Management for Professionals

Ferri Abolhassan *Editor*

Cyber Security. Simply. Make it Happen.

Leveraging Digitization Through IT Security

Springer

Management for Professionals

More information about this series at http://www.springer.com/series/10101

Ferri Abolhassan
Editor

Cyber Security. Simply. Make it Happen.

Leveraging Digitization Through IT Security

Springer

Editor
Ferri Abolhassan
Telekom Deutschland GmbH
Bonn, North Rhine-Westphalia
Germany

Editing: Gina Duscher, Gerd Halfwassen, Albert Hold, Beatrice Gaczensky, Dominique-Silvia Kemp, Thomas van Zütphen, Martin Farrent
Translation: Dr. Edward M. Bradburn, Daina Jauntirans, Stephen McLuckie, Niamh Ruddy and Jessica Spengler for Malinowski & Partner

ISSN 2192-8096 ISSN 2192-810X (electronic)
Management for Professionals
ISBN 978-3-319-46528-9 ISBN 978-3-319-46529-6 (eBook)
DOI 10.1007/978-3-319-46529-6

Library of Congress Control Number: 2016958508

Cover illustration: eStudio Calamar, Berlin/Figueres

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

Trust Is the Basis of Digitization

Thomas Kremer

When it comes to the future development of our society and economy, one word dominates the discussion: digitization. The consensus is that people, machines, and devices will become increasingly networked. The debate, however, is whether this is something good or bad. Will digitization unburden people and bring progress, comfort, and freedom? Or will it bring about the collapse of our social and welfare systems, turning us into transparent citizens who have lost control of their own data and whose labor is no longer needed? No single person can answer these questions – and the answers will probably not be black or white but rather somewhere in between. One thing is certain, however: we cannot prevent this development; we can only influence it. Experts predict that by the year 2020, more than 50 billion devices will be connected to one another, from smartphones to cars to industrial machines. This will generate an unimaginable amount of data to be stored and processed. And this data is going to be the most important resource for our digital society, the oil of our economy.

Digitization Offers Great Opportunities

Digitization undoubtedly promises great opportunities: safer road traffic thanks to self-driving cars, for example. Or the prospect of cumbersome tasks being handled by machines that can communicate directly with one another. Or even a longer and healthier life thanks to telemedicine applications and new research results emerging from the analysis of large volumes of data. But for digitization to succeed, it is critical for people to trust in data protection and the security of these new services. Without trust, people will not use the new services. On the contrary: Their knee-jerk reaction will be to try to prevent digital developments.

This is not possible, however. If we undermine the development of digitization in Europe, the new services will be created anyway – mostly on the west coast of the USA. Then, the only option for Europeans would be to send their data there and get modified products in return. Europe would become a kind of digital colony. In the

area of services for end customers, this is already largely the case. No one can get around Facebook, Google and Co. The chances are better in the market for business customer solutions. The Internet of Things and Industry 4.0 offer Europeans an opportunity to catch up with digitization.

Data Protection and Digital Business Models Are Not in Opposition

Politics, business, science, and society therefore have a responsibility to establish the right guide rails so that people can trust the new services. The digital sovereignty of the individual must be the priority here. This can be guaranteed by a high degree of transparency, freedom of choice for customers, and the development of solutions amenable to data protection. For this to be possible, data protection experts must be involved right from the start in the development of new products and services that handle personal data. Customers must be able to easily understand how their data will be used so that they can make informed decisions about it. Furthermore, we need effective methods of anonymizing and pseudonymizing data for digital business models so that individuals cannot be identified without their consent.

We have traditionally had a high level of data protection in Germany and Europe. It is good that the EU's General Data Protection Regulation will establish standardized rules throughout Europe which guarantee a high degree of data protection while at the same time enabling new digital business models. The focus cannot be on regulating individual industries or data processing models. Instead, we need clear, standardized guidelines for handling data, which create security and trust for customers and companies alike. People also have to be educated and informed about the use of technologies and their personal data – from an early age.

Security Has to Be Simple

Digitization additionally increases the risk of consumers and companies falling victim to digital attacks. The Center for Strategic and International Studies (CSIS) estimates that the economic damage from cyberattacks amounts to more than 400 billion euros per year worldwide. Up to 400,000 new viruses, worms, and Trojans are found in the network every day. What's more, cybercriminals can now take advantage of vulnerabilities within just a few hours and send deceptively realistic emails in order to sneak in malicious code. These criminals can then use the infected computers to hijack other machines in a corporate network and search for the information they want. It often takes months for the affected companies to notice that there was – or is – an attacker in their network.

Security authorities, companies, and private individuals therefore also have to upgrade in order to protect themselves better. Behavior-based and system-status

analyses are the keywords in cyberdefense today. Merely placing firewalls around IT systems is not enough. In many cases, the criminals have used sophisticated social-engineering mechanisms – so they are already in the network. The task then is to find them as quickly as possible. These attackers can be detected by monitoring anomalies in the network. To develop solutions such as this, Deutsche Telekom is currently pooling its expertise in a new organizational unit, "Telekom Security."

There is one principle at the forefront of these new security products: Security has to be simple. Until now, the security of solutions and products has tended to be a supplementary function added to a finished product. But it is increasingly being incorporated right from the start, thus ensuring better integration.

From the user's perspective, too, it is important to remember that four out of five attacks could be prevented using simple security measures. This is why it is so critical for users to always keep their virus protection and operating systems up to date, for example. Incidentally, smartphones are powerful computers that require just as much protection. This personal responsibility is yet another aspect of digital sovereignty.

As you can see, there are many facets to the digitization debate, and security is a critical factor for success. I am delighted that this book is giving cybersecurity the attention it demands, and I hope you enjoy reading it!

Yours,
Dr. Thomas Kremer

Member of the Board of Management for Data Privacy, Legal Affairs and Compliance of Deutsche Telekom

Dr. Thomas Kremer has been Member of the Board of Management for Data Privacy, Legal Affairs and Compliance at Deutsche Telekom since June 2012. He was appointed to the Government Commission on the German Corporate Governance Code in September 2013. He has also been Chairman of "Making Germany Safe on the Net" (DSiN) since November 2015. Before moving to Deutsche Telekom, Kremer worked for ThyssenKrupp AG, joining the company's legal department in 1994. In 2003, as General Counsel, he took over the management of ThyssenKrupp's Holding legal department, which also subsequently went on to develop the company's Compliance program. After taking over the management of the newly formed Corporate Center Legal and Compliance in 2009, Kremer was then appointed Executive Vice President in 2011.

Among other positions held prior to ThyssenKrupp and Telekom, Kremer also was an attorney at law firm Schäfer, Wipprecht, Schickert in Düsseldorf (now CMS Hasche Sigle). After graduating in law, Thomas Kremer worked as a research assistant at the University of Bonn in Germany before receiving his doctorate in law in 1994.

Contents

Security: The Real Challenge for Digitalization

1

Ferri Abolhassan

1.1 Introduction

Predicting train cancellations and thus avoiding what could amount to up to six-figure damages per cancellation. Or telling the purchasing department today which items customers are going to order the day after tomorrow. This is already a reality. Why do CIOs often know more about a company's core business than the CEO or specialist departments – and know it sooner? Because digitalization – with the IoT etc. – gives them access to a huge mass of information about customers, machines and processes. This is what is new. Such information enables CIOs to prepare and make decisions better and, above all, faster – ideally in real time. Now more than ever, the CIO is the most important sparring partner and source of inspiration for the CEO.

But for a CIO to do justice to this role, the technology has to work perfectly. Three things are needed to make sure the CIO is covered in this regard. First, the IT has to be stable. Second, any solutions have to interact reliably. And third, alongside high quality, a maximum level of security must be guaranteed. This is absolutely essential. As digitalization increases, companies are becoming more and more reliant on IT to survive. Quality, reliability **and** security must be ensured in the long term so that CIOs have the freedom they need to innovate. Then they can really pick up the pace with digitalization. The backbone for all this is the cloud. Only the cloud can centrally collect, store and evaluate the mass of structured and, above all, unstructured data and thus draw the maximum benefit from digital technologies – even as the mountain of data continues to grow.

