sächsische Verwaltungsnetz mit insgesamt 80.000 PC-Arbeitsplätzen in der Landes- und Kommunalverwaltung sowie 1.600 angeschlossenen Schulen und 28 weiteren Unternetzen über eine Besonderheit: eine Hackerfalle namens „HoneySens“. Das Sächsische Staatsministerium des Innern, das für die Informationssicherheit der Landesverwaltung verantwortlich ist, hat diese IT-Sicherheitslösung gemeinsam mit der Technischen Universität Dresden entwickelt und durch T-Systems Multimedia Solutions in die Praxis überführt. Die System HoneySens simuliert dabei Datenquellen, um Cyberangreifer anzulocken und Rückschlüsse auf ihre Methoden ziehen zu können. Durch diese Lösung konnte die Sicherheit des Verwaltungsnetzes deutlich erhöht werden.

HoneySens lockt Hacker in die Falle

Der Begriff „HoneySens“ setzt sich aus den Wörtern „Honeypot“ und „Sensor“ zusammen. Die Software täuscht über Sensoren im Netz verwundbare Punkte, die sogenannten „Honigtöpfe“ vor, welche für die Hacker besonders attraktiv sind. Die Hackerfallen dokumentieren bei einem Zugriff auf diese vermeintlichen Datenquellen wichtige Datenströme und übermitteln diese an einen zentralen Server zur Prüfung und Alarmierung des Administrators weiter. Durch den Einsatz der benutzerfreundlichen, wartungsarmen Webanwendung können Angriffe in Echtzeit bemerkt, der Ursprung des Angriffs identifiziert und entsprechende Gegenmaßnahmen sofort eingeleitet werden. Mithilfe der „Honigtöpfe“ konnten bereits wichtige Informationen über Angreifer gewonnen werden, die dazu dienen, das gesamte IT-System fortlaufend gegen Cyber-Attacken von außen besser zu schützen.

Hacker in der „Honigfalle“

Hackerangriffe auf die Datennetze von Behörden und Unternehmen nehmen deutlich zu. Um auf diese Gefahr rechtzeitig reagieren zu können, hat

Keine Chance für Netzwerk-Schnüffler
Die Honigfallen stellen für die Sächsische Landesverwaltung eine preiswerte und leicht administrierbare Möglichkeit dar, Angriffsmuster und die aktuellen Methoden der Cyberkriminellen „am lebenden Objekt“ kennenzulernen und ihnen gleichzeitig effektiv entgegenzuwirken. Der Einsatz von HoneySens bedarf nur wenige Ressourcen, um die Informationssicherheit innerhalb kürzester Zeit deutlich zu erhöhen. Gemeinsam mit weiteren Maßnahmen zur IT-Sicherheit und Mitarbeiterschulungen konnte so ein hohes Maß an Sicherheit geschaffen werden. Das Risiko von Datenverlusten und Datendiebstählen kann auf diese Weise deutlich minimiert werden. Gleichzeitig wird die Arbeits- und Handlungsfähigkeit der Landesverwaltung sichergestellt.

Ein weiterer Vorteil von HoneySens ist, dass es sich um eine kostengünstige As-a-Service-Lösung handelt. Damit wird die Sicherheitssoftware auch für kleinere Behörden und Unternehmen interessant.

Karl-Otto Feger

Mit Managed Security Services gegen Cyber-Angriffe

2017 war kein gutes Jahr für die Cybersecurity. Krypto-Trojaner wie Wanna Cry, Petna und Bad Rabbit richteten massive Schäden in Unternehmen und öffentlichen Einrichtungen an, und mit der Verwendung von IoT-Systemen für Botnetze – beispielsweise IoT_reaper oder IoTroop – haben sich neue Angriffsmuster etabliert. Entspannung ist nicht in Sicht, im Gegenteil: Cyber-Attacken begleiten die IT als ein ebenso lästiger wie gefährlicher Schatten.

Frank Reiländer, Head of Cybersecurity, CGI Deutschland Ltd. & Co. KG

Früherkennung und schnelle Analyse von konkreten Bedrohungen und von mehr oder weniger abstrakten Risiken sind daher für alle Unternehmen von essentieller Bedeutung. Das ist mittlerweile zwar allgemein bekannt, in der Praxis fehlen aber meist die personellen und technischen Ressourcen. Besonders kleinere und mittlere Firmen verfügen nicht über ausreichend IT-Security-Know-how, um ein eigenes Security Operation Center (SOC) aufzubauen, es ständig mit aktuellen Sicherheitstechnologien auszustatten und es auch noch rund um die Uhr zu betreiben.

Dennoch kommen Unternehmen um den Einsatz einer wirksamen und zuverlässigen Security-Lösung nicht herum. Sie müssen nicht nur eigene Sicherheitsbedürfnisse und Compliance-Vorgaben abdecken, sondern auch gesetzliche Vorschriften erfüllen, die sich unter anderem aus dem IT-Sicherheitsgesetz und der EU-Datenschutzgrundverordnung ergeben.

Aus dem Dilemma zwischen hohen Anforderungen und unzureichenden Ressourcen helfen die Managed Security Services (MSS) eines SOC-Spezialisten. Sie bieten unabhängig von eigenen Ressourcen einen maximalen Schutz vor Cyber-Bedrohungen und erlauben es, Risiken proaktiv und effizient zu managen.

MSS sind ein ganzheitliches Lösungskonzept, welches das gesamte Spektrum von End-to-End-Sicherheitsservices abdeckt. Es umfasst das Infrastruktur-Management, mit Teilbereichen wie Device-Management, oder Change-Management, und die Sicherheitsanalyse, das Monitoring und das Reporting mit daraus abgeleiteten Handlungsempfehlungen. Die MSS eines SOC umfassen die Überwachung und Analyse der aktuellen Bedrohungslandschaft, Risikomanagement sowie ein breites Spektrum von IT-Sicherheitsdienstleistungen. Dazu gehören unter anderem Virenschutz, E-Mail-, Netzwerk- und Firewall-Sicherheit, Remote Access, Identitäts- und Zugriffsmanagement, Endgeräte-Sicherheit und der Einsatz von Verschlüsselung. Mit einem SOC-Service können Unternehmen zwar nicht den Angriff aufhalten, aber doch die durchschnittliche Zeit bis zur Entdeckung eines Angriffs von rund 200 Tagen auf wenige Stunden und so die Risiken auf jeden Fall stark reduzieren.

MSS zählt zu den zentralen Leistungen, die CGI Unternehmen und Behörden zur Verfügung stellt. In den acht vernetzten SOCs, die CGI weltweit betreibt, werden jeden Monat hunderte Millionen Cyber-An-griffe erfasst und analysiert. CGI kennt damit stets die akute Bedrohungslage weltweit und kann Unternehmen mit in zahlreichen Projekten bewährten Verfahren und mit Sofortmaßnahmen bei verdächtigen Aktivitäten optimal beraten und schützen. MSS bietet allen Unternehmen, unabhängig von den verfügbaren Ressourcen, Cybersecurity auf höchstem Niveau.

Frank Reiländer

Kryptografische Verfahren bei Frankiermaschinen

Kryptografie spielt in der Cyber-Security eine wichtige Rolle. Spätestens seit den Enthüllungen durch Edward Snowden im Zuge der NSA-Affäre ist die Verschlüsselung sensibler Daten auch weiten Teilen der Bevölkerung ein Begriff. Ein anderer Einsatzbereich für kryptografische Verfahren ist kaum bekannt: der Fälschungsschutz von Frankiermaschinen.

Beim Thema verschlüsselte Nachrichten denken die meisten an WhatsApp, E-Mails und Co. Aber auch bei der Frankierung herkömmlicher Postsendungen wie Briefen spielt Verschlüsselung eine wichtige Rolle. Mithilfe von Frankiermaschinen wie denen von Francotyp-Postalia (FP) können Unternehmen eigenständig Porto auf ihre Briefpost drucken. Um sicherzustellen, dass die Frankiermaschinen nicht manipuliert werden, sichern kryptografische Verfahren diverse Prozesse ab. FP, der Spezialist für sicheres Mail-Business und digitale Kommunikationsprozesse, präsentiert inzwischen ein IoT Secure Edge Gateway auf der Basis firmeneigener Komponenten. Mit diesem Gateway können auch Industrieanlagen genauso wie Frankiermaschinen ihre sensiblen Daten sicher übertragen. Weltweit sind 200.000 Frankiermaschinen von FP im Einsatz, die jährlich Porto im Wert von über 1,2 Milliarden Euro drucken.

Funktionsweise der Frankiermaschine
Um eigenständig Briefsendungen zu frankieren, verwalten in Deutschland die DPAG und FP die Bonität des Kunden und stellen einen bestimmten Geldbetrag auf seinem Kunden-Account im FP-Datenzentrum ein. Von diesem Account wird ein Portokontingent auf die Frankiermaschine des Kunden geladen, das in einem speziell geschützten Sicherheitsmodul im Gerät gespeichert wird. Die DPAG zieht dieses Porto per Lastschrift vom Kunden wieder ein. Damit der Geldtransfer zwischen Kunden-Account und Frankiermaschine gegen Angriffe von außen geschützt ist, ist die Sicherung kryptografisch verschlüsselt. Der Kunde druckt mithilfe der Frankiermaschine den gewünschten Briefmarkenwert auf die Postsendung und das entsprechende Porto wird vom Betrag, der auf dem Sicherheitsmodul gespeichert ist, abgezogen.

Von symmetrischen zu asymmetrischen Verschlüsselungsalgorithmen
Schon seit den 1980er Jahren setzt FP Kryptografie ein. Diese hat in den vergangenen Jahrzehnten einen steten Wandel erlebt. Im Behördenumfeld wie auch in der Industrie setzte sich zunächst der Data Encryption Standard (DES) durch. Bei diesem symmetrischen Verfahren wird nur ein einziger Schlüssel genutzt, der Informationen sowohl ver- als auch entschlüsseln kann. Der Anwendungsbereich des DES-Algorithmus beschränkte sich damals bei den Frankiermaschinen auf den Geldtransfer vom Kunden-Account im FP-Datenzentrum in die Frankiermaschine sowie den Integritätsschutz von in der Maschine gespeicherten Daten. In den späten 1990er Jahren führte FP ihre erste Public-Key-Infrastruktur ein, ein asymmetrisches Verfahren der Kryptografie. Bei diesem System besteht ein Schlüssel aus einem Schlüsselpaar, einem öffentlichen und einem privaten Teil. Je nach Algorithmus können Daten verschlüsselt oder signiert werden.

Schutz der Daten im Hardware-Sicherheitsmodul
Im Zuge der Einführung der Public-Key-Infrastruktur wurde in die Frankiermaschinen in Form des Hardware-Sicherheitsmoduls (HSM) eine neue Komponente verbaut. Das HSM bietet Speicherplatz für Software, Schlüssel und Informationen wie den aktuellen Stand der Zähl-Variable und des Portokontingents. Diese Daten sind durch asymmetrische kryptografische Maßnahmen gesichert und zusätzlich vor sogenannten physikalischen Angriffen geschützt. Mit dem HMS erhält jedes Gerät zudem eine weltweit eindeutige kryptografische Identität, sein eigenes Schlüsselpaar und wird aufgrund kryptografischer Protokolle als autorisiertes FP-Produkt in den Datenzentralen erkannt. Diese Grundeigenschaft wird heute von jedem IoT Device erwartet, welches sensible Daten erfasst und bereitstellt.

Kryptografie in Barcodes
In vielen Ländern setzen die Postbehörden inzwischen einen zweidimensionalen Barcode ein. In diesem Barcode werden Informationen in zwei Richtungen kodiert und so eine höhere Informationsdichte pro Fläche im Vergleich zu einem linearen Strichcode erzielt. So enthält der Portoaufdruck neben dem lesbaren Teil, wie beispielsweise dem Portowert, auch einen digital kodierten Teil. Dieser umfasst unter anderem Informationen zur Identifikation der Frankiermaschine, eine Zähl-Variable des bereits gedruckten Portos sowie eine digitale Signatur. Diese garantiert die Einzigartigkeit und Fälschungssicherheit des Portoabdrucks. Die Postbehörden können durch Nutzung des öffentlichen Schlüssels verifizieren, ob der abgerechnete Portobetrag korrekt ist und von einer zugelassenen Maschine gedruckt wurde. Ein solches Verfahren ist in Deutschland seit 2004 mit dem Frankit-Abdruck im Einsatz.

Dirk Rosenau, Release-Management, Postal Relations und Kryptomodule, FP

Regelmäßige Überprüfung der Frankiermaschine
Um die Integrität der Software und damit die korrekte Ausführung des Gerätes sicherzustellen, wird nach dem Einschalten ein Secure-Boot-Prozess durchgeführt. Jede Softwarekomponente ist mit einer Signatur versehen. Beim Starten des Systems werden alle zur Ausführung benötigten Softwarekomponenten mit Hilfe von Signaturverifikationen auf Manipulation geprüft. Nur bei korrekter Signatur wird das Gerät gestartet und kann benutzt werden. Auf diese Weise stellt FP sicher, dass nur von FP und den Zulassungsstellen autorisierte Software zum Einsatz kommt.

Eine weitere Methode, bei der die Kryptografie zur Prüfung genutzt wird, ist das regelmäßige Auditieren. Hierbei meldet sich die Maschine beim Hersteller und weist ihre korrekte Funktionsfähigkeit nach, indem sie Informationen wie den Portoverbrauch oder den Betriebszustand der Maschine zur automatischen Verifikation an FP schickt. Meldet sich das Gerät in einem festgelegten Zeitraum nicht,

stellt es automatisch den Betrieb ein. Diese regelmäßig durchgeführten Audits verhindern Fälschungen und Manipulationen am Gerät.

Die Einsatzbereiche auf einen Blick
Mithilfe von Kryptografie sichert Francotyp-Postalia inzwischen sämtliche Dienste ab. Im Geschäftsfeld Frankieren setzt FP die Verschlüsselung in folgenden Bereichen ein:

- Beim Geldtransfer zwischen Kunden-Account und Frankiermaschine. So stellt FP sicher, dass die Kommunikation zwischen Datenzentrum und Gerät nicht manipuliert werden kann.
- Innerhalb des Hardware-Sicherheitsmoduls. Hier sind sämtliche Informationen integritätsgeschützt abgespeichert und sicherheitskritische Daten zusätzlich verschlüsselt.
- Bei der Erstellung des zweidimensionalen Barcodes des Portoaufdrucks. Dieser enthält neben dem lesbaren Teil auch einen digital kodierten und maschinenlesbaren Teil, der weitere Informationen wie z.B. eine digitale Signatur oder andere integritätssichernde Daten umfasst.
- Bei dem Secure-Boot-Prozess, um die Ausführung von zugelassener Software zu garantieren.
- Beim regelmäßigen Audit. Die Frankiermaschine weist durch verschlüsselte Datenübermittlung die korrekte Funktionsfähigkeit beim Hersteller nach.

Dirk Rosenau

1.4 SICHERHEIT IN DER CLOUD

Astrid Mehrtens-Haupt, Sales- & Channel Direktorin EMEA, Cogeco Peer 1

Wo die Reise hingeht – So rasant ändert sich die Cloud-Landschaft

Entstehung und Entwicklung der Cloud
Das Konzept des Cloud Computings entstand Ende der Siebziger Jahre, als die Virtualisierung und die gemeinsame Nutzung von Serverressourcen erfunden wurden. In den Neunzigern wurde das Konzept weiterentwickelt und es entstand die Forderung, dass Unternehmensanwendungen ohne komplexe Installationen einfach „im Web“ laufen sollten. Die Idee dahinter: Mitarbeiter sollten einen schnelleren und einfacheren Zugang zu Software-Upgrades und -Updates haben. Unternehmen wie Salesforce, Oracle und NetSuite waren die ersten, die diese Vorteile erkannten. Unsicherheiten und Ängste, die dieses neue Software-Modell mit sich brachte, kreisten um die Fragen, wo die Daten vorgehalten werden, wer Zugriff darauf hat, wie sich geschäftliche Kontinuität damit gewährleisten lässt und ob diese Plattformen überhaupt vertrauenswürdig sind.

Verbesserungen in der Netzwerktechnologie führten zu einer zunehmenden Verbreitung und zu mehr Vertrauen in das Cloud Computing. Die erste Welle, die Virtualisierung der Server, wurde weitestgehend von allen Unternehmen angenommen. Im nächsten Schritt begannen ehrgeizige CIOs damit, alles in die öffentliche Cloud zu schieben. In der Folge entwickelte sich das Cloud-Geschäftsmodell in drei Richtungen, bzw. Kategorien: Infrastructure-as-a-Service, Software-as-a-Service und Platform-as-a-Service.

„Cloud Hype“ 2017
Jede neue Technologie tritt mit dem Anspruch an, alle Probleme zu lösen, bis man feststellt, dass dies nicht der Fall ist. Tatsächlich bedeutet „neu“ etwas Zusätzliches zu dem, was bereits vorhanden ist. Während der „Hype“-Phase des Cloud Computings wurden entsprechend falsche Hoffnungen geweckt, nämlich dass der Wechsel in die Cloud eine kostengünstigere Lösung sei. Fehlende Expertise und Investitionen beim Aufsetzen einer Cloud-Strategie führten zu zahlreichen Fehlentscheidungen.

Einige Unternehmen, die auf eine Strategie des „alles aus der Cloud“ setzten, haben mittlerweile einen Rückzieher gemacht. Andere Organisationen dagegen planen, erhebliche Teile ihrer Assets in die Cloud zu setzen. Doch nur wenige haben ihre ehrgeizigen Ziele bislang erreicht, und die privaten Clouds, Colocation und Hosted Services sind lediglich Teil ihres Mixes geblieben.

Die öffentliche Cloud ist für “spritzige” Webanwendungen gut geeignet, doch für solide Fachanwendungen, die mit allen anderen Systemen integriert sein müssen, sind Inhouse- oder gehostete Lösungen die bessere Wahl. Einige der großen Anbieter führen, um ihren Umsatz zu erhöhen, immer wieder die Kosten von SaaS an. Sie bringen aber auch das Argument, dass die IaaS-Technologie anbieterunabhängig sei.

Cloud als Geschäfts-Tool
Nachdem das Thema „Cloud” geklärt und ein besseres Verständnis dafür geweckt war, verschob sich das Wertversprechen der Cloud für IT- und Geschäftsführer vom Preis auf das Geschäftsergebnis. Es ging dabei um Kundenerwartungen und wie die Vorteile der Cloud dazu genutzt werden können, um diese Erwartungen zu erfüllen oder gar zu übertreffen. Unternehmen betrachten das Wertangebot der Cloud für jede einzelne Anwendung separat: Was funktioniert wo am besten, wie erreicht man die beste Performance, welches sind Netzwerkanforderungen, wie sieht das Risiko aus, ist der Cloud-Anbieter ein Konkurrent, oder könnte er einer werden? Die Agilität und Flexibilität der Cloud unterstreicht ihre Eignung als mächtiges Geschäfts-Tool, doch sind Kontrolle, Sichtbarkeit und Management entscheidend, wenn es darum geht, ihr Potenzial auszuschöpfen.

Die Cloud wird dafür eingesetzt, um Innovationen sofort zu liefern, denn die dazu benötigten Fähigkeiten stehen bei Bedarf zur Verfügung, anders als beim traditionellen Modell. Hier müssen erst Investitionen in den Kauf von Infrastruktur getätigt werden und die Infrastruktur muss erst aufgebaut werden, bevor sie für die Zufriedenstellung von Kunden genutzt werden kann. Die Cloud kann privat oder öffentlich sein. Die private eignet sich besser für vorhersehbare Workloads mit Spitzen und Einbrüchen und einem Geschäftsmodell rund um Verbrauchswirtschaftlichkeit. Unternehmen sollten sich die folgende Frage stellen: Wie viel Zeit benötigt die IT-Abteilung, um eine VM zu provisionieren und bereitzustellen. Wer die entsprechenden Metriken eingibt wird sehen, ob sich sein Business Case in der Cloud lohnt.

Blick in die Glaskugel - Vorhersagen für die nächsten 5 - 10 Jahre
Klar ist, die Cloud-Kriege um Details sind vorbei: Die Zukunft heißt hybrid und Multi-Cloud. Hybrid-Lösungen sollten bedeuten, dass Workloads automatisch in die nächste, am besten optimierte, kosteneffiziente Umgebung gehen. Die Grundlage bilden der Leistungsbedarf, Sicherheitsfragen, der Speicherort der Daten, Charakteristiken der Anwendungs-Workloads, sowie der Bedarf der Endanwender. Im Einzelfall kann die Lösung in der öffentlichen oder auch in der privaten Cloud liegen, bei On-Premise oder gar einer Mischung aus allem.

Dazu bedarf es einer Überarbeitung der Anwendungsarchitektur. Sie muss von dem klassischen Dreiebenen- zum ereignisgetriebenen Modell wechseln. Cloud-Anbieter drängen deshalb auf den breiteren Einsatz von Cloud-nativen Applikationen. Während Unternehmen weiter dazu übergehen, öffentliche Clouds in Hyper-Größe zu nutzen, greifen Cloud-Anbieter auf On-premise-Datencenter zurück. Microsoft hingegen wird über Azure Stack und VMWare die wiederum die öffentliche Cloud stürmen. Dieser Trend wird sich in den nächsten fünf bis zehn Jahren noch verstärken.

Astrid Mehrtens-Haupt

Eine sichere Cloud-Plattform als Basis für die Smart Factory

„Smart Factory“ – dabei denkt man an intelligent vernetzte Anlagen, die miteinander kommunizieren; an Systeme, die selbstständig Daten erheben, austauschen und auswerten, die lernen, Entscheidungen zu treffen und bis zum fertigen Produkt alle nötigen Schritte selbst zu steuern. Je mehr Daten den vernetzten Systemen zur Verfügung stehen, umso schneller lernen sie und umso besser werden die Ergebnisse.

Doch digitale Daten sind nicht nur der Treibstoff, der die Digitalisierung und maschinelles Lernen voranbringt, sie sind auch eine unserer wertvollsten – und somit schützenswertesten – Ressourcen. Das gilt nicht nur für personenbezogene Daten, für deren Gewinnung und Verarbeitung der Gesetzgeber ohnehin besonders strenge Vorgaben macht (Stichwort: DSGVO), sondern auch für Firmengeheimnisse, Leistungskennzahlen (KPIs) und andere Interna.

Hemmt der Datenschutz die Digitalisierung?
Die Folge: Viele Unternehmen sind lieber vorsichtig und gehen tendenziell eher sparsam mit ihren Daten um. Zu groß ist die Angst vor Datenverlust – und zu gering ist das Vertrauen in vorhandene IT-Infrastrukturen, als dass man diesen massenhaft kritische Daten anvertrauen könnte.

Man ist sich einig: Für geschützten Datenaustausch, rechtskonforme Big-Data-Analysen und sichere Machine-to-Machine-Anwendungen braucht es eine geeignete Plattform, die vollen Datenschutz und volle Datensicherheit gewährleisten kann. Zugriffsrechte und Anonymisierung müssen klar geregelt sein – und der Unsicherheitsfaktor Mensch muss ausgeschlossen werden.

Doch wie kriegt man das eigene Rechenzentrum sicher? Sind Public-Cloud-Dienste oder Peer-to-Peer-Netzwerke eine Lösung? Oder müssen externe Sicherheitsexperten ran?

Probleme konventioneller Technologien
Tatsache ist: Herkömmliche Cloud-Infrastrukturen bieten für Internet-of-Things- und Industrie-4.0-Angebote nicht das nötige Maß an Sicherheit. Denn hier besteht grundsätzlich die Möglichkeit eines unbefugten Zugriffs, beispielsweise durch den Backend-Betreiber oder sein Personal. Peer-to-Peer-Netzwerke wiederum können zwar oft mit der nötigen Sicherheit aufwarten, sind aber im Gegensatz zu Cloud-Lösungen nicht beliebig skalierbar, was sie für einen Einsatz in der Smart Factory ungeeignet macht.

Eine versiegelte Plattform für sicherheitskritische Anwendungen
Mit der Sealed Platform haben Unternehmen nun ein hochsicheres Werkzeug für sicherheitskritische Cloud-Applikationen an der Hand, das diesen hohen Anforderungen genügt. Entwickelt wurde die Cloud-Plattform von Uniscon, einem Münchner Cloud-Security-Anbieter und TÜV-SÜD-Tochter, dessen versiegelte Cloud-Server bereits in den Rechenzentren der Deutschen Telekom stehen „Die Sealed Platform kombiniert die Vorteile einer Public Cloud mit einer Sicherheit, die jene einer privaten

Cloud noch übertrifft“, erklärt Uniscon-Mitgründer und -CTO Dr. Hubert Jäger. „Sie kann für alle Arten von Anwendungen und Betriebssystemen genutzt werden und fungiert somit als Enabler für rechts- und datenschutzkonforme SaaS , IoT-, und Industrie-4.0-Angebote.“

Anwendungen, die auf der Sealed Platform laufen, sind so sicher, dass selbst privilegierter Zugriff im Rechenzentrum oder auf Applikationsebene durch den Admin technisch ausgeschlossen ist. Es gibt heute schon eine Reihe von Anwendungen, die produktiv auf dieser Technologie laufen wie zum Besipiel:

- Big-Data-Analysen
- Dokumentenmanagement
- Apps, die personenbezogene Daten verarbeiten

Sealed Platform eignet sich für Applikationen, die einen besonders hohen Schutzbedarf haben. Dazu gehören Smart-Factory-Anwendungen wie Industrial Data Space - ein „Raum“ für den Austausch und die rechtskonforme Analyse von Daten. Genauso laufen aber auch Big Data Analyse-Software oder virtuelle Datenräume wie der KPI Data Space der TÜV-SÜD-Tochter Advimo darauf.

Bei letzterem handelt es sich um einen sicheren und rechtskonformen Datenraum speziell für den Austausch von KPIs über die Unternehmensgrenzen hinaus: Unternehmen laden ihre Kennzahlen – etwa Umsatz- oder Wartungsinformationen – in den Datenraum, wo diese automatisch anonymisiert und anschließend wieder zur Verfügung gestellt werden. So können Unternehmen die Kosten- und Nutzen-KPIs für vorbeugende Wartung (Preventive Maintenance) und vorausschauende Wartung (Predictive Maintenance) pro Jahr direkt miteinander vergleichen. In der Folge lassen sich Wartungszyklen optimieren und Kosten einsparen. Ein unbefugter Datenzugriff – auch durch andere Unternehmen im selben Datenraum – ist technisch ausgeschlossen, unternehmensinterne Informationen und personenbezogene Daten sind somit zuverlässig geschützt.

Dr. Ralf Rieken, COO, Uniscon GMBH

Rechtskonforme Datenverarbeitung

So lassen sich auf Basis einer sicheren und technisch gekapselten Cloud-Plattform wie der Sealed Platform auch digitale Geschäftsmodelle realisieren, die sonst wegen berechtigter Datenschutzbedenken oder strenger gesetzlicher Auflagen nicht umsetzbar wären.

Unternehmen wollen die Digitalisierung, und zwar möglichst ohne Kompromisse. Mit einer sicheren Cloud-Plattform lässt sich zumindest die Frage nach Datenschutz und Datensicherheit zufriedenstellend beantworten. Rein technisch steht der smarten Fabrik somit nichts mehr im Wege.

Dr. Ralf Rieken

Die Globalisierung erfordert die Transformation zur Cloud-Firewall

Das Implementieren, Patchen, Updaten, Upgraden und Verwalten von Hardware-Firewalls ist kostspielig, komplex und zudem anfällig. International tätige Unternehmen neigen daher zunehmend dazu Cloud-basierte Firewalls einzusetzen, die die Nutzerstandorte übergreifend integrieren, den Verwaltungsprozess vermindern und die gesamte Netzwerk-Sicherheit gewährleisten.

Zwei gängige Modelle an virtuellen Firewall lassen sich unterscheiden. Einerseits wird die Hardware-Firewall, auf der verschiedene virtuelle Instanzen betrieben werden können, zu einem Service Provider verlagert. Das zweite Ansatz wird bei einem Cloud-Anbieter vorgehalten.

Im ersten Modell stellt ein Service Provider eine Managed Firewall zur Verfügung. Nach wie vor kommt Hardware zum Einsatz, deren virtuelle Instanzen nicht nur betrieben, sondern auch gewartet oder aktualisiert werden müssen. Der Aufwand dafür wird allerdings an den Provider ausgelagert. Dieser kann limitiert durch die Kapazität der vorgehaltenen Hardware eine begrenzte Anzahl an Kunden per Firewall hosten.

Bei der Wahl einer Managed Firewall muss die Anzahl der Standorte berücksichtigt werden, an dem gehostete Firewalls zur Verfügung stehen. In aller Regel wird diese durch abgedeckte Geolocations begrenzt sein. Unternehmen müssen sich entscheiden, ob es mit Einschränkungen einhergeht, wenn der Anbieter seine Hardware beispielsweise nur an drei oder sechs Standorten vorhält. Es gilt das Angebot an Lokationen mit den Anforderungen abzugleichen, denn gerade im Bereich der Firewall ist es für viele Services wichtig, dass lokale IP-Adressen zur Verfügung stehen. Ein Beispiel: Wenn ein Unternehmen in Brasilien eine Niederlassung hat, ist für den Zoll eine brasilianische IP-Adresse erforderlich. Weniger Lokationen bedeuten in der Regel auch längere Wege und damit geringe Geschwindigkeit.