Data and the insights gained from it are becoming increasingly valuable. And they must be protected in every respect: physically, technically and legally. We know this, and yet we do too little about it – because security is complex,

F. Abolhassan (✉)
Telekom Deutschland GmbH, Bonn, North Rhine-Westphalia, Germany
e-mail: ferri.abolhassan@telekom.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_1

inconvenient and slow. This has to change. Security has to be simple so that it will be used. This means simple to acquire, to operate and to handle. Security is not an end in itself, after all. It is the prerequisite for digitalization to happen in the first place. Only then can it create real customer value. The only way to do this is with a cloud that offers maximum stability and security. This is the real challenge – and this is what will make security the springboard for digitalization.

1.2 Status Quo: The Cloud Is the Backbone of Digitalization

When analysts such as Gartner say the digitalization hype is already over (see Hagenau 2015), what they mean is this: "Gone are the days when digitalization and cloud computing were repeatedly heralded as the next big thing," as Forrester advisor Dan Bieler puts it. The excitement is giving way to sensible pragmatism. The cloud in particular found its way into companies long ago, and now these companies have to get down to work. The momentum of digital transformation can no longer be stopped, much less reversed. This is true regardless of where an individual company stands – whether it develops services in the cloud, or has to migrate entire legacy systems to the cloud, or wants to explore the Internet of Things.

No matter which current trend a company picks up on today, the basis of it will be the cloud. Something that was a new development just ten years ago is now a prerequisite for nearly every digitalization project. This is because only the cloud offers the capacity, cost-efficiency and agility needed to meet current and future demands of digitalization.

But what does the cloud actually look like? For some it is already a commodity, for others it is still a must-have. And why is it anything but trivial to get a company into the cloud? The answers to these questions are complex – not least because there is no such thing as THE cloud. The cloud has become highly diversified in recent years, so users can now choose from a variety of different options and implement the cloud solutions that best meet their requirements. These options cover everything from on-premise systems to private, public or hybrid clouds. And one question hovers above all of this: How secure will everything be if I connect one thing to the other?

It's a reasonable question. While public clouds are publicly accessible via the Internet, private clouds are designed more individually and offer extra protection by limiting access to a strictly defined user group. The hybrid cloud offers companies the best of both worlds: a combination of a private and public cloud with in-house IT. Customers themselves decide which data they want to host in the private or public cloud.

But the potential target of attack is growing – just look at the Internet of Things. And because up to 50 billion things are expected to be connected by the year 2020, according to IDG, this growth is exponential. As the number of sensors grows, so too will the amount of data they collect and the value of the insights it offers. This means that the need for protection is growing exponentially as well. It is no surprise

that the most recent Cloud Monitor study from Bitkom and KPMG reported that while cloud usage is on the rise, the security concerns of potential users are curbing stronger growth (see Bitkom and KPMG 2015). Specifically, 90 percent of the decision-makers in politics and business say that concerns about IT security are currently the most important obstacle to Industry 4.0 (see Hill 2015).

One thing is certain: Both digitalization and the cloud must meet the essential requirements of maximum security, reliability and quality – covering everything from the security of data, processes and networks to the security of data centers, infrastructures, applications and devices. But it is also necessary to protect the interaction between these elements – and to do so without making it arduous for the user. For this reason, security must mirror digitalization, and not just in terms of scalability. It also has to be simple to acquire, implement, operate and use.

1.3 Data Security: Only a Secure Cloud Will Lead to Secure Digitalization

Security – and, in the age of digitalization, data security in particular – is always the prerequisite for business success. The cloud has to be secure if it is going to have a future. Companies need the cloud to explore the potential of the IoT. But if IT security is so fundamentally important, and executives themselves acknowledge this, why do companies struggle to implement it? There are various reasons for this. Security is often perceived as being complex, expensive and difficult to implement – but this can be alleviated by security solutions that are easy and cost-efficient to use. A harder problem to solve in the long term is the lack of technical expertise, especially in small and medium-sized companies. Some security-specific courses of study at universities are already addressing this problem, but the accelerated training of a sufficient number of experts will take some time. Despite all of these obstructions to the implementation of security, urgent action is required. This is because the attacks are getting more professional, and the damage they cause is getting more severe. According to the German data security agency BSI, there are already attackers operating internationally who focus on extorting companies, especially those in the financial services sector. And the attraction of these companies is growing. Studies show that 33 percent of all financial services providers have fallen prey to cybercriminals at least once. The average in every other industry is 17 percent. The attackers specifically look for IT vulnerabilities and systematically exploit them. In the first nine months of 2015, the BSI reported a total of 847 critical vulnerabilities in the eleven most frequently used software products alone (see Sievers 2015).

But how can companies make the leap into a secure future where they are immune to threats of all kinds? And how do secure cloud solutions as the basis of digitalization have to be designed so that companies view them as an opportunity, rather than a risk?

1.3.1 Risk Transformation: It Has to Be Easy to Get into the Cloud

The cloud and digitalization are clearly the future. They promise great technological diversity and immeasurable potential for companies in every industry. But companies have good reasons for hesitating, and these reasons are as diverse as the technology itself. For one thing, these are technologically complex solutions which are almost impossible for corporate IT departments to manage on their own. Then there is the confusing array of providers whose lack of product transparency makes the decision even more difficult. And last but not least, there is investment. Before a company can exhaust the potential of the cloud, it has to make a financial commitment.

Planning risks and financial risks: After choosing a cloud solution, companies are often tied to a provider for a long time. This robs them of the flexibility they need to quickly and easily move to a secure cloud environment. In addition, long contracts scare off potential customers. There are few or no players (i.e., IT service providers) in the market who are seriously trying to absorb some of the business risk for companies. Ideas such as abolishing the vendor lock-in are considered taboo in the industry. The entire history of outsourcing is based on long-term contracts. For customers to leave this contractually protected space, they need to be very confident in the provision and availability of their own services and IT. This is where new concepts come in, such as outsourcing without long contractual commitments and the transformation of legacy applications in the cloud at a fixed price. The option of flexibly cancelling a contract at any time offers real added value and signals that an IT provider is willing to help bear the customer's risk. It also makes investments more calculable and costs more transparent. And faults on the part of the IT provider can be redressed immediately.

Operationalization risks: Complex IT architectures and landscapes that have evolved over years have traditionally been very difficult to transform digitally. They can involve hundreds or even thousands of applications which are often intertwined with one another. If one application is turned off, it is almost impossible to predict how this will impact the others. This is all the more serious because business-critical processes and infrastructures are always affected as well. The implementation of the highest security standards sets the bar even higher. "You don't become a 'cloudifier' – who can handle digital transformation, manage applications in diverse cloud models, and guarantee their security on top of that – overnight." – this comment by Andreas Zilch from PAC hits the nail on the head. Years of experience are needed for smooth cloud transformation and system integration in combination with application-specific cloud orchestration. This problem can be overcome by cooperating with IT integration experts when migrating complex application landscapes to the cloud while modernizing and consolidating systems at the same time. Furthermore, running state-of-the-art cloud and security technologies from high-security, certified data centers helps meet the strictest demands of data security and protection.

1.3.2 Risk of an Incident: Making Sure the Cloud Doesn't Crash

In addition to analyzing business risks and cooperating with IT experts, it is critical for cloud technologies to be secure in and of themselves – which also means they have to offer a high degree of reliability and availability so that users can count on them. Users also have to trust in their inherent security, which must work smoothly. But how are companies protected against failures?

Incident risks: Completely networked value chains and infrastructures in particular harbor a risk of incidents with severe consequences. Networked IT systems are controlling vital machines and processes more and more often today. We need to look no further than intensive care units and operating rooms, high-speed train lines and planes. Perfectly functioning IT is essential here. But it is also clear that incidents are inevitable in IT. The way to counter this is through prevention combined with swift problem detection and reaction – meaning an immediate, structured approach in the event of an incident – embedded in a holistic quality management system.

Comprehensive quality management makes it possible to get very close to 100 percent fail-safety. A three-pillar model has proven effective here. Component one: prevention. Companies identify their business-critical points at platform, process and personnel level – and they take precautions. For example, consistently redundant data center technology can lead to platform availabilities of up to 99.999 percent. This reduces the risk of failures to just a few minutes per year. Furthermore, processes must be classified and emergency plans developed for a variety of scenarios. And finally, quality must be a part of a company culture that is embodied by every employee. This is a process that takes years. Component two: readiness. It literally takes practice to be able to act competently in a crisis. At T-Systems, we hold up to 500 "fire drills" worldwide annually. Regularly simulating emergencies and checking all of the steps necessary for incident management ensures that platforms, processes and personnel are as prepared as possible for component three: action during an actual incident. During any incident, it is also essential that a manager on duty and a representative of top management take responsibility for working on the problem around the clock until it is solved.

Stable, secure cloud services are made possible by coordinated interaction between humans and technology. With this in mind, T-Systems plans to start establishing an ecosystem of partners this year who are all committed to the zero-error principle and comply with common rules for quality management. Cross-industry corporate cooperation will only work in the future if there is a unified industry standard for IT quality. "Made in Germany" is therefore becoming more and more of a seal of approval. T-Systems itself has already reduced its number of system outages by 95 percent to almost zero within just five years through its Zero Outage quality initiative and the certification of around 22,000 employees and 100 system partners. This aspect is gaining importance not only for corporations, but also for small and medium-sized companies and, in principle, for private consumers as well.

Automation of security: This structured and standardized approach is logical – after all, the cloud represents the automation of IT. Consequently, we now need security to be automated on every level. That is the way security can reflect the simplicity of cloud operations – as a managed service, for example. And that is the way products and services can be preinstalled and thoroughly put to the test right from the start. The security-by-design principle must be at the heart of all product development and implementation. This encompasses the security of software throughout a product's lifecycle, as well as all infrastructure and processes. It is also important to ensure intuitive operation so that users are not restricted in their capacity to act. Pioneering solutions already exist that offer companies these kinds of security standards following the quality assurance principle.

1.3.3 Risk of Technical/Physical Attack: A Castle Wall Alone Isn't Enough

Even in the digital age, physical barriers are needed to protect data from attack. Gradually but haphazardly upgrading firewalls and similar solutions is not especially productive on its own. A more promising approach is to continually bring in new fortifications and deploy them in a way that stops attackers in their tracks where previously nothing held them back. This resembles the approach of state-of-the-art, highly secure data centers holding the treasures of digitalization. Take the data center in Biere: This new T-Systems data center near Magdeburg in Germany is separated from adjacent streets by a four-meter-high earth wall. The entire facility is surrounded by a two-meter-high fence topped with barbed wire. Around 300 cameras and motion sensors ensure that attackers cannot penetrate the grounds undetected. For additional security, specially trained security guards patrol the grounds around the clock. Inside the building there are airlock doors, chip-card readers, palm scanners and motion detectors, several hundred sensors and a security center behind mirrored, bullet-proof glass. The heart of the data center can only be reached by crossing an elevated walkway. But physical security does not play the only key role in Biere. To defend against external attackers such as hackers or data thieves, all data flows through encrypted IP VPN tunnels, creating a closed system which is separated from public networks and protected against external access. Intrusion detection and prevention systems supplement the firewall and analyze whether malware has found its way into the data streams. TSL protocols, anti-malware, secure point-to-point connections, and identity and access management solutions ensure that only authorized employees have access to data that may only be used on a need-to-know basis. Unwelcome guests are treated to a veritable labyrinth of intelligent barriers that detect all intrusions, neutralize them and immediately initiate countermeasures. Prevention, detection, reaction – this is what a modern corporate security architecture should look like.

To increase its failure safety, the infrastructure in Biere has been designed redundantly. The data center has an architectural twin in Magdeburg, about 18 kilometers away. Connected by a dual fiber-optic cable and equipped with "twin-core" technology, each data center stores sensitive data redundantly, ensuring its availability even if one of the data centers goes offline. And the effort to ensure high availability goes even further: Connected two times over to a 110-kilovolt power line, the data center's own substation ensures a stable power supply. In the event of an incident, emergency power generators will kick in.

1.3.4 Risk of a Cyberattack: Ensuring Data and Devices Aren't Casualties

Physical attacks in the form of a malicious USB stick – see the Stuxnet virus, for example – are one thing. But the number of cyberattacks has increased even more significantly in recent years. When attackers strike, companies face hefty damages and failures with often far-reaching consequences. In February 2015, hackers acquired the social security numbers, mailing addresses and email addresses of around 80 million customers of Anthem, one of the largest health insurers in the USA. Salary information for customers and employees was stolen as well (see The New York Times 2015). The year before, hackers seized the data of 76 million private and 7 million business customers of the US bank JP Morgan Chase. Attackers apparently also gained access to a list of applications running on JP Morgan's computers. This meant they could examine every program and every web application for known vulnerabilities in order to find an entry point for penetrating the bank's systems again at a later date. Experts say it took the bank months to change its programs and applications (see The New York Times 2014).

Attackers have a variety of motives. They range from a simple "just because they can," through political goals, as is the case with Anonymous, all the way to financial interests, which can be realized through extortion by using crypto-trojans such as Locky (see Eikenberg 2016). Action is urgently required here because these external attacks are becoming increasingly sophisticated, and the attackers are usually well ahead of the companies.

To protect themselves, IT managers have to know where the weaknesses are. But this isn't easy. The opportunities and scenarios for attacks have become very complex. However, technological approaches already exist that can help companies with detection. For example, the defense-in-depth approach divides IT architectures into multiple layers and places security mechanisms on each layer. Once intruders have breached the castle wall – the physical protective barrier – they face the next obstacles: firewalls that prevent unauthorized network access. Then there are honeypots that distract them from their actual goal by simulating the behavior of users, for example. And, to protect the data itself, there are now a variety of

encryption solutions available, which make it impossible for attackers to actually use any valuable information they find.

Looking at the security technologies available today, it is clear that their value often depends on how easy they are to implement. Easy-to-install big-data real-time analyses study the behavior of data and detect behavioral and status anomalies – on both stationary servers and mobile devices. It gets even easier for companies when not only the data itself but also its protective mechanisms – including firewalls, intrusion protection systems, and virus or malware protection – are moved to the cloud.

Once security technology has been implemented and its fail-safety is guaranteed, companies must address another, often more serious vulnerability: Human weaknesses must not be underestimated, and they can undermine many of the most sophisticated security mechanisms – and intentionally or not, the consequences are the same. The simplest example is a telephone call from a supposed technician (think "social engineering") who asks for confidential login information. Only training and dissemination of knowledge can help to avoid this kind of error. In general, sharing knowledge and information is an important protection strategy against attackers. Four eyes see more than two – and the same applies to companies who can warn each other before threats spill over and spread. Voluntary organizations such as the Cyber Security Sharing and Analytics (CSSA) association show how this is done. It is equally important to gain an information advantage in your own company. The first cooperative projects have already started here between Deutsche Telekom, the Hochschule für Telekommunikation Leipzig (HfTL) and the Telekom Campus of Ben Gurion University in Israel.

In addition to the technical, human and knowledge-based prerequisites, it is important not to neglect data protection, because as we move toward a digital society, this aspect in particular will be put to the test. However, we must also make a distinction between an American and a European understanding of data protection and data security. Current discussions concerning the EU-US Privacy Shield show where these definitions diverge.

In Germany, companies must comply with especially strict federal data protection legislation. But these strict regulations are what make data-security specifications "Made in Germany" so internationally popular. For instance, the T-Systems cloud data center in Biere is now being used by 50 IT market leaders and has reached a capacity utilization of 70 percent in a very short time. The outstanding technology, architecture and security of our data centers is a good example of how Germany can reclaim value creation for Europe in an IT market dominated primarily by US companies. The traditionally extremely high level of expertise in the area of encryption technologies (encryption/decryption) could be a promising second area of activity in the IT security sector.

1.4 Looking to the Future

This overview of current IT security requirements shows just how complex the issue is. But in which direction will these developments go as they pick up speed – as they undoubtedly will? And where are we headed in the fight against attacks on the security of data, applications and processes? What is certain is that as digitalization progresses, system autonomy will grow as well. The proportion of communication and collaboration not handled by humans will continue to rise in the future. Thanks to smart data and machine learning (ML), machines and systems will become clever enough in the coming years to evolve autonomously. This means that a company's security DNA might also be able to continually optimize itself and adapt to the latest security requirements and threats.

The greatest benefit to users in this context will be the ability of machine learning to identify patterns and further develop this skill by means of independent self-learning. While most of today's security solutions are still rule-based and have to be modified and optimized by people, the security systems of the future will be able to do this themselves – much more efficiently than is currently possible. Just think of intrusion detection systems that can identify out-of-the-ordinary trespassers. Machine learning can detect and reveal such irregularities very quickly.