Die Systemkomplexität gibt den Ausschlag

Im zweiten Modell der „virtuelle Firewall“ ist die Hardware bei einem Cloud-Provider gehostet. Auch hier steht der Servicegedanke für den Kunden im Mittelpunkt. Ein Amazon-Kunde kann relativ schnell einen Firewall-Service über diesen Dienst aufsetzen und monatlich bezahlen. Auch hier muss geprüft werden, wie es sich mit der Anzahl an angebotenen Standorten verhält. Amazon bietet beispielsweise Verfügbarkeitszonen für seine Services an. Das bedeutet, dass Kunden innerhalb einer Georegion, wie einer Stadt, einem Land oder gar Kontinent auf Verfügbarkeitszonen zugreifen und dort gegebenenfalls sogar auf redundante Services bauen kann. Mit einem solchen Ansatz hat ein Unternehmen seine Skalierbarkeit relativ elegant gelöst.

Amazon bietet den Service der virtuellen Firewall als Infrastructure as a Service (IaaS) an. Der Vorteil gegenüber dem Managed Firewall Ansatz ist die größere Anzahl an Rechenzentren und die Möglichkeit der schnellen Implementierung. Außerdem hat der Kunde mehr Kontrolle über die Firewall. Diese Kontrolle erkauft er sich allerdings wieder durch Mehraufwand für die IT-Abteilung in Form von Konfiguration, Updates, Upgrades und Patchen. Je mehr dieser virtuellen Firewalls betrieben werden, desto mehr Ressourcen müssen für die Verwaltung dieser virtuellen Firewalls einkalkuliert werden.

Bei einer Entscheidung für einen Ansatz sollte die Komplexität der Administration berücksichtigt werden. Muss beispielsweise eine Third Party Software eingesetzt werden für die Verwaltung über mehrere Lokationen hinweg und wie werden Policies verwaltet. Können Policies über alle Standorte hinweg in Echtzeit aktualisiert werden, um im Bedarfsfall schnell mit Patches reagieren zu können, ohne dass kritische Sicherheitslücken auftreten? Auch das Logging über mehrere Standorte darf nicht zur administrativen Herausforderung werden. Im Fall des bei AWS gehosteten Firewall-Ansatzes kommt zur Pflege der Logs ein SIEM-Service zum Einsatz, der lizensiert werden muss. Es gilt also bei der Entscheidung für oder gegen einen Ansatz die Systemkomplexität im Auge zu behalten.

Was kann eine echte Cloud-Firewall?

Weder bei einem Managed Firewall-Service oder einer in der Cloud gehosteten virtuellen Firewall kommen die Vorzüge des echten Cloud-Effekts zum Tragen. Im Unterschied zu dem Betrieb der Firewall in einer virtualisierten Umgebung ist bei einer echten Cloud-basierten Firewall der Cloud-Anbieter für Updates, Upgrades, Capacity Planning und Patches verantwortlich. Die Aufgabe des Aufsetzens und der Wartung der Firewall inklusive der Anforderungen an die Skalierbarkeit geht in die Verantwortung des Cloud Providers über. Deshalb sollten die Service Level Agreements mit dem Anbieter genau geprüft werden. Denn nicht nur der Betrieb, sondern ebenfalls das Trouble Shooting wechselt in den Verantwortungsbereich des Service-Anbieters.

Ein Cloud-basierter Ansatz sollte keine Hardware-Komponente mehr enthalten, sondern von Grund auf als Security as a Service aufgesetzt sein. Der Cloud-Anbieter stellt ein voll integriertes User Interface zur Verfügung, das über alle Standorte und Anwender hinweg in Echtzeit integriert ist. Damit kann Real-Time Log Correlation abgedeckt werden, so dass die Komplexität für die Inbetriebnahme, den laufenden Betrieb und das Trouble-Shooting deutlich verringert sind. Echtzeitkontrolle über Policies ist über das User Interface für den Kunden jederzeit möglich.

Fazit

Unternehmen, die nach einer Firewall-Lösung für Standorte suchen, an denen keine Netzwerksegmentierung erforderlich ist, sind mit einer virtuellen oder Cloud-basierten Lösung gut beraten. An Standorten, an denen sie keine eigene Hardware-Infrastruktur vorhalten können, wie Niederlassungen, ist eine Cloud-Firewall gut geeignet, die erforderliche Sicherheit bei stark verringertem Administrationsaufwand zu bieten. Mit einer steigenden globalen Ausbreitung und der damit einhergehenden wachsenden Anzahl an Niederlassungen und Standorten weltweit ist im Zeitalter der Digitalisierung eine echte Cloud-basierte Firewall der adäquate Lösungsansatz.

Mathias Widler

Mathias Widler, Area Director/ General Manager/ EMEA Central, Zscaler

1.5 RISIKEN

Millennials und die Cyberrisiken

Unternehmen rätseln seit rund einem Jahrzehnt darüber, wie sie sich erfolgreich an die Generation der Millennials anpassen können. Unter Millennials versteht man die Generation, die zwischen 1980 bis Mitte der 90ziger geboren wurden.

Die öffentliche Diskussion und zahlreiche Studien vermitteln den Eindruck, als ob es sich um eine ganz andere Spezies handelt, die speziell auf sie abgestimmte Maßnahmen benötigt, um sie ganzheitlich aus Unternehmenssicht zufrieden zu stellen. Unabhängig verschiedener Charakteristika wie etwa die Einstellung zur Arbeit oder die Gestaltung des eigenen Lebens ist eine Erkenntnis nicht von der Hand zu weisen – die Millennials gelten als weitaus technisch versierter als die Generation der Baby Boomer (geboren zwischen 1946 – 1964). Millennials sind mit dem Internet von Anfang an aufgewachsen, wodurch sie auch als Digital Natives bezeichnet werden. Die jüngsten Forschungen haben jedoch gezeigt, dass sie trotz und gerade wegen dieser Tatsache weitaus wahrscheinlicher auf Cyber-Betrug hereinfallen. Die Annahme, dass sie die Grundlagen für mehr Cybersicherheit von Beginn an gelernt hat, wird durch den jüngsten Bericht State of the Phish 2018 von Wombat Security widerlegt: Gerade durch die Selbstverständlichkeit des Internets und den verfügbaren Angeboten ist zu beobachten, dass die jüngere Generation mit dem Thema Cyber-Sicherheit fahrlässig umgeht.

Social Engineering erfolgreichster Angriffsvektor

Während 72 Prozent der befragten Baby Boomer Phishing-Attacken als solche richtig erkannten,

waren es bei den Millennials nur 61 Prozent. Darüber hinaus haben Untersuchungen von Get Safe Online ergeben, dass junge Menschen besonders anfällig für sogenannte „Familien- und Freundesbetrügereien“ sind. Die Vorgehensweise ist bei dieser Art von Attacke denkbar einfach: Betrüger geben sich als Angehörige der Opfer aus, nachdem die Betrüger die Social-Media-Accounts der Angehörigen gehackt haben. Das Ziel der Betrüger ist es, durch geschickte Manipulation und Anfragen an die Opfer diese zur Zahlung eines Geldbetrages zu bewegen. Das Datendienstleistungsunternehmen Experian hat bei einer Untersuchung außerdem festgestellt, dass Menschen von Mitte bis Ende 20 mit einer höheren Wahrscheinlichkeit auf Betrügereien reinfallen, als die Generation 60+. Get Safe Online gibt an, dass es einige Gründe gibt, warum junge Menschen häufiger auf Betrügereien hereinfallen: Zunächst nutzt die jüngere Zielgruppe Online-Angebote wesentlich intensiver, daher bieten sich Betrügern höhere Chancen, die Millennials über verschiedene Kontaktpunkte, zum Beispiel über Email oder Social Media, anzugreifen. Außerdem gehen Millennials davon aus, dass nur ältere Menschen Opfer von Betrügereien werden. Ein weiterer Grund liegt in der Annahme, dass Kriminelle ihre Phishing-Attacken nicht zielgerichtet auf individuelle Personen fahren. Man denke hierbei an die bekannte Betrugsmasche des nigerianischen Prinzen von der einer der Hintermänner kürzlich in den USA verhaftet wurde: Per E-Mail erhält das potentielle Opfer die Benachrichtigung, dass es eine Erbschaft von einem Prinzen aus Nigeria zu erwarten habe. Für die Transaktion fordern die Betrüger den Zugang zum Bankkonto des Opfers oder fordern es auf, für die Abwicklung des Prozesses Gebühren zu entrichten. Solche bekannten Angriffe mögen zunächst bei einer Vielzahl an Empfängern der Millennials keine Beachtung finden, Angriffe mithilfe von Social Engineering wiederum, also die Manipulation der Opfer unter Vortäuschung einer falschen Identität, versprechen eine höhere Erfolgsquote.

Amy Baker, Vice President of Marketing, Wombat Security

Mit zielgruppenspezifischer Weiterbildung zur Cybersicherheit

Diese Ergebnisse zeigen, dass Millennials eine andere Einstellung zum Thema Cybersicherheit haben als ihre Baby-Boomer-Kollegen, da sie unterschiedlich mit der modernen Technologie interagieren. Dies stellt natürlich auch ein Risiko für den betrieblichen Ablauf dar, da Millennials am Arbeitsplatz ein ähnliches Online-Verhalten wie im privaten Umfeld aufweisen dürften. Aus betriebswirtschaftlicher Sicht bedeutet dies daher, dass Unternehmen bei der Konzeption und Durchführung von Weiterbildungsangeboten zur Cybersicherheit eine andere Herangehensweise, gerade hinsichtlich der jüngeren Zielgruppe, in Betracht ziehen sollten.

Regelmäßige Weiterbildung im Bereich Cybersicherheit ist für alle Generationen elementar, aber im Hinblick auf Millennials ist dies der Schlüssel, um unbekümmerte Verhaltensweisen zum Besseren zu verändern. Darüber hinaus sollten Unternehmen sicherstellen, dass die Weiterbildungsangebote die Lebenswirklichkeit der Millennials abdecken. Themen wie die Sicherheit für mobile Geräte und Anwendungen sowie Verhaltensregeln für einen sicheren Umgang mit Social Media und dem Internet im Allgemeinen sollten im Fokus stehen.

Um die jüngere Generation für das Thema Cybersicherheit zu begeistern, sollten die Weiterbildungsangebote interaktiv und klar verständlich sein. Eine Trainingseinheit, die länger als 15 Minuten dauert, birgt die Gefahr in sich, dass die Aufmerksamkeitsspanne wieder nachlässt. Gamification kann hier das Wissen auf eine spielerische Art und Weise der betreffenden Zielgruppe vermitteln.

Abschließend müssen sich Verantwortliche in Unternehmen darüber bewusst sein, dass sie es mit einer Generation zu tun haben, für die die ortsunabhängige Nutzung modernster Technologien zum normalen Lebensalltag gehören. Wahrscheinlich resultiert aus dieser Mentalität eine höhere Produktivität, jedoch sind Unternehmen gut darin beraten, die junge Generation auf die stetig aufkommenden Cyber-Risiken zu sensibilisieren und sie zu einem sicheren Umgang mit der modernen Technologie ganzheitlich zu schulen – und dies am besten bevor Cyberangriffe erfolgreich sind.

Amy Baker

Wie sicher sind Kryptobörsen?

Kryptowährungen sind durch den Kursanstieg von Bitcoin heutzutage in aller Munde, jedoch sind diese oder andere Alternativen wie Etherum oder Litecoin nur in der Theorie vor Diebstahl gesichert. Kryptowährungen funktionieren nach dem gleichen Prinzip wie klassische E-Zahlungssysteme, wie beispielsweise WebMoney oder PayPal. Daher weisen Kryptobörsen auch ähnliche Probleme auf. Vor allem beim Passwortschutz sollten die Plattformen, trotz dezentraler und anonymer Transaktionen, weiter nachrüsten.

Der Passwort-Manager Dashlane veröffentlichte eine Studie, bei der die weltweit beliebten Kryptobörsen auf Passwortrichtlinien geprüft wurden. „Password Power Rankings™ von Kryptowährung-Webseiten“ beinhaltet Untersuchungen von 35 der weltweit beliebtesten Webseiten zum Handeln und Verwalten von Kryptowährungen. Das Ergebnis zeigte, dass Nutzerkonten auf mehr als 70 Prozent dieser Webseiten erheblichen Risiken in Bezug auf Finanzdiebstahl ausgesetzt sind. Der Grund sind unsichere Passwortrichtlinien.

Sicherheitsexperten von Dashlane haben jede Webseite im Hinblick auf fünf entscheidende Passwort- und Kontosicherheits-Kriterien untersucht. Für jedes erfüllte Kriterium erhielt eine Webseite einen Punkt, wobei das Erreichen der Höchstpunktzahl von fünf Punkten Voraussetzung für das Bestehen des Tests war. Jede Punktzahl unter fünf galt als ungenügend und bedeutete, dass die Mindestanforderungen für gute Passwort-Sicherheit nicht erfüllt wurden.

Das Anmelden bei einer Website für Kryptowährungen ist vergleichbar mit dem Eröffnen eines Bankkontos. Solche Seiten speichern die persönlichen Bankkonto- und Kreditkarteninformationen, die Bitcoins und weitere digitale Vermögenswerte. Deshalb ist es entscheidend, dass Ihr Konto in puncto Sicherheit nichts zu wünschen übriglässt. Die Tatsache, dass Nutzer bei den meisten Webseiten unglaublich schwache Passwörter erstellen können, sollte die Alarmglocken in der ganzen Branche klingeln lassen.

Kritische Sicherheitslücken

Trotz des wachsenden Interesses an Kryptowährungen bieten die meisten führenden Webseiten ihren Kunden keine angemessenen Schutzmaßnahmen für Passwort- und Kontosicherheit. Diese unzureichenden Sicherheitsstandards bedeuten eine Gefahr für das Krypto-Vermögen von Tausenden von Nutzern.

1. Gefährliche Passwortanforderungen: Erstaunliche 43 Prozent der geprüften Webseiten erlauben es ihren Nutzern, Konten mit Passwörtern mit sieben oder weniger Zeichen zu erstellen und ganze 34 Prozent erfordern keine alphanumerischen Passwörter. Die Prüfbeauftragten von Dashlane konnten wiederholt Konten mit schwachen Passwörtern wie z. B. „12345“ und „Passwort“ erstellen. In einem Fall reichte sogar der Buchstabe „a“ aus.

Darüber hinaus fand Dashlane heraus, dass weniger als 50 Prozent der Webseiten Benutzern während der Kontoeinrichtung Tools zur Bewertung der Passwortstärke zur Verfügung stellten.

2. Unterdurchschnittliche Sicherheit: Im Vergleich zum Dashlane-Ranking 2017 für führende Verbraucher-Portale schnitten die Krypto-Seiten schlecht ab. Im Rahmen des Rankings von Verbraucher-Webseiten, bei dem Webseiten wie Apple, Zalando, Facebook und PayPal bewertet wurden, erhielten nur 48,8 Prozent eine ungenügende Note. Diese Ergebnisse stehen in starkem Kontrast zu den 71 Prozent an Krypto-Seiten, die unsere Prüfung 2018 nicht bestanden haben.

Obwohl die Branche sich selbst mit Innovation im Bereich der Cybersicherheit rühmt, weisen die meisten Webseiten für Kryptowährungen eine schlechtere Passwort-Sicherheit auf als durchschnittliche Mainstream-Webseiten.

Emmanuel Schalit, CEO, Dashlane

Abb.: Ranking 2018, Dashlane

Best Practices für die Sicherheit von Kryptowährungen
Wenn Nutzer sich bei einer neuen Webseite anmelden, sollte unbedingt zuallererst die Zwei-Faktor-Authentifizierung aktiviert werden. Jede legitime Webseite bietet eine Option für die Zwei-Faktor-Authentifizierung an, und es gibt kein Szenario, in dem dieser Schritt übersprungen werden sollte.

Für Kryptowährungs- und sonstige digitale Konten gibt es ein paar einfache Maßnahmen, die jeder ergreifen sollte, um die eigene Online-Sicherheit zu verbessern:

- Ein einzigartiges Passwort für jedes Online-Konto verwenden.
- Passwörter erstellen, die über das Minimum von acht Zeichen hinausgehen.
- Passwörter mit einer Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen erstellen.
- Passwörter vermeiden, die gängige Begriffe oder Redewendungen, Umgangssprache, Ortsbezeichnungen oder Namen enthalten.
- Einen Passwort-Manager für das Erstellen, Speichern und Verwalten von Passwörtern verwenden.

Methodik
Die Studie wurde von Dashlane zwischen dem 12. und 19. März 2018 durchgeführt. Die Experten bewerteten 35 beliebte Webseiten für Kryptowährungen im Hinblick auf fünf Sicherheitskriterien. Nur Anbieter, die Benutzern erlauben, Konten innerhalb von Browsern zu erstellen, wurden getestet. Solche Webseiten, die das Herunterladen einer Software oder mobilen App erfordern, waren nicht Teil der Untersuchung. Dashlane hat jede Webseite mindestens viermal getestet, um die Genauigkeit der Ergebnisse zu gewährleisten. Eine Website erhielt einen Punkt für jedes erfüllte Kriterium, wobei fünf Punkte die Höchstpunktzahl darstellten. Fünf von fünf Punkten waren außerdem die Voraussetzung, um den Test zu bestehen und die Anforderungen für gute Passwort-Sicherheit zu erfüllen. Das Ranking spiegelt ausschließlich das Sicherheitsniveau jeder Webseite im Hinblick auf Passwort- und Kontoschutz wider. Emmanuel Schalit

Security Information and Event Management – Verdächtiges frühzeitig erkennen

In der IT Security ist Zeit ein wichtiger Faktor. Denn nur wer verdächtige Verhaltensmuster im Unternehmensnetzwerk rechtzeitig erkennt, kann schnell reagieren und größeren Schaden vermeiden. Ein Security Information and Event Management (SIEM) ist dabei eine unverzichtbare Hilfe. Auch für kleinere und mittelständische Unternehmen gibt es geeignete Lösungen.

Unternehmen haben heute eine Vielzahl von Sicherheitssystemen in Betrieb – von Proxies und Firewalls bis Intrusion Prevention and Detection. Sie alle liefern umfangreiche Daten. Ein Security Information and Event Management (SIEM) sammelt diese Log-Dateien in einer zentralen Datenbank. Zusätzlich bezieht es auch Informationen von anderen Netzwerksystemen mit ein, zum Beispiel Server, Switches und Router. Das SIEM kann die gesammelten Daten in Korrelation setzen und auswerten. Dadurch gewinnen Sicherheitsverantwortliche ein ganzheitliches Bild aller Aktivitäten im Netzwerk, können Zusammenhänge erkennen und verdächtige Verhaltensweisen schnell aufdecken.

Analysieren, warnen und Schwachstellen aufdecken
Versucht ein Nutzer zum Beispiel mehrfach vergeblich, sich bei verschiedenen Systemen anzumelden, und ist dann plötzlich erfolgreich, deutet das auf einen Sicherheitsvorfall hin. Auch wenn sich jemand kurz hintereinander von verschiedenen Standorten aus per VPN im Unternehmensnetzwerk einwählt, ist dies verdächtig. Das SIEM erkennt, dass etwas nicht mit rechten Dingen zugehen kann, und schlägt Alarm. Bei entsprechender Konfiguration kann es auch selbst direkt Aktionen durchführen, um das entdeckte Risiko zu mindern – zum Beispiel eine Firewall-Regel ändern.

Ein SIEM konzentriert sich jedoch nicht nur auf die Auswertung von Events. Um auffälliges Nutzerverhalten jederzeit im Blick zu behalten, enthalten viele Lösungen User and Entity Behavior Analytics (UEBA). Sie beobachten und analysieren das Verhalten von Anwendern sowie Endgeräten. Dazu erstellt das SIEM Verhaltensprofile, die etwa Logins, Aktivitäten innerhalb eines Netzwerks oder den Zugriff auf Dateien und Ordner berücksichtigen. Versucht etwa ein Mitarbeiter, sensible Informationen zu versenden, könnte das ein Hinweis auf Datenklau sein. Werden bei einem Endgerät ungewöhnliche Aktivitäten festgestellt, liegt die Vermutung nahe, dass es gehackt wurde – was oft ein Anzeichen für einen Sabotageversuch ist.

Auch bei der rückblickenden Aufklärung von Vorfällen leistet das SIEM wertvolle Hilfe. Anhand der Datenauswertung versetzt es Administratoren in die Lage, genau nachzuvollziehen, was passiert ist. Wurde zum Beispiel ein System kompromittiert, können sie feststellen, welche Aktionen zuvor im Netzwerk abgelaufen sind. Damit lässt sich die Sicherheitsverletzung exakt protokollieren. Gleichzeitig hilft eine solche Analyse dabei, Schwachstellen aufzudecken und mit geeigneten Maßnahmen zu schließen.

Darauf sollten Sie bei einer SIEM-Lösung achten
Ein SIEM ist immer nur so gut wie die Logdateien, die es erhält. Für eine umfassende Darstellung der Sicherheitslage sollte es herstellerübergreifend mit möglichst vielen Systemen kompatibel sein. Vorsicht also bei Lösungen, die nur mit den Produkten des eigenen Herstellers zusammenarbeiten, denn mit ihnen lässt sich lediglich ein Teil der Infrastruktur abdecken. Außerdem sollten Unternehmen darauf achten, dass sich das SIEM einfach administrieren lässt. Bei frei verfügbaren Angeboten ist das häufig nicht der Fall und die Inbetriebnahme wird zur aufwändigen Bastelei.

SIEM-Lösungen haben den Ruf, teuer zu sein. Deshalb leisten sich vorwiegend größere Unternehmen ein solches Sicherheitssystem. Doch auch kleinere Betriebe sollten sich nicht abschrecken lassen. Häufig gibt es die Möglichkeit, die Kosten überschaubar zu halten, indem man zunächst einmal nur wenige wichtige Logquellen auswertet. Denn meist hängen die Preise davon ab, wie viele Loginformationen pro Sekunde verarbeitet werden.

SIEM als Managed Service
Alternativ gibt es auch die Möglichkeit, SIEM bei einem Managed Services Provider als Leistung in Anspruch zu nehmen. Das hat den Vorteil, dass Unternehmen selbst keine Software kaufen müssen. Der Dienstleister stellt diese zur Verfügung und rechnet nach verbrauchten Ressourcen ab. Auch um den Betrieb kümmert er sich. Unternehmen müssen lediglich festlegen, welche Log-Dateien sie auswerten möchten. Dies können sie jeden Monat ganz nach Bedarf ändern. Ein SIEM im Service-Modell ist also für alle Unternehmen empfehlenswert, die Flexibilität wünschen und selbst kein Know-how aufbauen möchten.

Das SIEM wird intelligent
Ein SIEM kann Angriffe zwar nicht verhindern, sie aber frühzeitig aufdecken. Es übernimmt quasi die Funktion eines Feuermelders und schlägt Alarm, wenn es einen „Brand“ entdeckt. Security Verantwortliche können schnell geeignete Maßnahmen ergreifen, bevor größerer Schaden entsteht.

Da ein SIEM die Reaktionszeiten erheblich verkürzt, sollte heute kein Unternehmen mehr darauf verzichten. Künftig wird künstliche Intelligenz zunehmend Einzug in das Security Information and Event Management halten. Solche selbstlernenden Systeme können Gefahren noch schneller erkennen. Erste Lösungen gibt es bereits, zum Beispiel IBM QRadar mit integrierter Watson-Funktionalität oder die TLM-Plattform von LogRhythm mit selbstlernenden Analysefunktionen aus der Cloud. Eike Trapp

Was macht Klickbetrug so attraktiv?

Laut dem Bundesverband für Digitale Wirtschaft (BVDW) e.V. betrug das Nettovolumen für digitale Werbung (Online und Mobile) im letzten Jahr 1,928 Milliarden Euro. Eine lukrative Zeit für Werbetreibende und somit auch für Betrüger. Schaut man sich parallel dazu die aktuellen Marktanalysen zum Anzeigenbetrug, dem sogenannten Ad-Fraud an, wird schnell klar, wie viel von den investierten Werbebudgets nicht optimal eingesetzt werden. Die Ad-Fraud Bekämpfung ist ein ständiges Wettrüsten mit zunehmender Raffinesse und täglich neuen Bot-Netzwerken, da sich die Methoden ständig ändern.

Anzeigenbetrug ist eine Goldgrube
Ad-Fraud ist äußerst risikoarm und bietet gleichzeitig sehr hohe Gewinnchancen. Ein wesentlicher Anreiz sind die hohen Geldbeträge, die sich mit gefälschten Webseiten und Klicks erzielen lassen. Betrüger können potenziell Milliarden einstreichen. Außerdem entfällt bei Ad-Fraud das Problem der Skalierung. Haben Kriminelle es geschafft, Traffic auf einer Fake-Webseite zu generieren und dafür bezahlt zu werden, können sie auf unbestimmte Zeit so weitermachen. Die einzigen Beschränkungen für Betrüger sind die technischen Grenzen ihres Botnets. Zudem ist im Online-Werbebetrug-Sektor das Risiko, bestraft zu werden, relativ gering.

Ad-Fraud wird kaum bestraft
Publisher, Vermarkter, Ad-Networks und Ad-Exchanges, Anbieter von Malware-Anbieter – alle Beteiligten im Prozess der Auslieferung betrügerischen Traffics oder falschen Anzeigen-Impressions sind so verflochten miteinander, dass es beinahe unmöglich ist, die Quellen zu ermitteln. Man vermutet, das Hacker und sogenannte Botnet-Operator vorrangig männlich sind, aus Osteuropa, Russland oder Asien stammen und vor allem aus Gebieten, wo es juristisch fast unmöglich ist, jemanden wegen Anzeigenbetrug zu verurteilen. Ad-Fraud fällt in vielen Ländern in eine rechtliche Grauzone, was die strafrechtliche Verfolgung erheblich erschwert. Es wird zudem davon ausgegangen, dass Hacker und Botnet-Operator nicht die ein und dieselbe Person sind. Hacker sind oft zwischen 18 und 35 Jahren, während Botnet-Operator überwiegend älter als 35 Jahre sind.

Ein Klick ist leicht zu faken
Um besser zu verstehen, warum Anzeigenbetrug in der Online-Werbung floriert, hilft ein Blick auf die

Eike Trapp, Senior Security Consultant, Axians IT Security

Oliver Hülse, Managing Director CEE, Integral Ad Science

Metriken der Erfolgsmessung. Ad-Fraud hat sich unter anderem zu einem großen Problem entwickelt, weil die Branche sich zu lange auf suboptimale Metriken zur Erfolgsmessung fokussiert hat. Anstelle von Conversions, bei denen der User eine Aktion ausführt – wie beispielsweise ein Kauf – wurden und werden immer noch Metriken wie die Klickrate als Indikatoren für die Effektivität von Werbung genutzt. Eine Kampagnenauswertung, die sich auf einen Markenwiedererkennungswert stützt oder auf eine echte Interaktion des Nutzers mit der Marke, ist für Ad-Fraud unanfällig. Verhaltensmetriken hingegen, wie ein einfacher Klick, lassen sich sehr leicht manipulieren.

Ad-Fraud Bekämpfung ist eine kollektive Aufgabe
Obwohl in den letzten Jahren komplexe Technologien gegen Ad-Fraud entwickelt wurden, ist für eine wirksame Bekämpfung von Ad-Fraud ein branchenweites Umdenken in Bezug auf die Messmethoden notwendig. Metriken, die den Grad der Markenbekanntheit oder vorab definierte Conversions erfassen, garantieren, dass Werbung echte, interessierte Nutzer erreicht. Zudem läßt sich der Kampf gegen Ad-Fraud nur gewinnen, wenn Netzwerke, Geräte, Browser sowie Userverhalten durch Data Science und Technologien besser analysiert werden. Risiken müssen durch Malware-Analyse, Software-Zerlegung und Infiltration von Hacker-Gemeinschaften identifiziert werden und Technologien dementsprechend weiterentwickelt werden. Diese Aufgabe übernehmen Verifizierungs- und Optimierungsanbieter.

Der Kampf gegen Fraud lässt sich nur gewinnen, wenn man nicht nur technologisch auf neuestem Stand ist, sondern auch neuen Methoden schnell entgegenwirken kann. Wenn alle Mitglieder des digitalen Ökosystems vorhandene Technologien auch einsetzen und dazu beitragen, sie konstant weiterzuentwickeln, hat die Branche eine Chance, das Wettrüsten mit den betrügerischen Netzwerken zu gewinnen und ein transparentes, fraud-freies digitales Werbeumfeld zu schaffen.

Oliver Hülse

1.6 CYBER-ATTACKEN

Verbreitung von Ransomware – Beobachtungen zur Entwicklung

Vor vier Jahren wurde die Aussage, dass Cryptolocker bald an einzelne E-Mail-Adresse im Internet verschickt werden, belächelt. Damals haben Cyberkriminelle Phishing-E-Mails an Millionen von E-Mail-Adressen verschickt und Ransomware-Varianten über infizierte Links oder Word-Dokumente verbreitet, ohne dass sich Rückschlüsse auf die wahre Zielgruppe ziehen ließen. Von Studenten bis hin zu Großeltern, von Privatanwendern bis hin zu IT-Experten – jegliche Gruppen wurden Opfer dieser Angriffe. Als die Ransomware dann jedoch damit begann, netzwerkfähige Ressourcen zu verschlüsseln, schenkten ihr auch Unternehmen mehr Aufmerksamkeit.

In dieser Phase der Entwicklung wurde die sogenannte Scattershot-Delivery-Methode mit der Funktion der Verschlüsselung von Dateien auf dem lokalen Dateisystem und auf Unternehmensserver-Ressourcen kombiniert. Die Verschlüsselung des Dateiservers einer Infrastruktur oder des NAS (Network Attached Storage)-Systems verursacht mehr Schaden für Unternehmen als die Verschlüsselung eines einzelnen Arbeitsplatzes. Aus diesem Grund erhielten die Incident Response-Hotlines verstärkt Anrufe, bei denen IT-Administratoren auf der Suche nach einer Lösung verstärkt wissen wollten, welche Auswirkungen eine Lösegeldzahlung haben könnte.