Or take user authentication and access control: ML systems can differentiate between even the subtlest nuances in how a user hits a keyboard. When a user logs in by typing a sentence, the system knows immediately whether the keystrokes match the user's profile or not. Pattern recognition through machine learning will eventually progress to the point that authentication will be possible using gestures, regardless of the device used. Bank customers might be able to transfer money by writing their name in the air, for example. There are almost no limits to the possible usage scenarios. And even today, we are already using smart, ML-based automation tools in data centers for the cloud.

1.5 Conclusion

The Internet has transformed society. Communication, business models and processes, big data – everything is getting easier, faster and more cost-efficient. The cloud makes it possible. And security has to keep up – taking into account one aspect above all: It must become easy to acquire and easy to use. For security, too, the cloud is the key to success. We must also increasingly turn our attention to protecting data, not just protecting infrastructures. Traditional castle walls that repel attackers are still an important part of security concepts in modern architectures, but a comprehensive security strategy demands additional measures so that companies are prepared if an intruder has already breached the fortifications. Pioneering developments in the field of machine learning already show: As the interface between humans and machines grows simpler, security must adapt to these new processes and user behaviors as well. Otherwise companies run the risk of disrupting their business processes and workflows. And security has to be simple,

following the plug-and-play principle. The invention and widespread utilization of the cloud has made this simplicity a reality. Let us use the cloud as our model and create a secure digital future.

References

Bitkom Research GmbH on behalf of KPMG AG Wirtschaftsprüfungsgesellschaft. (2015). *Cloud-Monitor 2015*. Accessed May 30, 2016, from https://www.bitkom.org/Publikationen/2015/Studien/Cloud-Monitor-2015/Cloud-Monitor-2015-KPMG-Bitkom-Research.pdf

Eikenberg, R. (2016). *Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde*. heise.de. Accessed June 1, 2016, from http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html

Hagenau, T. (2015). *Cloud computing – der Hype ist vorbei*. computerwoche.de. Accessed May 30, 2016, from http://www.computerwoche.de/a/cloud-computing-der-hype-ist-vorbei,3069749

Hill, J. (2015). *Mit Industrie 4.0 steigt das Angriffsrisiko*. computerwoche.de. Accessed May 30, 2016, from http://www.computerwoche.de/a/mit-industrie-4-0-steigt-das-angriffsrisiko,3219509

Sievers, U. (2015). *Cyber-Angriffe werden immer professioneller*. VDI-nachrichten.de. Accessed June 1, 2016, from http://www.vdi-nachrichten.com/Technik-Gesellschaft/Cyber-Angriffe-professioneller

The New York Times. (2014). *Neglected server provided entry for JPMorgan hackers*. Accessed June 14, 2016, from http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/?_r=0

The New York Times. (2015). *Anthem hacking points to security vulnerability of health care industry*. Accessed June 13, 2016, from http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0

Ferri Abolhassan After receiving his doctorate in computer science, Abolhassan began his professional career in R&D at Siemens in Munich, Germany, followed by several years at IBM in San Jose, USA. In 1992, he joined software vendor SAP, where he held a number of senior positions until 2001, including a spell as Senior Vice President of the global Retail Solutions business unit. Following a four-year tenure as Co-CEO and Co-Chairman at IDS Scheer, he returned to SAP in 2005, most recently as Executive Vice President, Large Enterprise for EMEA. In 2008, Abolhassan took over the newly-created position of Head of Systems Integration at T-Systems and at the same time joined the company's Board of Management. His management portfolio was later expanded to include the Production unit. In 2013, Abolhassan was appointed Director of Delivery before becoming Director of the IT division in 2015, overseeing approximately 30,000 employees and 6,000 customers. In December 2015, Abolhassan also took over the task of setting up the Telekom Security business unit, which will bundle all the security departments in the Deutsche Telekom corporation. In October 2016, he moved to Telekom Deutschland, where he heads the newly created business area Service Transformation as its Managing Director.

In 2011, he launched the successful "Zero Outage" program to safeguard T-Systems' quality standards in the face of growing process complexity. Not only is the program now certified by

Germany's technical inspection agency TÜV, but customer satisfaction has also risen to its highest level in the company's history, setting a new benchmark in the industry. T-Systems now plans to work with partners to create a new industry standard based on the Zero Outage principle. Abolhassan also initiated the construction of a new cloud data center in Germany (Magdeburg/Biere), completed in 2014. The expansion of the facility due to high demand began in 2016. The plan is for storage and computing capacity to have risen by 150 percent on completion in 2018.

To address new IT security challenges, Deutsche Telekom initiated a new organizational unit for security solutions at the end of 2015. In addition to his other tasks, Abolhassan is in charge of launching that unit, which combines and consolidates all of Deutsche Telekom's security activities and will market the company's cyber-security offerings. One primary goal is improved integration of in-house security teams to counter the thousands of daily attacks by cybercriminals. Another objective is to exploit this internal experience to offer customers best-of-breed products and solutions across their entire value chains.

Security Policy: Rules for Cyberspace

2

Wolfgang Ischinger

A computer worm infests Iranian nuclear power plant systems, a cyberattack cripples sections of the Ukrainian electrical grid, intruders penetrate the German Parliament's IT system and steal sensitive data. No longer merely the stuff of science fiction novels cyberspace as a setting for security policy disputes and even a stage for conflicts, has long since become part of our reality.

"I have given Cyber Command . . . really its first wartime assignment," declared United States Secretary of Defense Ashton Carter in Washington in early April 2016 (Financial Times 2016) in a statement directed against ISIS and interpreted by many as the first governmental cyberwar declaration. It is no longer possible to address security policy challenges or to lay out strategies today without factoring in the digital realm.

In fact, our current situation is similar to that some 70 years ago, when the invention of the nuclear bomb fundamentally changed the strategic landscape. The technical possibilities offered by the information revolution are less tangible, and their effects are considerably more complex and multi-faceted, but as in the nuclear revolution, they are fundamentally changing the playing field for international security policy. We are already facing massive challenges along with complex ethical, legal and political questions as the result of attacks by hackers on critical infrastructure, the online recruiting of jihadi fighters and the development of autonomous weapons systems. And technological change will march on, bringing new possibilities that open up any number of opportunities, while at the same time further magnifying the potential dangers associated with cyberspace. We must continually assess the opportunities – as well as the risks – of digital progress in terms of security policy and consider the necessary steps for dealing with them appropriately.

W. Ischinger (✉)
Stiftung Münchner Sicherheitskonferenz gemeinnützige GmbH, Prinzregentenstr. 7, 80538 Munich, Germany
e-mail: ischinger@securityconference.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_2

2.1 Taking Stock: Digital Warfare in the 21st Century

The possibilities of cyberwarfare have radically changed the character of modern conflict. In particular, one trend that we have observed increasingly in recent decades continues unabated: Conflicts are often asymmetrical, i.e., they no longer take place between state actors. Compared with the building of nuclear weapons, the barriers to entry for a "cyberwarrior" are, of course, far lower. It is true that major cyberwarfare operations, such as the one that damaged Iranian centrifuges by introducing the Stuxnet virus, are only possible when backed by substantial resources at a level generally only available to state actors. However, a far smaller amount of money combined with the necessary skills is enough to cause significant damage.

Terrorist groups have also discovered the digital world for themselves. ISIS makes use of the opportunities offered by cyberspace extensively and effectively: A significant factor in the organization's expansion is its digital strategy (see Munich Security Report 2016). Whether it is recruiting new members, spreading its propaganda messages, or communicating internally, the group known as the "Islamic State" is constantly expanding – not just physically, but digitally as well. As early as 2014, Robert Hannigan, head of the UK's GCHQ intelligence service, warned that social networks had already become the "command-and-control networks of choice" (Financial Times 2014) for groups such as ISIS. At this year's Munich Security Conference, he underscored this observation and called for more active and more effective measures to be taken in the online fight against jihadi terror (see Munich Security Conference 2016).

This battle is also being fought by private hacker groups like Anonymous, which provides a fitting illustration of today's digital battlefield: "Make no mistake: #Anonymous is at war with #Daesh. We won't stop opposing #IslamicState. We're also better hackers." This tweet was sent out by Anonymous after the Paris attacks in November 2015. In other words, a private hacker group operating in a space that was barely there 25 years ago, has declared digital war on the world's most powerful and dangerous terrorist group, which was non-existent just a few years ago. What would have sounded like an absurd description of a conflict not too long ago, is reality today. And this type of asymmetrical, multi-layered conflict will only become more prevalent in the future.