Dieser Trend zur Verschlüsselung von Netzwerkfreigaben durch Ransomware und die damit verbundene erhöhte Aufmerksamkeit ist wahrscheinlich der Beginn der nächsten Phase der Ransomware-Verteilungstechniken.

Der Aufstieg des Remote Desktop-Protokolls
Angreifer und Opfer interagierten aufgrund der Auswirkungen der Ransomware auf die Unternehmensumgebung vermehrt miteinander um die Zahlung des Lösegeldes zu diskutieren. 2016 gab es dann zudem verstärkt Masseninfektionen, bei denen mehrere kritische Unternehmensbereiche in der Umgebung des Opfers gleichzeitig infiziert wurden. Die Security Community führte weitere Untersuchungen durch, was den Verdacht bestätigte: Cyberkriminelle haben, das von Microsoft entwickelte Remote Desktop-Protocol (ein proprietäres Protokoll, kurz RDP) genutzt, um über eine grafische Oberfläche eines entfernten Systems in der Umgebung des Opfers Fuß zu fassen.

Sobald die Angreifer in ein System eingedrungen waren, wurden in der Regel Tools eingesetzt, die es ermöglicht haben, falsch konfigurierte und unbeabsichtigte Benutzer/Gruppen/ Administrator-Beziehungen zu finden und diese Schwachstellen auszunutzen. Fehlkonfigurierte oder unbeabsichtigte Active Directory-Konfigurationen sind der beste Freund eines Cyberkriminellen. Sie ermöglichen den Angreifern den Zugriff auf die Rechte des Domainadministrators und somit auch den Zugriff auf das Netzwerk. Die Cyberkriminellen finden dadurch heraus, welche Objekte besonders wertvoll für das Opfer und somit auch für den Angreifer sind, und infizieren diese.

Nachdem kritische Server und Backup-Systeme in der Umgebung identifiziert wurden, konnten die Angreifer nun integrierte Windows-Systemadministrationswerkzeuge verwenden, um jede Ransomware massenhaft einzusetzen. Angreifer versuchten nicht mehr, jede Person im Internet per E-Mail zu erreichen – mit dem Remote Desktop-Protocol wussten sie genau, auf was sie sich konzentrieren sollten, und infizierten gleichzeitig kritische Vermögenswerte dank ihres neu erlangten tiefen Zugriffs in die Umgebung der Opfer.

Die nächste Stufe der Ransomware: Botnetze
Die Taktik, das RDP als Ausgangsbasis für diese massenhaften, geplanten, interaktiven oder manuellen Einsätze von Ransomware zu verwenden, war sehr verbreitet. Mit jüngsten Fällen wie der Ryuk-Ransomware sehen die Sicherheitsforscher jedoch eine Weiterentwicklung der Taktik. Bei der Untersuchung, ob sich Opfer durch RDP exponiert haben, wurden entweder keine RDP gefunden, oder es war nur über VPN zugänglich und nicht direkt mit dem Internet verbunden. Diese Fälle erforderten tiefere Untersuchungen. In mehreren weiteren Fällen wurden Bot-Infektionen gefunden, die mit dem Auftreten von Ransomware-Infektionen korrelieren.

Im letzten Monat wurden vermehrt TrickBot-, Emotet- und AdvisorsBot-Infektionen beobachtet, die mit dem Zeitpunkt der Bereitstellung von Ransomware übereinstimmen. Diese Bot-Infektionen sind in der Opferumgebung weit verbreitet und haben ebenfalls falsch konfigurierte Active Directory-Beziehungen genutzt, um sich im Netzwerk auszubreiten.

In diesen Fällen wurde festgestellt, dass Phishing-E-Mails mit bösartigen Word-Dokumenten der Bot-Zustellungsvektor sind. Diese Dokumente enthalten Makros – eine Folge von Anweisungen und Deklarationen, die per einfachem Aufruf ausgeführt werden können. In TrickBot und AdvisorsBot Infektionsuntersuchungen im Zusammenhang mit Ransomware wurde festgestellt, dass das Opfer folgende Aktionen durchgeführt hat:

1. Die Phishing-Mail wurde geöffnet.
2. Das bösartige Dokument wurde geöffnet.
3. Makros zur Ausführung wurden aktiviert.

An dieser Stelle installiert der ausführbare Inhalt in den Makros entweder einen Bot oder er erreicht den Botnet Command-and-Control-Server, um letztendlich die Bot-Malware herunterzuladen.

Wir sehen dies als eine Weiterentwicklung der Ransomware-Auslieferungstaktik. Es gibt einen beobachtbaren Trend bei der Bereitstellung von Ransomware, der von opportunistischem Phishing über kompromittiertes RDP geht.

Zusammenfassend gehen die Sicherheitsforscher davon aus, dass Bot-Aktivitäten für den Vertrieb von Ransomware zunehmen werden. Bots sind eine einfache Methode zur Verbreitung zusätzlicher Malware, was sie wiederum zu einer attraktiven Möglichkeit für die Verbreitung von Ransomware macht.

Dietmar Schnabel

Dietmar Schnabel, Regional Director Central Europe, Check Point Softwares Technology

CEO-Fraud: Wenn Unternehmen auf Knopfdruck Millionen verlieren

Und wieder ist es passiert, diesmal bei einem niederländischen Filmunternehmen namens Pathé. Anfang des Jahres fielen hier der Managing Director und der CFO auf Betrüger herein, die insgesamt 21 Millionen US-Dollar erbeuten konnten. Aus Angst bei einem angeblichen Zukauf nicht schnell genug zu reagieren, entschieden sich die beiden Manager entgegen allen Bedenken zu einem Geldtransfer. Der Fall wurde inzwischen vor einem Gericht verhandelt und abgeschlossen, das Geld ging komplett verloren.

Die Angriffsmethode CEO-Fraud verbreitet sich auch in Deutschland rasant. Anfang des Jahres hatte eine Studie von PwC zum Thema Wirtschaftskriminalität den Anstieg dieser Art von Betrugsfällen nachgewiesen. Demnach waren seit 2016 40 Prozent der deutschen Unternehmen mindestens einmal vom „Chef-Betrug“ betroffen .

Auch in anderen Ländern wie Österreich versuchen Cyberkriminelle ihr Glück . So war im November bekannt geworden, dass Mitarbeiter von Autohäusern von angeblichen CEOs angewiesen wurden, größere Geldbeträge nach Deutschland und Polen zu überweisen. Diebe gibt es also auch hierzulande, die sich dieser Taktiken und Tricks bedienen.

Der aktuelle Hackerangriff auf die Hotelkette Marriott lässt außerdem erahnen, dass die erbeuteten Datensätzen vor allem für zukünftige CEO-Frauds genutzt werden . Die erbeuteten Datensätze, angereichert mit Informationen aus den sozialen Netzwerken, eignen sich hervorragend dafür. Daher sollten sich Organisationen und ihre Manager vorausschauend darauf vorbereiten, da sie mit hoher Wahrscheinlichkeit ins Fadenkreuz von cyberkriminellen Banden geraten. In einigen dunklen Ecken des Internets, oder aber ganz offen in einschlägig bekannten sozialen Netzwerken werden die Daten der Hotelkette sicherlich in den nächsten Wochen meistbietend verkauft werden.

CEO-Fraud: Die Masche
Ein Tag, an dem ein CEO-Betrug geschieht, verläuft wie jeder andere Tag. Die Mitarbeiter erledigen ihre normalen Aufgaben und arbeiten mit den Menschen, mit denen sie normalerweise zusammenarbeiten. In der Regel beginnen die meisten CEO-Betrugsfälle mit einer Phishing-E-Mail. Eine angriffstypische Email erscheint zunächst völlig legitim, da die richtige E-Mail-Adresse, das richtige Logo oder ein anderes innerhalb des Unternehmens vertrautes

Zeichen verwendet wird, um sich als vertrauenswürdige Bank, Lieferant, IRS-Beamter oder Manager auszugeben.

Soziale Medien verraten Cyberkriminellen oft zahlreiche Details, damit diese auf Nachfragen detaillierte Kenntnisse über die Interna des Unternehmens vorweisen können. Und manchmal kann ein besonders schlauer Bösewicht sogar Monate im Voraus auf das unternehmensinterne IT-Netzwerk zugreifen und so Gewohnheiten und Protokolle analysieren, um die richtige Führungskraft oder Autorität noch genauer verkörpern zu können.

Solche Phishing-E-Mails, die extrem glaubwürdig wirken, veranlassen oft auch versierte Mitarbeiter, eine große Geldsumme zu überweisen oder sensible Daten mit den Bösewichten zu teilen.

Die Frage ist: Funktioniert Phishing wirklich noch überall? Die Antwort lautet: Ja, sehr gut sogar. Der Data Breach Investigations Report von Verizon 2018 macht es deutlich: Phishing war im Jahr 2017 kennzeichnend für 98 Prozent der Social Engineering-Angriffe und war an 93 Prozent aller Sicherheitsvorfälle beteiligt.

Die Opfer reichen von Mitarbeitern aus Personal- und IT-Abteilungen über Führungskräfte auf Managementebene bis hin zu Personen mit Genehmigungen zur Überweisung von Geldbeträgen. Die tatsächlichen Techniken variieren. Manchmal bezieht sich eine E-Mail eine auf eine langjährige Beziehung mit einem Lieferanten und verlangt nun, dass Gelder auf ein anderes Konto als bislang hinterlegt überwiesen werden. Oder sie hacken das E-Mail-Konto eines Mitarbeiters, um für einen Lieferanten des Unternehmens eine Rechnung zu stellen, wobei die Zahlungen auf falsche Konten überwiesen werden. Sogar Fälschungen von Steuerunterlagen sind in den USA bekannt geworden, damit sich die Betrüger am Fiskus vorbei bedienen konnten.

Die Anfragen erscheinen legitim und gerechtfertigt, deshalb wird der Betrug selten früh genug entdeckt, um rechtzeitig und noch vor dem finanziellen Verlust gestoppt zu werden. Und nicht nur das gestohlene Geld hat Auswirkungen auf das Unternehmen. Mehrere Klagen wurden bereits im Namen von Mitarbeitern eingereicht, da ihr Arbeitgeber ihre persönlichen Daten nicht ausreichend geschützt hatte. So musste der US-Festplattenhersteller Seagate Mitarbeitern Schadenersatz nach einem CEO-Fraud zahlen, weil im Rahmen eines Sicherheitsvorfalls in 2016 personenbezogene Daten verloren gingen.

Fazit

Manager und Mitarbeiter in den Finanzabteilungen - aber nicht nur hier - sollten ein „New School“ Security Awareness-Training durchlaufen, welches solche Szenarien bereits berücksichtigt und automatisiert simulierte Angriffe in Kombination mit sofortigen Abhilfemaßnahmen durchführt. So gelingt eine gezielte Vorbereitung auf derart ausgereifte Betrügereien. Mitarbeiter werden so zu einer „menschlichen Firewall“, denn sie erkennen Betrugsversuche sofort oder können diese zumindest als verdächtig einzustufen. E-Mails oder Anrufe können dann an verantwortliche Stellen im Unternehmen weitergeleitet und eskaliert werden. Tipps und Checklisten zur Erkennung des CEO Frauds finden sich unter anderem in dem CEO Fraud Prevention Manual von KnowBe4.

Detlev Weise

Detlev Weise, Co-Founder, exploqii

Referenzen: **[1]** https://www.pwc.de/de/pressemitteilungen/2018/wirtschaftskriminalitaet-ceo-fraud-wird-zum-massendelikt.html **[2]** https://www.meinbezirk.at/innsbruck/c-lokales/wieder-sind-internet-betrueger-am-werk-ceo-fraud_a3032637 **[3]** https://blog.botfrei.de/2018/12/gastbeitrag-datendiebstahl-bei-marriott/ **[4]** https://www.handelsblatt.com/technik/it-internet/soziales-netzwerk-cyber-kriminelle-nutzen-facebook-als-plattform-seite-2/3457860-2.html?ticket=ST-3198185-Mn6EA2RjpdY1nbdRFUqZ-ap5 **[5]** https://www.verizonenterprise.com/verizon-insights-lab/dbir/ **[6]** https://cdn2.hubspot.net/hubfs/241394/CEO%20Fraud%20Manual.pdf

Cyberangriffe – Vorsorge senkt Risiko und Folgeerscheinungen

Es wird schlimmer: Nahezu täglich erreichen die Öffentlichkeit Nachrichten zu neuen Angriffen auf geschäftliche und private PCs. Die Kriminellen setzen dabei in vielen Fällen so genannte Ransomware ein, also Software, die die Dateien auf dem Rechner verschlüsselt und damit für den Anwender unbrauchbar macht. Die Angreifer versprechen jedoch, dem Opfer einen Schlüssel zu liefern, um die Dateien zu entschlüsseln und damit wieder nutzen zu können. Doch das ist nicht immer der Fall. Was für den privaten Anwender im besten Falle nur ein großes Ärgernis ist, kann für Unternehmen lebensbedrohend werden – so millionenfach geschehen letztes Jahr. Viele Firmen und Organisationen waren wochenlang damit beschäftigt, die Folgen eines solchen globalen Cyberangriffs zunächst zu minimieren und dann zu beseitigen. Die Annahme, es handle sich bei der Attacke um eine Ausnahme, ist komplett falsch. Im Gegenteil: Die Zahl der Angriffe wird zunehmen, auf private wie Business-Rechner.

Angriffe werden immer intelligenter

Die Experten des Marktforschungsinstituts Osterman Research haben sich im Auftrag von Quest diesen Markt genau angesehen und im April 2018 die Ergebnisse der Untersuchungen veröffentlicht. Diese Studie kommt dabei zu teilweise überraschenden Ergebnissen: Zwar hat die Zahl der Ransomware-Angriffe leicht abgenommen, die Vielfalt und damit die Gefährlichkeit ist jedoch gestiegen. So hat sich beispielsweise zwischen Januar 2017 und Februar 2018 der Variantenreichtum um fast Dreiviertel (74 Prozent) erhöht. Zudem konzentrieren sich die Angreifer bei ihren Angriffen verstärkt auf einzelne Branchen, etwa den öffentlichen Sektor oder das Gesundheitswesen. Doch nicht nur diese Entwicklung bereitet der IT-Industrie große Sorgen, denn auch andere Formen digitaler Kriminalität nehmen zu: Allein im vergangenen Jahr verdoppelten sich die Fälle von Malware Injection und auch die Attacke via E-Mail kommt immer mehr zum Einsatz. So waren im Februar 2018 drei von 10.000 E-Mails Phishing-Versuche und drei von 2.000 E-Mails enthielten Malware. Das bedeutet, dass ein mittelständisches Unternehmen mit 500 Mail-Empfängern pro Jahr mit 15 Phishing-Versuchen und 77 Mailware-Angriffen rechnen muss. In Großunternehmen mit etlichen tausend Angestellten ist die Lage entsprechend weitaus dramatischer. Und dabei sind noch gar nicht alle Angriffsoptionen erfasst, denn auch bei mobilen Endgeräten steigt die Bedrohung an. Im Jahr 2017 nahmen Mailware-Angriffe auf diesem Gebiet um 54 Prozent zu.