State actors are becoming increasingly active as well – partly in order to develop offensive capabilities and partly to ready themselves for the countless threats they face in cyberspace – and these activities extend far beyond online jihadism. The dissemination of falsified information for the purpose of intentionally manipulating certain segments of the population has become commonplace and is being given a huge boost by the opportunities offered by the online world. This was demonstrated quite recently in the calculated dissemination of false information in the "Lisa Case" in early 2016 (see Federal Academy for Security Policy 2016). Some states maintain entire "troll armies" that comment on news articles or distribute news and opinions favorable to those governments in social media. The ability of the public in our democracies to form opinions suffers as a result, particularly when this

creates alternative public spheres that exist in their own reality, almost entirely walled off from political discourse and the facts.

Another danger stems from attacks on and damage to the institutions of democracy themselves. The large-scale assault on the German Parliament in summer 2015 made this very clear to us here in Germany (see FAZ 2016b). Attacks on critical infrastructure also have the potential to cause untold loss and damage. For instance, more than 700,000 households were temporarily left without electricity as a result of the strike against the Ukrainian power grid in December 2015 (see FAZ 2016a). It is hard to imagine what would happen if such attacks were even more widespread, and mobile communications, transportation and the water supply in densely populated regions were to be crippled in a matter of hours. Speaking on the sidelines of the 2016 Munich Security Conference, the Netherlands' foreign minister Bert Koenders called cyber arms "weapons of mass disruption," in contrast with nuclear, chemical or biological weapons of mass destruction (see Rijksoverheid 2016). Add to that billions in losses for companies as a result of corporate espionage, sabotage and data theft, the cost of which amounts to 51 billion euros each year in Germany alone (see Bitkom 2015), along with other financial losses occurring as "side effects" of digital progress.

Incidentally, such threats are anything but a purely Western problem. The expanding economies of the Global South are particularly vulnerable to the dangers of cyberspace. Often, the digitalization processes in these countries are especially rapid, sometimes occurring without any sort of safeguards whatsoever. A recently published report put economic losses in Kenya due to cybercrime at 146 million US dollars (see Serianu 2015). And South Africa saw approximately 6,000 attacks on its infrastructure, Internet providers and companies in October 2015 alone (see Times Live 2015).

2.2 Challenges for the Political Sphere: Rules, Resources and Expertise

Thus, politicians have to take faster and more effective action against cyberspace threats. One of the most basic problems in this regard is that, in many cases, politicians do not have the necessary expertise in this area. But they must make critical decisions nonetheless. The general public also frequently lacks sufficient understanding and basic knowledge of the topic in view of its complexity and the continual change in cyberspace. This is why we need digital "interpreters" to explain complex processes in simple terms everyone can understand. In the vast majority of cases, today's decision-makers have no affinity for digital issues, let alone professional expertise. And often, there is no common language for dialog between experts and politicians, although this is a basic prerequisite for the implementation of the necessary decisions.

In Germany these days, there is at least awareness of the immense challenges posed by cybersecurity, and initial key steps have been taken. A welcome announcement was made in spring 2016 by the German Federal Ministry of

Defense when it said that the German armed forces (Bundeswehr) would be restructured and a cyberforce added, and that the number of cyberexperts in the Ministry would be massively increased (see Wiegold 2016).

But we still have to ask ourselves whether our efforts are enough. Has society understood how greatly our future security and prosperity will depend on how well-prepared we are digitally? Former US President Barack Obama wanted to earmark line items totaling 19 billion US dollars for cybersecurity in the country's 2017 budget (see Reuters 2016). The British government has announced that it will nearly double its expenditure on cybersecurity over the next five years (see Gov.uk 2015). These are the orders of magnitude in which we must think.

We thus need more expertise, but also more capabilities in terms of resources and structures – well beyond what is called for in the German Ministry of Defense's reform. Universities and other institutions of higher education must be integrated into this effort so that professionals receive training and continuing education at an early stage. Implementation of even the best plans for new cybersecurity structures will fail if we do not succeed in recruiting computer and software specialists, developers and programmers. Thus, one of the key questions will therefore be how to inspire an interest in German military service among younger people who are not necessarily passionately interested in security and defense policy – and how these experts entering the defense ministry can work under Germany's complex public service legislation.

Many significant issues can no longer be resolved by politicians alone: Which technical resources do we have at our disposal for gaining the upper hand over terrorist organizations on the digital battlefield? How can we protect ourselves from attacks by foreign intelligence services that attempt to steal state secrets or sabotage our elected representatives and their independent decision-making process? In order to address these questions together and jointly create the conditions for a free, secure and open Internet, politicians require the support and trust of the private sector and other non-state experts in the field. Last summer, a reporting requirement was introduced in Germany as part of the IT Security Act, which will also be implemented across the EU as part of the Network and Information Security (NIS) Directive. This constitutes another important step toward closer cooperation.

Other questions also remain largely unanswered: What line has to be crossed for cyberattacks to be considered an act of war? How can we respond appropriately to such attacks, and what rules should be followed in carrying out such a response? What happens if there are strong indications as to who is responsible for a massive cyberattack, but no conclusive evidence is available? What implications do these considerations have on Article 5 of the NATO Treaty? NATO has declared that cyberspace will be acknowledged as an independent operational area in the future (see NATO 2016). This could also mean that cyberattacks could trigger the mutual defense clause (see NATO 2015).

Due to the fact that national borders are very fuzzy in cyberspace, transnational forms of cooperation such as NATO play a particularly important role here. Although it is primarily the job of each nation state to guarantee its own security, some responsibilities could be in much better hands at European or NATO level.

In recent years, the practices of some intelligence services have led many Germans to view cooperation with international partners with some skepticism. Particularly their attitude towards the American partner has deteriorated substantially as a result of the NSA affair. According to a survey by the German Marshall Fund, the number of all individuals surveyed in Germany who view the United States positively dropped a full 14 percent points from 2011 to 2014, from 72 to 58 percent (see The German Marshall Fund of the United States 2015). Fortunately, both sides have slowly inched back together in the meanwhile. In May 2015, German confidence in the bilateral alliance had again risen to 62 percent (see Pew Research Center 2015). Some skepticism remains, however, along with fundamental differences in the cyberpolicy of the two countries. This is also reminiscent of the early days of the nuclear age when US allies had to come together before their concerns would be heard by Washington (see Ischinger et al. 2014). For this reason, one of the key objectives must be for Germany and the United States, along with other countries, to build a consensus on the basic pillars of international cyberpolicy. Only based on a clear EU position can we succeed in gradually reaching transcontinental agreement on "reliable rules of the game" (see FAZ 2014) for cyberspace – as called for by Telekom CEO Timotheus Höttges as early as 2014 at the Cyber Security Summit in Bonn, organized by the company and the Munich Security Conference. For several years now, the Munich Security Conference along with Deutsche Telekom has been organizing roundtables and summits on cybersecurity issues, bringing together decision-makers and experts from across the globe, for instance in Silicon Valley in the fall of 2016.

The more sophisticated the possibilities provided by cyberspace become, the more important it is to underpin them with a set of norms and rules. Key here is fundamentally updating international law, which does not yet address or govern cyberwarfare as such. In contrast to nuclear security, for instance, the cyberarena to date has no internationally recognized, multilateral body of regulations that specifically governs the conduct of cyberwar. Nonetheless, some countries, including the two cybergiants – China and the United States – were able to reach initial agreement on the subject of industrial espionage in the fall of 2015. Attempts to arrive at more far-reaching standards for cyberspace have also been underway for some time now. These include the (further) development of the Tallinn Manual, which was initiated in 2009 and elaborated by legal experts from various NATO member states. An initial draft was presented in 2013 (see CCDCOE 2013). However, this standard is not legally binding, and thus international implementation and enforcement of the recommendations have been lacking to date.

Democracies in particular, such as the member states of the European Union, should strive for a free, open and secure Internet as a global public asset. The European Union can still be much more active in this regard and drive the development of international standards. During this process, it will repeatedly run into obstacles. While there already are fundamental differences in cyberpolicy even in transatlantic relations, authoritarian states weigh up security and freedom on the Internet very differently. For this reason, German mistrust of the United States on the issue of data security is largely misguided: We face much greater danger from

other directions. According to information by the German Federal Intelligence Service, the attack on the German Bundestag was steered by Russia (see Zeit 2016). And recently, CIA Director James R. Clapper, speaking before the US Senate, emphasized that, "Russia and China continue to have the most sophisticated cyberprograms" (The Diplomat 2016). Many other countries are also working on offensive cybercapabilities. We are, there is no other way to put it, in the middle of a digital arms race. Precisely for this reason, it is all the more important to work out common minimum standards and fundamental rules as quickly as possible.