Dass dies nicht ohne Folge bleibt, ist offensichtlich. So gaben 28 Prozent der in der Studie befragten Unternehmen an, dass ein oder mehrere Systeme mit Malware verseucht wurden. Bei einem Viertel der Befragten wurden gezielte E-Mail-Angriffe von einem kompromittierten Konto aus vorgenommen. Und ein weiteres Viertel dieser Firmen verzeichnete den Verlust von sensiblen oder vertraulichen Informationen.

Unternehmen sind nicht hilflos

Auch wenn es den Kriminellen immer wieder gelingt, die Sicherheitsmechanismen zu überwinden, so gibt es dennoch für die Unternehmen keinen Grund, den Kopf in den Sand zu stecken. Selbstverständlich sind Firewalls, Malware-Scanner und andere Maßnahmen unerlässlich, um die Sicherheit der Unternehmens-IT so weit wie möglich zu gewährleisten. Da dies niemals vollständig gelingen wird, müssen die Firmen auch für den Fall eines erfolgreichen Angriffs entsprechend Vorsorge treffen.

An erster Stelle steht dabei – obwohl dies von vielen Unternehmen nicht genügend berücksichtigt wird – die effektive Sicherung der Daten. Blickt man gut ein Jahr zurück auf die WannaCry- und NotPetya-Angriffe aus dem Jahr 2017 zurück, bei denen weltweit auf Millionen PCs Daten verschlüsselt wurden, wird schnell deutlich, dass die Unternehmen, die eine intelligente Backup-Strategie eingesetzt haben, auf der sicheren Seite waren. Denn statt sich überhaupt mit den verschlüsselten Daten auseinandersetzen zu müssen, waren nach dem – falls überhaupt notwendigen – Neuaufsetzen der PCs sofort alle Daten wieder aus der Sicherung verfügbar. Hier sollten IT-Verantwortliche darauf achten, dass die Sicherung plattformübergreifend – also für physische und virtuelle Systeme – erfolgt. Um entsprechend flexibel reagieren zu können, sollten die Sicherungs- und Wiederherstellungslösungen dabei skalierbar sein. Damit ist zumindest der erste Schritt getan.

Ergänzend dazu sollten sich die IT-Verantwortlichen auch weitere Maßnahmen in Betracht ziehen, um diesen Gefahren gegenüber gewappnet zu sein. Dazu gehört beispielsweise Disaster Recovery as a Service (DRaaS), falls die eigenen Ressourcen versagen sollten. Bei DRaaS erfolgt eine automatische Replikation auf einen lokalen oder Remote-Standby-Server beziehungsweise einer virtuellen Maschine. Diese Replikation ermöglich im Fall der Fälle die Wiederherstellung der Daten und Systeme. Zu empfehlen ist dabei, diesen Prozess zu automatisieren. Denn dann können IT-Verantwortliche ihre Administratoren entlasten, so dass diese wiederum ihr Augenmerk komplexeren Aufgaben schenken können.

Schulung nicht vergessen

Sind diese Mechanismen implementiert, ist ein wichtiger Schritt getan, die Folgen eines – aus Sicht der Cyberkriminellen – erfolgreichen Angriffs zu minimieren. Dennoch bedarf es in jedem Falle auch der Absicherung des E-Mail-Systems mit einer passenden Security-Lösung, um dieses Einfallstor so klein wie möglich zu halten.

An dieser Stelle noch eine weitere Empfehlung: Ist der Schadensfall bereits eingetreten, reduzieren sogenannte Cyber-Versicherungen zumindest die finanziell erlittenen Verluste durch Ausfallzeiten, Rechtskosten oder Cyber-Erpressung.

Im Lichte der Entwicklung ist es unumgänglich, die eigenen IT-Sicherheitsmaßnahmen auf den Prüfstand zu stellen. Dazu gehört auch und an erster Stelle die permanente Sensibilisierung und Schulung der Mitarbeiter im Bereich Security. Denn nur dann können die technischen Sicherheitsmaßnahmen ihr volles Schutzpotenzial zur Geltung bringen.

Glücklicherweise bietet der Markt heute Anbieter, die ihr Know-how in die Konzeption, Planung und Implementierung intelligenter Sicherheitsmaßnahmen einbringen können. Denn bei der IT-Sicherheit zu lange zu warten, bedeutet, die Zukunft des Unternehmens zu riskieren.

Stefan Bösner

Stefan Bösner, Systems Consultant/ Data Protection, Quest Software

Cybersicherheit 2018: KI kämpft gegen KI

Wie Unternehmen künstliche Intelligenz (KI) nutzen können, um den KI-Systemen von Cyberkriminellen auf Augenhöhe zu begegnen.
Der Einsatz künstlicher Intelligenz ist nicht allein das Privileg der Guten und Korrekten. Neueste Trends zeigen: Auch Cyberkriminelle haben intelligente Technologien für sich entdeckt. Sie lernen immer besser, künstliche Intelligenz für ihre Zwecke zu missbrauchen. Doch die Unternehmen reagieren. Dazu werden sie einerseits gezwungen durch die im Mai 2018 in Kraft tretende Datenschutz-Grundverordnung (EU-DSGVO). Sie erkennen aber auch, insbesondere nach den jüngsten Vorfällen, echten

Christian Nern, Head of Security Software, IBM Germany

Matthias Ems, Associate Partner Security Services, IBM Germany

Handlungsbedarf. Und sie sind nicht machtlos – ganz im Gegenteil: Der Einsatz KI-basierter ganzheitlicher IT-Sicherheitslösungen ist ein wirksames Mittel, den Kampf um den Schutz ihrer Daten für sich zu entscheiden.

Die von IBM Security erhobenen IT-Security-Trends für das Jahr 2018 zeigen: Cyberkriminelle beherrschen ihr Handwerk und nutzen für ihre Angriffe immer häufiger künstliche Intelligenz. Zudem sorgt die voranschreitende Digitalisierung dafür, dass solche Attacken nicht länger lokal oder regional verortet sind, sondern sich in kurzer Zeit über die ganze Welt verbreiten. Auch das vermehrte Aufkommen von IoT-Geräten (Internet of Things) beflügelt diese Entwicklung. Gleichzeitig führt die Digitalisierung dazu, dass Cyberkriminelle weltweit besser denn je miteinander vernetzt sind. Best Practices werden von ihnen gesammelt, bewährte Angriffsmethoden weiterentwickelt. Trotzdem haben die Datendiebe damit bisher nur einzelne Schlachten gewonnen, nicht den ganzen Kampf.

Trends bestätigen: Security-Expertise der Unternehmen nimmt zu

Denn andererseits zeigen die aktuellen Trends auch, dass Unternehmen nicht zuletzt im Zuge der kommenden EU-Datenschutz-Grundverordnung (EU-DSGVO) ihre IT-Security-Expertise weiter ausbauen. Sie können damit den Cyberkriminellen gestärkter denn je entgegentreten. Es scheint damit auch sehr wahrscheinlich, dass 2018 zu einem Jahr wird, in dem die meisten großen Unternehmen erstmals in der Lage sind, schnell und angemessen auf Datenpannen und Cyberangriffe zu reagieren – trotz der aktuell bekanntgewordenen Sicherheitslücken in bestimmten Mikroprozessoren.

Immer häufiger bedienen sie sich dafür ganzheitlicher SIEM-Lösungen (Security Information and Event Management) und IT-Sicherheitslösungen auf Basis künstlicher Intelligenz, wie sie beispielsweise IBM mit Watson for Cyber Security bietet. Das bedeutet im Umkehrschluss: immer mehr Unternehmen verzichten auf ein unübersichtliches Sammelsurium einzelner Sicherheitslösungen, die im Zweifel eher ein Weniger als ein Mehr an Schutz bieten.

Best Practice: Ganzheitliche Sicherheitslösungen unterstützt durch KI

Für eine effiziente Cybersicherheit ist es wichtig zu wissen, was in der eigenen IT-Landschaft zu jedem Zeitpunkt passiert. Wollen sich Unternehmen gegen Angriffe wirkungsvoll schützen, so müssen sie in Echtzeit einschätzen können, welche ihrer Systeme möglicherweise von einer Cyberattacke oder einer Datenpanne betroffen sind. So können sie, basierend auf Analysen der relevanten Sicherheits-Log-Daten, schnell und umfassend geeignete Schritte einleiten. Dazu brauchen sie hocheffiziente SIEM-Lösungen, die gleichzeitig für maximale Transparenz sorgen.

Hat sich ein Unternehmen im Kampf um die Sicherheit seiner sensiblen Unternehmensdaten mithilfe einer SIEM-Lösung erst einmal den nötigen Überblick verschafft, kann künstliche Intelligenz schließlich bei der Auswertung der sicherheitsrelevanten Daten helfen und so den Abwehrkampf insgesamt beschleunigen. KI-basierte Sicherheitslösungen bringen Unternehmen dabei auf drei verschiedenen Wegen mit den Cyberkriminellen auf Augenhöhe:

- **Zeitersparnis**
  Bei der Abwehr von Cyberattacken ist jede Minute kostbar. Durch Analysen mithilfe intelligenter Systeme erhalten Unternehmen eine schnelle Übersicht über die Datenlage. Dies geschieht innerhalb von Minuten, anstelle von Stunden oder Tagen. So kann der Zeitvorsprung der Cyberkriminellen schneller eingeholt werden. Damit hält sich auch der mögliche finanzielle und materielle Schaden in Grenzen.
- **Überblick über alle relevanten Informationen**
  KI-Sicherheitslösungen berücksichtigen die gesamte relevante und aktuelle Informationsbasis – egal ob es sich um unternehmensinterne oder global verfügbare Daten handelt. Sicherheitsanalysten können damit ihre Entscheidungen auf Basis einer wesentlich umfangreicheren Gefahren-Auswertung treffen und nicht nur aufgrund eines auf die Schnelle erstellten Ausschnitts.
- **Assistenz durch KI-Systeme**
  KI-basierte Sicherheitslösungen sollen und können geschulte Analysten nicht komplett ersetzen. Nur sie kennen die Interna des Unternehmens und wissen die Analyseergebnisse entsprechend zu deuten. Allerdings kann künstliche Intelligenz Sicherheitsexperten bei ihrer Analyse erheblich entlasten und unterstützen. Sie gewinnen dadurch wertvolle Zeit für die Behebung von Sicherheitsvorfällen und für die wichtige IT-Forensik.

Künstliche Intelligenz als Schlüssel für mehr IT-Sicherheit

Mithilfe künstlicher Intelligenz werden Unternehmen also wieder in die Lage versetzt, mit Datendieben Schritt zu halten. Dank umfassender KI-gestützter Analysen sind sie beim Aufspüren und Ausmerzen von Sicherheitslücken effektiver unterwegs und können damit Cyberattacken sehr viel schneller unschädlich machen. Diese Erkenntnis setzt sich auch immer mehr durch: Laut einer Studie des IBM Institute for Business Value wird die Verbreitung von intelligenten, KI-Sicherheitslösungen in den nächsten Jahren signifikant zunehmen.

Um darüber hinaus den Schaden möglichst gering zu halten und nicht mehr nur reaktiv auf Angriffe zu antworten, sollte es in Zukunft dann auch möglich sein, weitgehend proaktiv Angriffe vorauszusehen und abzuwehren. Dies geschieht mittels KI-Analysesystemen, die prognostizieren, wie hoch in jedem Moment die Bedrohung durch welche Art von Cyberattacken ist. Basis solcher Prognosen sind Erkenntnisse darüber, wo zu einem beliebigen Zeitpunkt Angriffe welcher Art und nach welchen Mustern registriert werden. In einer solchen Zukunft wird der Kampf der – hoffentlich überlegenen – Unternehmens-KI gegen die KI von Cyberkriminellen womöglich gar nicht mehr nötig sein. Dann schauen sich beide KI-Systeme nur einen Moment wie zwei wütende Wölfe an, wobei das unterlegene Tier seine Schwäche spürt und sich instinktiv zurückzieht.

Christian Nern, Matthias Ems

1.7 RECHT

Cybersicherheit und Verbraucherrechte: der Dreisprung der EU

Wir alle, die wir die digitale Revolution von der ersten Minute an miterlebt haben, kennen es nicht anders: Geräte veralten rapide, funktionieren nur fehlerhaft oder geben plötzlich den Geist auf; sie werden gehackt oder sind auf einmal nicht mehr kompatibel zum Stand der Technik. Aus dem hochmodernen Device wird innerhalb weniger Jahre ein digitales Auslaufmodell.

Wir haben uns daran gewöhnt, dass wir mit unseren Produkten und etwaigen Problemen oft allein gelassen werden. Wenn der Hersteller einen Tag nach dem Kauf des neuen Handys dessen Support einstellt, nehmen wir es mit einem Seufzen in Kauf: wahrscheinlich haben wir uns bei der Produktwahl nicht ausreichend informiert. In irgendeinem Forum, irgendeiner User-Group wurde die Einstellung sicher angekündigt. Ähnlich im Fall von Sicherheitslücken: meist obliegt es dem Kunden, sich zu informieren und Gegenmaßnahmen zu ergreifen. Mit unserem Schaden werden wir nicht selten allein gelassen.

Zeit für ein neues Verständnis von Verbraucherrechten und Sicherheit

Doch es ist Zeit, sich von dieser Einstellung zu verabschieden. Nicht nur vom Standpunkt der Verbraucherrechte her ist ein Umdenken nötig: Die niedrigen Standards bei der fortlaufenden Unterstützung digitaler Produkte stellen ein massives Sicherheitsrisiko dar. Ein Gerät, das nicht supportet wird, ist ein unsicheres Gerät; ohne Updates werden Sicherheitslücken nicht behoben. Es droht zur Waffe in einem Bot-Netz zu werden und damit die Durchschlagskraft von Cyber-Attacken weiter zu erhöhen.

Beim Design digitaler Systeme ist die Update-Tauglichkeit eine von drei unverzichtbaren Doktrinen (die anderen beiden sind durchgängige Verschlüsselung und die konsequente Forderung von Authentifizierung und Autorisierung jedes Zugriffs). Für die sichere digitale Welt muss sie einklagbar sein, ebenso wie Hersteller für Fehler in Haftung genommen werden müssen. Jede Forderung nach „Security by design“ ist Makulatur, solange man einen säumigen Hersteller nicht für seine unsicheren Geräte verantwortlich machen kann.

Die Sicherheit unserer digitalen Infrastruktur ist zu wichtig, als dass der Staat sie nicht durch entsprechende Gesetze gewährleisten muss. Die Forderung nach verlässlichen Produkten mit einer garantierten Lebensdauer ist deswegen eine Aufgabe für die Politik. Die Hoffnung, dass sich der Markt in puncto IT-Sicherheit selbst reguliert, ohne dass der Gesetzgeber eingreift, dürfte selbst der größte Optimist mittlerweile aufgegeben haben.

Digitaler Binnenmarkt funktioniert nicht mit „analogen“ Gesetzen

Die EU hat die Förderung des digitalen Binnenmarktes zu einem Kernziel erklärt. Doch anders als in anderen Branchen, wo gemeinsame Standards schon 2008 mit dem „New Legislative Framework“ eingeführt wurden, ist der Digitalmarkt noch immer uneinheitlich reguliert. Schlimmer noch: In vielen Fällen finden Gesetze aus der prä-digitalen Ära Anwendung. So etwa beim Urteil eines niederländischen Gerichts: Im Juni dieses Jahres hatte es eine Klage eines Verbraucherschutzbundes abgewiesen, der verlässliche Update-Garantiezeiten für Smartphones gefordert hatte. Ganz im Sinne herkömmlicher Produkthaftung hatte das Gericht entschieden, dass der Hersteller für zukünftige Ereignisse wie Sicherheitslücken nicht zur Verantwortung zu ziehen ist und Updates deswegen nicht einklagt werden könnten.

Damit geht die Rechtslage an den besonderen Umständen der digitalen Welt vorbei: Mag bei einem herkömmlichen Produkt die Entwicklung mit der Auslieferung abgeschlossen sein – bei internetfähigen Geräten und Software endet sie erst mit dem Ende der Nutzung. Niemand außer dem Hersteller vermag Produkte zu aktualisieren und ihre Sicherheit zu gewährleisten. Ohne zeitgemäße Gesetze, die diese Sondersituation anerkennen, werden alle Bemühungen zur IT-Sicherheit ins Leere laufen.

Nationale Vorstöße, wie sie derzeit beispielsweise in Deutschland diskutiert werden, sind lobenswert, werden das Problem aber nicht abschließend lösen. Es muss eine einheitliche, EU-weite Regelung zur Einführung einer verpflichtenden Sicherheitskennzeichnung analog zum bekannten CE-Kennzeichen her. Auch die Hersteller-Pflicht, Updates für einen bestimmten Zeitraum nach Kauf eines Geräts bereit zu stellen, muss im Binnenmarkt einheitlich verankert werden.

Eine einheitliche, moderne und sicherheitsfokussierte Einführung von Update- Pflichten und Mindeststandards innerhalb der EU hätte noch einen weiteren Vorteil: sie würde präventiv wirken und die Widerstandsfähigkeit („Resilience“) der IT-Infrastruktur erhöhen: Billiganbietern, die an Sicherheit und Updates sparen, würde sie einen Riegel vorschieben und gleichzeitig die Marktchancen derjenigen Hersteller stärken, die von Grund auf sicherer designte Produkte anbieten.

EU Cybersecurity Act: Erste Schritte

Erfreulicherweise ist die EU hier bereits aktiv geworden. Sie strebt im „EU Cybersecurity Act“ erste Schritte zur Verbesserung der Sicherheit an, darunter die Stärkung der ENISA, des europäischen Äquivalents zum BSI, und die Einführung einheitlicher Zertifizierungsschemata für internetfähige-Produkte. Diese sollen dann in allen Mitgliedstaaten verlässlich Auskunft über das Sicherheitsniveau internetfähiger Produkte geben.

Ein Entwurf der EU-Kommission liegt seit September letzten Jahres auf dem Tisch, die endgültige Verabschiedung steht aber noch aus. Änderungen sind also noch möglich. Sie sind aus meiner Sicht auch nötig.

Ralf Koenzen, Gründer und Geschäftsführer, LANCOM Systems GmbH

Denn die im aktuellen Entwurf verankerten freiwilligen Sicherheitszertifizierungen werden das Problem der fehlenden Cybersicherheit alleine nicht lösen. Hierfür bräuchte es verpflichtende Sicherheitsmindeststandards für alle Produkte, die in irgendeiner Weise mit dem oder über das Internet kommunizieren. Und: es bräuchte zusätzlich eine gesetzliche Pflicht für die Hersteller, Sicherheitslücken schnellstmöglich nach Bekanntwerden zu schließen.

Ein aus meiner Sicht entscheidendes Argument hierfür liegt in der besonderen Art der digitalen Welt begründet: anders als bei Autos, Zahnpasta oder Lebensmitteln ist ein einmal zugelassenes digitales Produkt nur vorübergehend sicher. Die sich verändernde Bedrohungssituation, neue Schwachstellen und Angriffsmuster erfordern zwingend, dass das Herz dieser Produkte – die Software oder auch Firmware – dauerhaft überprüft und bei Bedarf aktualisiert wird. Freiwillige Einmal-Zertifizierungen sind nicht auf diese zyklischen Anforderungen ausgelegt. Sie erfüllen damit ein zentrales Ziel der IT-Sicherheitspolitik nicht – böten aber gleichwohl den Herstellern eine gute Gelegenheit, sich durch zusätzliche, besondere Sicherheitsmerkmale aus der Masse der Anbieter hervorzuheben.

Jetzt oder nie

Um die Sicherheit im Cyberraum langfristig zu fördern, muss die EU einen Dreisprung vollziehen: Sicherheits-Mindeststandards, die Update-Pflicht und Sicherheits-Zertifizierungen gehören thematisch fest zusammen. Sie sind zentrale Elemente für die digitale Sicherheit ebenso wie für die digitale Souveränität sowohl des einzelnen Verbrauchers als auch des Wirtschaftsstandorts Europa als Ganzes. Diese Maßnahmen müssen Teil des EU Cyber Security Act werden.

Dabei gilt es keine Zeit zu verlieren. Eine EU-Richtlinie, würde sie morgen verabschiedet, benötigt Zeit zur Umsetzung in nationales Recht. Auch die Industrie braucht Zeit: Um Produkte gemäß verpflichtender Sicherheits-Mindeststandards zu entwickeln und zu produzieren, brauchen die Hersteller offizielle Normen, an denen sie sich orientieren können. Diese gilt es zunächst zu entwickeln. Ein Prozess, der mitunter Jahre dauert.

Je länger die EU also jetzt braucht, um die gesetzlichen Grundlagen zu legen, desto länger verschiebt sich die Lösung unserer Cybersicherheitsprobleme in die Zukunft. Desto länger werden Verbraucher – aber auch die Wirtschaft – weiter mit auftretenden Sicherheitslücken alleine gelassen und hängen allein vom guten Willen der Hersteller ab.

Machen wir uns nichts vor: sollten es Mindeststandards & Update-Pflichten nicht mehr in den aktuellen Entwurf schaffen, wird die Stärkung der Verbraucherrechte in der digitalen Welt noch lange auf sich warten lassen. Denn dass eine gerade verabschiedete Richtlinie schon kurz darauf wieder angepackt wird, ist sehr unrealistisch.

Doch genau diese Zeit haben wir nicht.

Ralf Koenzen

Der einfache Weg zum sicheren und gesetzeskonformen Geschäft

In der EU greift bald ein strengerer Datenschutz. Dieser lässt sich mit Maskierung personenbezogener Daten realisieren, wofür sich vor allem Data-Ops-Plattformen eignen.

Zum Jahresauftakt führten Meltdown und Spectre, zwei Sicherheitslücken in Prozessoren, vor Augen, wie massiv die Sicherheit von privaten Daten in Gefahr geraten kann. Kurzfristig helfen Updates. Auf lange Sicht wirkt in Unternehmen nur ein vollständiges Sicherheitskonzept, das auch abhandelt, wie das eigene Geschäft mit bestehenden und künftigen Gesetzen in Einklang gebracht wird. Im Fokus steht aktuell die EU-Datenschutzgrundverordnung (DSGVO), die für alle Unternehmen ab 25. Mai 2018 verbindlich ist.

Die DSGVO vereinheitlicht den Datenschutz personenbezogener Daten von EU-Bürgern. Die Verordnung regelt dazu den Umgang mit persönlichen Daten wie Nutzernamen, IP-Adressen, GPS-Koordinaten, Telefonnummern, Kreditkartennummer oder Nutzerverhaltensdaten strenger. Die betreffende Person ist der Dateneigentümer, der einer Datenverarbeitung durch ein Unternehmen künftig ausdrücklich zustimmen muss. Jeder EU-Bürger hat das Recht, sein Einverständnis zu widerrufen. Bei Verstößen gegen die DSGVO drohen Unternehmen Strafen bis zu 20 Millionen Euro oder bis zu vier Prozent ihres weltweit erzielten Jahresumsatzes.

Aufwändige Vorarbeit zum automatisierten Datenmanagement

Umfragen legen nahe, dass IT- und Compliance-Verantwortliche vor allem den Aufwand fürchten, um einen DSGVO-konformen Datenumgang zu erreichen. Fehlendes Problembewusstsein gepaart mit Unwissenheit über die Verordnung hält daneben viele Firmen ab, konkrete Maßnahmen zu ergreifen.

Ein Unternehmen kommt jedoch nicht um den Aufwand herum, zu klären, wo seine Daten liegen und wer auf sie zugreift beziehungsweise zugreifen kann. Im nächsten Schritt geht es darum, die Interaktion von Nutzern, Prozessen und Technologien so zu organisieren, dass Geschäftsinteressen und Gesetzesvorgaben gleichermaßen gewahrt bleiben. Schlussendlich soll ein schnelles, automatisiertes und sicheres Datenmanagement entstehen. Hierfür bietet die DataOps-Technologie einen vielversprechenden Ansatz. Dabei handelt es sich um eine Technologie, mit deren Hilfe sich Daten aus verschiedenen Quellen sehr schnell und bei Bedarf auch gesichert bereitstellen lassen – etwa für die Anwendungsentwicklung oder für Cloud-Migrationen.

Virtuelle Datenkopien erstellen

Eine DataOps-Lösung wie die Delphix Dynamic Data Platform wird auf den gängigen Virtualisierungsplattformen (Hypervisors) installiert und erstellt virtuelle Datenkopien aus Datenbanken wie Oracle, SQL Server, DB2, mySQL oder Sybase, aber auch Applikationen. Standardschnittstellen binden die verschiedenen Datenquellen ein. Die Synchronisation der virtuellen Datenumgebungen mit den Produktivdaten erfolgt inkrementell, das heißt, es werden nur die Änderungen in der Datenquelle in die komprimierte Datenkopie übertragen.

Die DSGVO nennt explizit Verschlüsselung und Pseudonymisierung von Daten als legitime Verfahren, um personenbezogene Daten ausreichend zu schützen. Wendet ein Unternehmen nachweislich eines der Verfahren an, erlischt das Widerrufrecht des Dateneigentümers. DataOps-Plattformen verfügen über Bibliotheken, die aufzeigen, wo in der Unternehmens-IT sensible Daten abliegen. Die Technologie identifiziert die Informationen, die unter das DSGVO fallen, und implementiert notwendige Maßnahmen in die Geschäftsprozesse.

Maskierung und multiple Kopien

Für die Pseudonymisierung von Daten kommen Maskierungs-Tools zum Einsatz, um persönliche Angaben zu verändern. Beim Maskieren bleibt das ursprüngliche Dateiformat erhalten. Ein Zuordnen zu einer Person, also ein Dechiffrieren, ist dann nur mit zusätzlichen Informationen und Mitteln möglich. Die DSGVO stellt allerdings die Bedingung, dass diese Informationen separat abliegen müssen. Nur so bleiben maskierte Daten bei einem Diebstahl oder Verlust geschützt.

Die erfolgreiche Maskierung von Daten in Produktivsystemen markiert einen Zwischenschritt. Ändern sich die Produktivdaten, hat das Konsequenzen: Ein Unternehmen muss dann eine entsprechende Kopie der geschützten Daten den anderen Geschäftsbereichen zur Verfügung stellen. Was zunächst harmlos klingt, entpuppt sich beim genaueren Hinschauen als anspruchsvolle Aufgabe: Über 90 Prozent aller internen Unternehmensdaten basieren auf Kopien, die für sekundäre Anwendungen wie Software-Entwicklung und Test, Reporting, Analyse und Backups verwendet werden. Diese Kopien einzeln zu maskieren, entspräche einem immensen Aufwand. Moderne Plattformen maskieren alle nötigen Daten in einem Zuge und stellen dann multiple maskierte Kopien für die unterschiedlichen Anwender bereit, ohne dass zusätzlicher Speicherplatzbedarf und Zeitaufwand entstehen oder die Agilität des Geschäfts leidet.

Abgesicherte Geschäftsinteressen

Maskierung mit einer DataOps-Plattform bietet Unternehmen die Chance, das eigene Geschäft schneller, einfacher, kostengünstig und gemäß der DSGVO auszurichten. Die DataOps-Technologie befähigt Unternehmen zudem, mehr Gespür für ihre Daten zu entwickeln. Auch darauf kommt es in unserer streng regulierten wie datengetriebenen Welt an. In dieser entscheidet das aufeinander Abstimmen von IT-Sicherheit, Datenschutz und Geschäftsinteressen darüber, ob jemand künftig Erfolge einfährt oder andere vorbeiziehen lassen muss.

Minas Botzoglou

Minas Botzoglou, Regional Director, Delphix Corp.

Regelbasiertes DRM schützt kritische Informationen

Das Digitale Rechtemanagement bietet eine flexible, automatisierbare und praktikable Möglichkeit, um kritische Unternehmensdokumente wirksam vor unbefugten Zugriffen schützen.

Digitales Rechtemanagement (DRM) stammt ursprünglich aus der Musik- und Filmindustrie. In der Zwischenzeit nutzen Anwender DRM auch in weiteren Anwendungsszenarien wie dem Schutz kritischer Informationen. Der Grund dafür ist leicht nachzuvollziehen: Die früher üblichen Verfahren haben sich angesichts immer raffinierterer Angriffe auf IT-Systeme als nicht mehr ausreichend erwiesen. Dafür gibt es zwei Gründe: Erstens lassen sich externe Angreifer nicht mit hundertprozentiger Sicherheit von den eigenen Systemen aussperren. Zudem sind

Patrick Schraut, Vice President, Consulting Europe, NTT Security

die traditionellen Methoden unwirksam, wenn Angriffe von innen erfolgen – etwa dann, wenn Daten von Mitarbeitern aus Unachtsamkeit oder Unkenntnis kompromittiert werden. Zweitens ist der Schutz des Zugriffs auf Daten beziehungsweise Dokumente in vielen Fällen unwirksam. Unternehmen schützen sich beispielsweise durch eine technische Schnittstellenkontrolle davor, dass Daten per E-Mail verschickt werden können. Das verhindert aber nicht den Datenabfluss per USB-Stick.