2.3 Outlook: A Strategy for the Digital Age

As I wrote at the beginning, in some ways we find ourselves in a situation similar to around 70 years ago, when the invention of the nuclear bomb fundamentally changed the strategic landscape. Although the parallels should not be overemphasized in view of the obvious differences between a nuclear warhead and code, we stand at the beginning of an era of uncertain developments, and that is similar to the post-1945 period. The full effects of new cyber instruments on international security policy and on how wars and conflicts are fought cannot really be foreseen yet. Cyberregulations do not (yet) exist.

But we are experiencing the risks of cyberspace every day. We must seize the opportunity arising from this: the potential for better preparing against these hazards and for developing means of addressing them effectively. For this reason, new approaches are needed. This applies to the national level first of all. The recent restructuring of the German armed forces and the Ministry of Defense is an important step in this regard that must be followed by others. Additional momentum is expected from the new German federal cybersecurity strategy, which will replace the predecessor document written in 2011 (see German Federal Government 2016). At the regional level, what is necessary first and foremost is better coordination within the EU and a drive toward joint initiatives to set comprehensive standards for cyberspace. Ultimately, the greatest challenge appears to be developing and implementing authoritative standards worldwide and agreeing on the basic tenets of international cybersecurity policy.

The process will be long, but it has prospects for success. The attempt in the 1960s to develop rules for the nuclear age was equally complex, but ultimately successful: Steps were taken toward arms control and disarmament, even though the danger was only contained, not eliminated. In this day and age, we must succeed in carrying out a similar international process to develop a common strategy for the significantly more complex digital age. Only then can we ensure together that the potential risks of cyberspace are minimized as much as possible and the numerous opportunities offered by a free, open and secure Internet are realized. It is not yet too late.

References

Bitkom (2015). *Studie zu Wirtschaftsschutz und Cybercrime*. Accessed June 16, 2016, from https://www.bitkom.org/Presse/Presseinformation/Studie-zu-Wirtschaftsschutz-und-Cybercrime.html

CCDCOE (2013). *Tallinn manual process*. Accessed June 16, 2016, from https://ccdcoe.org/tallinn-manual.html

Die Bundesregierung (2016). *Kabinettsklausur in Meseberg – Digitalisierung gemeinsam vorantreiben*. Accessed June 16, 2016, from https://www.bundesregierung.de/Content/DE/Artikel/2016/05/2016-05-24-digitalisierung-meseberg.html

FAZ (2014). *Cyber security summit – Jeder ist bedroht*. Accessed June 16, 2016, from http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/telekom-chef-thimotheus-hoettges-jeder-ist-bedroht-jeder-staat-jedes-unternehmen-jeder-buerger-13243841.html

FAZ (2016a). *Cyber-Sicherheit: Die Hackerdämmerung*. Accessed June 16, 2016, from http://www.faz.net/aktuell/wissen/physik-mehr/ukrainischer-stromausfall-war-ein-hacker-angriff-14005472-p2.html?printPagedArticle=true#pageIndex_2

FAZ (2016b). *Netzangriff auf Bundestag – Es begann mit einer E-Mail*. Accessed June 16, 2016, from http://www.faz.net/aktuell/feuilleton/medien/neue-details-zum-cyberangriff-auf-den-bundestag-14114851.html

Federal Academy for Security Policy (2016). *The Lisa Case – STRATCOM lessons for European States (Security Policy Working Paper, No. 11/2016)*. Accessed June 16, 2016, from https://www.baks.bund.de/sites/baks010/files/working_paper_2016_11.pdf

Financial Times (2014). *The web is a terrorist's command-and-control network of choice*. Accessed June 16, 2016, from http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3rjx7E4aL

Financial Times (2016). *US launches online assault against Isis*. Accessed June 16, 2016, from http://www.ft.com/cms/s/0/4d98edd0-fba5-11e5-b3f6-11d5706b613b.html#axzz4BkAXAl00

Gov.uk (2015). *Chancellor's speech to GCHQ on cyber security*. Accessed June 16, 2016, from https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

Ischinger, W., & Bunde, T. (2014). *Die Zukunft des Westens im digitalen Zeitalter*. FAZ of January 30, 2014.

Munich Security Conference (2016). *Panel discussion "'Daeshing' terror and safeguarding liberties"*. Accessed June 16, 2016, from https://www.securityconference.de/mediathek/video/panel-discussion-daeshing-terror-and-safeguarding-liberties/filter/video/?tx_dreipctvmediacenter_mediacenter[venue]=36&cHash=3c81bfeba609faf81063d1ece9232f09

Munich Security Report (2016). *Munich security report 2016*. Accessed June 16, 2016, from https://www.securityconference.de/aktivitaeten/munich-security-report/

NATO (2015). *Keynote speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO transformation seminar*. Accessed June 16, 2016, from http://www.nato.int/cps/fr/natohq/opinions_118435.htm?selectedLocale=fr

NATO (2016). *NATO Defence Ministers agree to enhance collective defence and deterrence*. Accessed June 17, 2016, from http://www.nato.int/cps/en/natohq/news_132356.htm?

Pew Research Center (2015). *Germany and the United States: Reliable allies*. Accessed June 16, 2016, from http://www.pewglobal.org/2015/05/07/germany-and-the-united-states-reliable-allies/

Reuters (2016). *Concerned by Cyber Threat, Obama seeks big increase in funding*. Accessed June 16, 2016, from http://www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1

Rjiksoverheid (2016). *Toespraak van minister Koenders bij de Münchner Sicherheitskonferenz*. Accessed June 16, 2016, from https://www.rijksoverheid.nl/regering/inhoud/bewindspersonen/bert-koenders/documenten/toespraken/2016/02/12/toespraak-van-minister-koenders-munchner-sicherheitskonferenz

Serianu (2015). *Kenya cyber security report 2015*. Accessed June 16, 2016, from http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf

The Diplomat (2016). *Top US spy chief: China still successful in cyber espionage against US*. Accessed June 16, 2016, from http://thediplomat.com/2016/02/top-us-spy-chief-china-still-successful-in-cyber-espionage-against-us/

The German Marshall Fund of the United States (2015). *Report of the task force on the future of German-American relations*. Accessed June 16, 2016, from http://www.gmfus.org/publications/longstanding-partners-changing-times

Times Live (2015). *It's one hack of a problem*. Accessed June 16, 2016, from http://m.timeslive.co.za/thetimes/?articleId=15801457

Wiegold, T. (2016). *Cyberkrieger, Computernerds und IT-Einkäufer: Bundeswehr stellt sich neu auf*. Accessed June 16, 2016, from http://augengeradeaus.net/2016/04/cyberkrieger-computernerds-und-it-einkaeufer-bundeswehr-stellt-sich-neu-auf/

Zeit online (2016). *Deutscher Bundestag – Hackerangriff wurde aus Russland gesteuert*. Accessed June 16, 2016, from http://www.zeit.de/digital/2016-01/hackerangriff-bundestag-russland-nachrichtendienst-bundesanwaltschaft

Wolfgang Ischinger Ambassador Ischinger is Chairman of the Munich Security Conference and Senior Professor for Security Policy and Diplomatic Practice at the Hertie School of Governance in Berlin.

A graduate in law and international relationships, Ischinger first worked in the cabinet of the UN Secretary-General before moving to the German Federal Foreign Office in 1975.

This included postings to the embassies in Washington, D.C. and Paris, and a period from 1982 to 1990 as a senior assistant to Hans-Dietrich Genscher, the German Minister for Foreign Affairs at the time. From 1993 to 1998, he was Director of the Policy Planning Staff and later Political Director, before serving as State Secretary from 1998 to 2001. He was Ambassador to the USA from 2001 to 2006, and Ambassador to the United Kingdom from 2006 to 2008. He was appointed Chairman of the Munich Security Conference in 2008. He also held the position of Global Head of Governmental Relations at Allianz SE (Munich) from 2008 to 2015.