Im Unterschied zu herkömmlichen Methoden schützt DRM nicht die Zugriffe, sondern die Informationen selbst. Zunächst einmal müssen Unternehmen dazu Dokumente klassifizieren und abhängig von der Einstufung anschließend verschlüsseln. Infolgedessen haben nur Personen beziehungsweise Rollen, die über entsprechende Rechte verfügen, Zugriff auf die Daten. Allgemein zugänglich sind lediglich Dokumente, die als unkritisch eingestuft wurden. Ohne die erforderlichen Rechte ist kein Zugriff möglich, da das Dokument nicht entschlüsselt werden kann. DRM schützt das Dokument selbst, nicht aber den Kanal, auf dem es möglicherweise das Unternehmen verlässt. Administratoren etwa können ohne Sicherheitseinbußen Dateien kopieren und verschieben. Das Dokument bleibt verschlüsselt; der Administrator kann aus seiner Rolle keine Lese-Rechte ableiten.

Eine entscheidende Anforderung an ein auch in der Praxis wirksames DRM-Verfahren ist die möglichst weitgehende Automatisierung. Klassifizierung und Zugriffsmanagement können so regelbasiert ablaufen. Bei der Sicherheit gilt eine einfache Regel: Der Schutz muss einfach und praktikabel sein, weil die Nutzer ansonsten immer versuchen werden, ihn zu umgehen.

DRM basiert auf Regeln

Aus Sicht eines Bearbeiters läuft der DRM-Prozess so ab: Legt er eine Datei an, öffnet sich ein Pop-up-Fenster, das zwingend die Klassifikation abfragt. Ab einem zuvor festgelegten Level, beispielsweise „vertraulich“, wird die Datei verschlüsselt gespeichert. Um die Bedienbarkeit, aber auch die Gewährleistung einer systematischen und konsistenten Klassifizierung sicherzustellen, sollte dieser Basisprozess aber so weit wie möglich automatisiert werden. Bei einer regelbasierten Klassifizierung lassen sich verschiedene Ansatzpunkte unterscheiden:

- Organisations-basierte Klassifizierung: Dokumente aus der Personalabteilung oder dem Bereich Forschung und Entwicklung werden immer als vertraulich eingestuft;
- Rollen-basierte Klassifizierung: Einzelne Gruppen von Mitarbeitern, etwa Führungskräfte, IT-Administratoren oder Sachbearbeiter, erhalten immer, unter bestimmten Bedingungen oder nie Zugriff auf einzelne Klassen von Dokumenten;
- Quellen-basierte Klassifizierung: Unterlagen aus bestimmten Anwendungen, wie der Lohn- und Gehaltsabrechnung oder aus CRM-Systemen, werden automatisch als vertraulich klassifiziert; das gleiche gilt, wenn Kopien davon beispielsweise in Word oder Excel weiterverarbeitet werden sollen;
- Projekt-basierte Klassifizierung: Dokumente, die bei der Entwicklung neuer Produkte oder auch im Alltag in den dazu vorgesehenen Ordern abgelegt werden, zum Beispiel in Ordnern wie „Forschung und Entwicklung“ oder „Protokolle von Vorstandssitzungen“, werden automatisch klassifiziert und verschlüsselt gespeichert;
- Content-basierte Klassifizierung: Eine modernere DRM-Lösung ist in der Lage, mit Hilfe von Schlüsselwörtern im Text, beispielsweise Kreditkartennummern, Kontonummern, Namen von Mitarbeitern und Kunden, im Text eine Klassifizierung vorzunehmen und die passende DRM-Stufe zuzuweisen.

Solche Klassifizierungen können nicht starr sein, sie müssen vielmehr über eine gewisse Dynamik verfügen. Mitarbeiter verlassen das Unternehmen und neue werden eingestellt. Ein lange Zeit vertrauliches Projekt ist nach der allgemeinen Markteinführung eines Produkts nur noch in Teilen vertraulich.

Mit DRM lassen sich nicht nur strukturierte kritische, sondern auch unstrukturierte Informationen sehr gut sichern. Bei Unternehmen aus allen Branchen haben seit einiger Zeit schon die außerhalb strukturierter Datenbanken vorgehaltenen Daten, beispielsweise Dokumente, Grafiken, Diagramme, Präsentationen, Fotos oder Videos, massiv zugenommen.

Eine DRM-Lösung ist in der Lage, alle Formen und Formate problemlos zu verarbeiten – und dies nicht nur mit Daten im unternehmenseigenen Rechenzentrum, sondern auch in der mobilen Welt. Tablets oder Smartphones können dann nicht nur online mit dem Rechteserver im Rechenzentrum kooperieren, damit klassifizierte Dokumente freigegeben werden. Administratoren sind in der Lage, auch offline bestimmte Rechte für einen Tag zu vergeben – nimmt der Mitarbeiter mit einem mobilen Gerät nicht innerhalb von 24 Stunden Verbindung mit dem Rechteserver auf, erlischt seine Berechtigung automatisch.

Ein regelbasiertes DRM erfüllt zwei zentrale Anforderungen: erstens Sicherheit durch Verschlüsselung und zweitens Praktikabilität durch weitgehende Automatisierung. DRM hat sich bereits bei vielen Unternehmen bewährt und ist auf dem besten Weg, sich als Standard zu etablieren. Patrick Schraut

Der Mensch zuerst

Die digitale Welt hat uns neue Möglichkeiten eröffnet, miteinander in Kontakt zu treten. Asynchron, unverbindlich und demokratischer. Vorbei sind die Zeiten, in denen die Damen im Vorzimmer entscheiden, wer durchgestellt wird. Heute reicht das Premiumabo bei LinkedIn und schon kann ich anschreiben, wen ich will.

Was sich erst einmal anhört wie paradiesische Zustände, ist bei näherem Hinsehen eine Einladung zur Zeitverkürzung. Ganze Phasen der Geschäftsanbahnung fallen unter den Tisch und damit auch das Wichtigste, was gute Beziehungen ausmacht.

Der bloße digitale Zugriff kann zwischenmenschliches Vertrauen nicht ersetzen. Getippte Buchstaben sind nicht das Gleiche wie Gespräche, in denen wir Antennen für unser Gegenüber entwickeln. In denen wir mal einen Schritt vorpreschen, um dann zu merken, dass der andere nicht reagiert. Deshalb wieder warten, ihn reden lassen, ihm zuhören und plötzlich verstehen, warum unser Gesprächspartner eben noch verhalten reagiert hat.

Mitgefühl können wir nur im menschlichen Miteinander entwickeln. Im Austausch, im gemeinsamen Erleben und Betrachten von Situationen und Herausforderungen. Erst wenn sich zwei Menschen wirklich kennen, ihre Bedürfnisse und Historie füreinander greifbar werden, macht es Sinn, über gemeinsame Pläne und Geschäfte zu sprechen.

So schließt der Begriff „Kaltakquise“ einen Beziehungsmangel mit ein. Wer sich kalt begegnet, ist vorher nicht warm miteinander geworden. Der Flyer eines Politikers im Briefkasten wird nie die gleiche Wirkung haben, wie eine Tür-zu-Tür-Offensive, in der der Politiker sich persönlich vorstellt und sich Fragen öffnet. Sich in die Augen zu schauen, wird nie altmodisch.

Anstatt also gleich im dritten Satz Leistungen anzubieten oder auf LinkedIn vorgefertigte Massenmails zu schicken, sollten wir uns fragen: Wie baue ich eine Beziehung zu einem Menschen auf? Die Antwort ist immer gleich: Indem ich mich für ihn interessiere und ihm zuhöre. Mir Zeit nehme für diesen Menschen, seine Geschichte und sein Wesen.

Nur so entsteht eine Chance für mehr. Für Gespräche, verbindliche Verabredungen, gegenseitige Besuche und berührende Zeiten miteinander. Solche tragfähigen Beziehungen können auch in Aufträgen münden. Wer Weltanschauungen teilt, kann auch gemeinsame Geschäftsideen entwickeln, die dann auf sicherem Boden stehen. Sales-Funnel und geführte Customer Journeys sind sicher eine zeitgemäße Ergänzung, doch nichts schlägt die echte Verbindung zwischen Menschen. Ein Gedanke, der sich auch auf Teams ausweiten lässt.

Seit fast 20 Jahren leite ich Workshops. Abends vor der Veranstaltung treffen wir uns mit der gesamten Teilnehmergruppe zum Abendessen. Wir tauschen uns aus und erzählen die echten, bewegenden Geschichten, die uns zu den Menschen gemacht haben, die wir heute sind. So können wir ein Gefühl für unser Sein entwickeln und am nächsten Morgen - auch fachlich - auf einer ganz anderen Ebene starten. Die nächsten Tage laufen in einem tiefen Vertrauen, weil sich die Menschen wirklich begegnet sind. Sie haben die Verletzlichkeit, die Werte und die Emotionen des anderen kennen- und respektieren gelernt. So entsteht Kreativität.

Erfolg kommt, wenn Menschen ein echtes Team sind. Dazu brauchen sie Zeit, sich zu erzählen und sich zu stützen. Beziehung geht vor Inhalt. Der Rest klappt dann schon.

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

Foto: Privat

Management in Zeiten der Digitalisierung war gleich zu Beginn das Thema des international bekannten Wirtschaftsexperten Prof. Dr. Fredmund Malik (Erfolgsautor und CEO, Malik Institute for Complexity and Management).

Dr. Jörg Ochs (SWM) sprach über die Digitalisierung einer bis zu hundert Jahre alten Infrastruktur – den Wasser- und Gasrohren – in München.

MÜNCHEN

Digitale Stadt München e. V.

DIGICON 2018

Ein volles Haus mit 353 Teilnehmern aus über 200 Firmen, visionäre und schwungvolle Vorträge, ein spannendes Rennen um den 3. Münchner Digital Innovation Award und zukunftsweisende Ideen auf dem Marktplatz der Innovationen bei Cocktails und kulinarischen Finessen – das alles war die DIGICON 2018. Internationale Experten aus Wirtschaft und Wissenschaft stellten den Teilnehmern neueste Trends, Entwicklungen und Ergebnisse rund um das Thema Machine Learning vor. Anwender referierten über Success Stories, Analysten über die Methoden dahinter. Am 21. und 22. November 2018 hatten die Teilnehmer im Palais Lenbach die Möglichkeit, sich zu diesen Themen auszutauschen und neueste, bahnbrechende Entwicklungen zum Machine Learning aus Perspektiven wie Quantencomputing, Data Mining und Reinforcement Learning zu betrachten.

In den Pausen sowie beim exklusiven Galaabend gab es – bereichert durch kulinarische Köstlichkeiten von Feinkost Käfer – jede Menge Gelegenheit zum Netzwerken.

V.l.n.r.: Aleksandra Solda-Zaccaro (Messe München GmbH) im Gespräch mit Boris Radke (ProSiebenSat.1), Mirco Bharpalania (Lufthansa Group) und Josef Meier (Fortinet GmbH) nach den Impulsvorträgen zum Thema „Fortschritt durch Innovation und Technik“

Die Gäste der DIGICON konnten mit ihren „Innocoins“ das innovativste Untenehmen wählen. Den Preis im Wert von 10.000 Euro Mediavolumen im DIGITALE WELT Magazin hat am Ende das Start-up „BPU Blockchain Power Unit GmbH“ gewonnen.

Zu dem Thema „Quantencomputing und Reinforcement Learning als Innovationstreiber“ gab es Impulsvorträge von Prof. Dr. Patrick van der Smagt (Direktor AI Research VW, zweiter von links), Dr. Sebastian Feld (Leiter QAR-Lab, LMU München, dritter von links) und Dr. Heiko Udluft (Airbus, ganz rechts). Moderiert wurde die Diskussion von Karin Kekulé (ganz links).

Am zweiten Messetag fand der jährliche Pitch-Battle um den begehrten Münchner Digital Innovation Award statt. Die Jury war durch Ralf Schneider (GROUP Chief Information Officer, ALLIANZ SE), Ewa Duerr (Product Ops Lead, Google) und Rupert Schäfer (Geschäftsführer, The Nunatak Group) vertreten.

Die historischen Hallen des Palais Lenbach boten wunderbare Rahmenbedingungen für die DIGICON 2018.

Am Ende konnte sich beim Pitch-Battle das Start-up Nect.com mit seinem Produkt „Selfie Ident“ durchsetzen.

Im Parterre des Palais Lenbach präsentierten sich 12 Firmen am „Marktplatz der Innovationen“ mit ihren neuartigen Produkten.

Nach der Kür des innovativsten Marktplatzes wurde noch bis spät in den Abend zu stimmungsvoller Musik und herrlichen Cocktails gefeiert.

Fotos: Digitale Stadt München e.V.

FACHBEIRAT

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
CIO 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 Florentina Hofbauer
Blog Steffen Illium, Tanja Zecca
Redaktionsassistenz Kerstin Fischer, Katja Grenner
Mitarbeiter dieser Ausgabe Sebastian Feld, Carsten Hahn, Thomy Phan, Kyrill Schmid, Christoph Roch
Schlussredaktion Barbara Haber

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 Mitgliedsbeitrag 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

für den DIGITALE-WELT-Blog

Die nächste DIGITALE WELT erscheint am 05.06.2019

Werden Sie Teil unserer hochkarätigen Autorenschaft und platzieren Sie Ihre Digitalthemen von morgen auf der Plattform von heute mit bislang **430.000*** Klicks.

UNSERE AKTUELLEN BLOG-RUBRIKEN:

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

INTERESSE GEWECKT?
Dann melden Sie sich bei der DIGITALE WELT-Redaktion per E-Mail: **blog@digitaleweltmagazin.de** oder telefonisch unter der **+49 89 2180 9171**.

***Unsere Beiträge wurden online unter www.digitaleweltmagazin.de/blog veröffentlicht und erzielten dabei die oben genannte Klickanzahl im Zeitraum 01. August 2017 – 04. Februar 2019.**

Leitfaden zur Veröffentlichung von Fachbeiträgen

FÜR IHRE EINREICHUNG SIND FOLGENDE DINGE ZU BEACHTEN:

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

DAFÜR KOMMEN SIE IN DEN GENUSS FOLGENDER LEISTUNGEN:

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

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

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

Wir freuen uns auf Ihren Fachbeitrag mit Ihrem Expertenwissen.

Ihr DIGITALE WELT Team

WIR ERWEITERN HORIZONTE. DAMIT IDEEN WACHSEN KÖNNEN.

ES IST AN DER ZEIT, SCHON HEUTE FÜR GROSSARTIGE IDEEN VON MORGEN ZU BEGEISTERN.

Die Zukunft erfinden wir alle gemeinsam. Deshalb fördern wir weltweit soziale Projekte, übernehmen Verantwortung für Jugend, Bildung und Technik und leisten einen Beitrag für die Gesellschaft. **Gemeinsam mit unseren Marken gestalten wir richtungsweisende Ideen, die neue Wege eröffnen. Von der Vision zum Erlebnis.**
www.bmwgroup.com/next100

GEMEINSAM SCHREIBEN WIR GESCHICHTE. DIE DER ZUKUNFT.

BMW GROUP THE NEXT 100 YEARS

BMW MINI Rolls-Royce Motor Cars Limited