Ambassador Ischinger represented the EU in the Troika Kosovo negotiations in 2007 and the OSCE in efforts to establish a national dialog in Ukraine in 2014. In 2015, he was appointed Chairperson of an OSCE-mandated Panel of Eminent Persons to strengthen the European security architecture.

He currently advises companies, governments and international organizations. He is a member of the Supervisory Board of Allianz Deutschland AG and Allianz Private Krankenversicherung (APKV), and a member of the European Advisory Council of Investcorp (London/New York). He also serves on the Steering Committee of the German Council on Foreign Relations (DGAP), the Board of Atlantik-Brücke, the Board of Trustees for SWP (Berlin), SIPRI (Stockholm), AICGS (Washington, DC) and The American Academy in Berlin, the Advisory Board of the Federal Academy for Security Policy (BAKS) and the Center for European Reform (London), and the Board of Directors of the Atlantic Council. He received the Leo Baeck Medal in 2008 and was decorated with the Federal Cross of Merit in 2009.

Data Protection Empowerment

3

Peter Schaar

The term "data protection" implies that data requires a protective hand. It therefore comes as no surprise that it is often confused or used synonymously with other terms describing similar subject matter, such as IT security. The fact that this misunderstanding seems almost impossible to clear up is due in part to the unfortunate choice of words. Data protection is not about the protection of data per se, but about the protection of personal data in light of the right to informational self-determination and the preservation of the private sphere – which is why another term for it is data privacy.

Data protection laws impose rules on anyone handling personal data. These protection obligations are directed primarily at the state, although government agencies themselves collect huge amounts of personal data, often on the basis of sovereign authority. It is precisely because of these special powers that the data protection laws applicable to government agencies contain especially detailed rules that simultaneously permit and restrict the collection, processing and use of personal information. Data protection is a fundamental right that places limits on the state's thirst for knowledge, as the German Federal Constitutional Court has repeatedly ruled. Data protection regulations for businesses in general, on the other hand, are quite flexible. Companies are allowed to collect, process and use data as long as this is necessary to accomplish a task – such as concluding and executing a contract – or for other justified purposes. Ultimately, personal data may be processed as long as the person affected has consented to this. With the rise of services that are supposedly free but actually financed through the use of personal data, individuals are increasingly being required to give blanket consent to the extensive use of their data in ways they may not even be aware of. Legally defined powers to collect and use personal data stake out the framework within which entities can gather or process data. But even if the goal of this is to secure a space for

P. Schaar (✉)
Spessartstr. 11, 14197 Berlin, Germany
e-mail: peter.schaar@email.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_3

individuals in which they can, in principle, control "their" data, this alone does not really guarantee the right to self-determination in a technologized world.

When empowerment is brought up in this context, it is not meant in the sense of prohibition and permission, or even of consent, but rather with respect to designing technology so that control over personal data is returned to the individual.

3.1 Code Is Law

Digital systems whose functionality is determined by hardware and software have at least as much influence as legal regulations when it comes to the options available to the individuals who use these systems or whose data is processed by third parties. "Code is law" – this provocative but nonetheless accurate statement made by Lawrence Lessig (see Lessig 1999) in the last year of the 20th century is more relevant now than ever before. The design and configuration of hardware and software determines what data is collected and how it is handled. The technical decisions made when a system is designed therefore have a decisive influence on what data is gathered and stored, who can access it, and how humans will interact with the machines in question and with other humans. This is not only, or even primarily, about individual pieces of (personal) data, but rather about structural decisions that have an impact far beyond the actual data processing itself. The people in charge of the technology also have the power of decision over how information is used. And they use this "data power" to gain economic or political advantages. As a result, the individuals who use this technology and whose data is processed increasingly become objects.

The mechanisms implemented in hardware and software are moving closer to people and defining more and more aspects of their everyday lives. Smartphones, intelligent kitchen gadgets and digitally controlled heating systems are becoming a norm that only hard-nosed nostalgics try to avoid. Radio-controlled pacemakers and other implants not only measure vital signs, they can also actively influence our health.

An epochal change is currently underway, one driven by increasingly powerful information technology: In the age of Small Data, (personal) data was the material used in processes designed to fulfill a certain task, but the focus of Big Data is to amass as much data as possible (data maximization) and link it beyond the context in which it was originally gathered. The principles of necessity and purpose underlying the classic data protection model are increasingly coming under pressure. Since Edward Snowden's revelations at the latest, no one can deny that the triumphant advance of the Internet, not to mention the Internet of Things, has heralded a golden age for public and private data collectors, leaving individuals relatively helpless in the face of it.

This situation is diametrically opposed to the fundamental right to informational self-determination, which was established by the German Federal Constitutional Court in 1983 in its famous population census decision. "In the context of modern data processing," this fundamental right guarantees.

> "... in principle the power of individuals to make their own decisions concerning the disclosure and use of their personal data." (BVerfG 65,1, p.1, headnote 1)

This ruling was based largely on the Court's assessment "that, since personally identifiable information could be collected and processed automatically, individuals must not become mere informational objects." Data processing conditions had to be defined in a way that preserved human dignity and guaranteed the free development of personality. If people had to fear that every aspect of their behavior might be recorded and compiled to create a personality profile, they would not be able to develop or make decisions freely. Instead, they would waive the exercise of certain rights and avoid behaviors that could potentially have negative consequences for them. The Federal Constitutional Court confirmed and expanded upon this view in a number of other rulings. Of particular note here is a decision from 2008 defining a fundamental right to safeguards regarding the confidentiality and integrity of information technology systems (known as the IT Basic Law).

In light of this, data protection cannot and must not be restricted to defining legal limits for processing individual pieces of data. Instead, it must be about designing information technology in compliance with basic rights. The preconditions for this are not all that bad, as the new world of IT offers several points of departure for designs that are compatible with data protection. Unlike the classic mainframe-based data processing systems in the data centers of the 20th century, which operated beyond the reach of the people affected by them, individuals in the 21st-century world of IT are increasingly "users" and thus actors in these information technology systems.

But while it is true that digitalization is leading to growing masses of data – with the corresponding hazards – we must not forget that this same development harbors opportunities for informational self-determination. Unlike the computer dinosaurs in mainframe data centers, modern technical devices are often within our grasp, or at least within our virtual reach. So why not give the affected individuals – us, the users – far more ways of controlling them?

This is why questions about the design, functionality and embedding of information technology have taken on existential significance for the future of society and the personal development of the individual. As "code" influences our life more and more, the question of who determines the code and which rules it follows becomes increasingly important.

3.2 Empowerment

The realization that there is a connection between the legal and technical demands placed on information technology is not new. The basic ideas behind "privacy by design" go back to the 1990s. Under the heading of privacy-enhancing technologies (PET), the Dutch data protection expert John Borking developed a coherent system of information technology measures for avoiding or eliminating personally identifiable data (see IPC 1995). But this concept of data avoidance or data minimization, which

has been anchored in the German Federal Data Protection Act since 2001, has barely gained a foothold in practice, especially because economic interests and (at least since the terror attacks of September 11, 2001) public and national security needs have taken precedence.

But as IT systems grow more powerful, it is worth dusting off some of these approaches to privacy-friendly technology design, developing them further and bringing them to life. Now more than ever, technical tools are the only way to rein in the rampant collection, correlation and evaluation of data without foregoing the advantages of using IT. Interactive, multiply networked IT structures and the services provided through them are highly designable. In many cases it is possible to find solutions that allow users or the people concerned to gain or regain control over their data without impacting functionality. Such approaches could center on intelligent devices, such as smartphones, that manage our data protection preferences and enable us to monitor and control where our data is sent.

The P3P (Platform for Privacy Preferences) approach developed more than 15 years ago could be a good starting point for this type of data protection agents. This is an internationally standardized platform (created by the WWW Consortium) for exchanging data protection information for websites. P3P is supposed to give web users a fast, automated overview of which personal data is being processed by website operators or third parties and for what purposes. Users specify their preferences for the protection of their own data in a P3P agent, such as a P3P-enabled browser. The software agent compares these user preferences with the website operator's standardized description of its data processing practices. If there are any discrepancies, the user is alerted. In this case, the website can only be accessed – and the data transferred – if users explicitly release their data.

This model could also be applied to the Internet of Things. However, it would have to be standardized and implemented in the software. For example, a transparent energy management system could be established for digital electricity grids, without energy suppliers or Internet service providers such as Google gaining access to the usage details for devices connected to a smart meter in a household. The decisive factors here, as in other fields of application for smart technologies, are where the data converges, who can access it and who can use it. It is clearly useful for energy users to have more knowledge about their consumption so that they can take action accordingly – with regard to useless standby settings, for example, or replacing power-guzzling electrical appliances. Energy suppliers, on the other hand, do not need to know the details of individual device usage or room thermostat settings in order to plan their network load distribution or to feed energy into the grid. They only need to be aware of the load development in each network segment – not even in each individual household. A privacy-friendly solution could send detailed consumption values to a user's smartphone. If third parties were interested in this data, it would only be sent to them after the user had explicitly consented to this.

Intelligent driver assistance systems can work without centrally collecting data about an individual driver's location and driving habits. Navigation systems can also identify traffic jams without recording personalized driving behavior. We already have powerful systems for measuring traffic loads which use pseudonymized and anonymized data, or even get by without any personal data whatsoever – such as the

"smart traffic lights" and traffic routing in the city of Mannheim. As in the case of the electricity network, users should have extensive control over the detailed data they generate in intelligent vehicles. In any event, there must be no chance that this information could be sent to third parties behind the user's back.

In principle, technical systems must be designed to get by without personal data and give individuals the power of decision over their own data. If individualized data has to be stored – for fitness trackers or health apps, for example – there must be a guarantee that the data will be stored under the users' control and only sent to third parties under the conditions stipulated by the users themselves. The widespread practice of automatically storing such data in a cloud controlled exclusively by the provider is highly problematic from the standpoint of data protection laws.

Since individual identity data is generally not needed for data analyses, anonymized data is usually sufficient here. An "intelligent car" equipped with information technology can measure any number of environmental and driving parameters. But much of this data is needed only for a very short period of time, sometimes for just a few seconds. Systems should be designed in a way this information is deleted or at least anonymized once it has served its purpose. If further analyses are to be conducted with the data, the driver or owner must be informed in advance and technical protection measures must be in place, such as anonymization technology. Anonymization and, in some cases – such as long-term medical studies – the use of pseudonyms should become standard practices, with deviations permitted only in special cases and with the full knowledge of the affected individuals. Anonymization and the creation of pseudonyms should be decentralized as much as possible and should not take place on the server side.

Cryptographic methods that protect confidential information from being monitored and recorded are also very important. Efforts to prohibit encrypted communication and install backdoors in information technology for the use of intelligence agencies and other authorities are counterproductive. They interfere with the right to informational self-determination and they weaken IT security – and not just when it comes to exposing criminal activity. With cryptography, too, there must be a stipulation that cryptomaterial – especially the keys that are used – will be generated and managed under the user's control.

Approaches such as P3P and the Do Not Track standard on the web are steps in the right direction, but they must be developed further and, above all, actually implemented. They are essentially limited to the message that Internet services should honor the private sphere. To this day, many websites still ignore the browser preferences set by users. Some "data privacy statements" even say that providers are not prevented from collecting much larger amounts of personal data than the users desire. Future data protection technologies must effectively prevent the disclosure of personal information if this is what the user has requested. The technology used in the latest ad blockers shows that this can work. Additionally, the corresponding measures must be legally enforced – and the opportunities for legal enforcement will rise with the recently adopted European General Data Protection Regulation, which calls for much harsher sanctions against data protection violations than previous data protection laws.

3.3 Information Technology and Social Values

The extent to which we are able to take the achievements and values of civilization into account as our lives are digitalized will determine the character of the information society towards which we are moving at an ever-faster pace.

The success of this also depends on the design of the technology. The "civilization" of IT will only be possible when people – as citizens and consumers alike – can move within a framework of trust in information technology. They must be confident that the technology complies with key rules and regulations, and that the usage conditions are stable. Only then will they be able to rely on the trustworthiness of information technology systems.

All considerations about the future of the information society must center on the individual and his or her right to self-determination and opportunities for personal development. Self-determination is the ability of individuals to control their informational image. Individuals should also have access to technologies that allow them to make their own decisions regarding what they want to reveal about themselves.

References

BVerfG (1983). *Decision from December 15, 1983 (Census decision)*. Accessed June 20, 2016, from http://openjur.de/u/268440.html

IPC (1995). *Privacy-enhancing technologies: The path to anonymity* (vol 1). Accessed June 20, 2016, from https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329

Lessig, L. (1999) *Code and other laws of cyberspace* (p. 5). New York: Basic Books.

Peter Schaar is Chairman of the European Academy for Freedom of Information and Data Protection (EAID). He is also President of the Arbitration Body of the Germany Society for Health Insurance Card Telematics Applications (gematik). 2003–2013 he has been a German Federal Commissioner for data protection and freedom of information. Schaar is the author of numerous publications, including "Datenschutz im Internet [Data Protection and the Internet]" (2002), "Das Ende der Privatsphäre [The End of Privacy]" (2007), "Total überwacht – Wie wir in Zukunft unsere Daten schützen [Total Surveillance: Protecting our Data in the Future]" (2014) and "Das digitale Wir – Der Weg in die transparente Gesellschaft [Our Digital Selves: Becoming a Transparent Society]" (2015). His work has received many accolades, including the Political Book Prize from the Friedrich Ebert Foundation and the eco Internet Award in 2008, the GDD's German Data Protection Prize in 2013 and the Louis D. Brandeis Privacy Award in the following year.

Red Teaming and Wargaming: How Can Management and Supervisory Board Members Become More Involved in Cybersecurity?

4

A Traditional Military Approach Applied to Strategy Development in the Field of Cybersecurity

Marco Gercke

4.1 Cybersecurity: A Management Board Issue

When Deutsche Bahn CEO Rüdiger Grube in 2013 was quoted as saying that cybersecurity at his company was a management board issue, not something left to the system administrators (see van Zütphen 2013), this was something out of the ordinary as cybersecurity did not count as a traditional board issue at the time. These days Grube is in the best of company, because the topic of cybersecurity is now on the management board agenda of an increasing number of enterprises. A group of CEOs from 23 German blue chips even discussed it at length at the 2014 Munich Security Conference (see Gercke et al. 2014).

In view of the growing number of attacks on large companies (see Tsukayama 2012) and SMEs (see Securitymagazine 2013) that could jeopardize their future, integrating the management board is a logical move. Even if there is disagreement with regard to the number of attacks, management board members of large companies can ill afford to ignore the threat, in particular because of the liability risk it entails. For stock corporations there is even a legal framework from which the obligation can be inferred. Section 91(2) of the German Stock Corporation Act (AktG) sets out that the management board must establish a suitable risk management system to ensure that developments threatening the survival of the company are detected – as part of the ordinary management of business as defined in Section 93(1) AktG. While the wording of the law does not contain an explicit obligation with regard to cybersecurity, it is widely accepted in literature that cybersecurity is a component of risk management and that a breach of duty under Section 91(2) AktG may lead to the members of the management board being held

M. Gercke (✉)
Cybercrime Research Institute GmbH, Niehler Str. 35, 50733 Cologne, Germany
e-mail: gercke@cybercrime.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_4

personally liable (see Bürgers and Israel 2014; Trappehl 2009; von Holleben and Menz 2010).

4.2 Integrating the Management Board into Existing Cybersecurity Strategies

One challenge for companies in general and for their management boards in particular is determining how to integrate management board members into the company's overall strategy. In contrast to the technical aspects of cybersecurity, where standards such as ISO 27001 provide clear structures, there is a lack of appropriate guidance on the involvement of management board and supervisory board members. One of the main issues must be to clarify a company's own cybersecurity strategy to incorporate the decision-makers in a meaningful way, at least when the companies wish to develop a serious strategy – something that is not always the case.

A detailed look at the cybersecurity strategies of countries and private companies reveals that, to this day, the relevant documents are frequently relatively short and focus less on concrete instructions and more on declarations of intent. What is actually needed are strategies that in addition to basic statements contain clear guidelines on responsibility, processes, and technical specifications (see Gercke 2013: 136–142).

When such a complex strategy is being developed, important questions in connection with the inclusion of the management board almost inevitably arise. For example: Which incidents invoke the board's responsibility? While nobody will seriously notify the management board of every single IT incident that occurs at a large company, mundane events may at the same time provide the gateway for complex attacks. Any delegation of responsibilities that has already taken place – for instance from the management board to a crisis unit that becomes active in an emergency – may also be significant in this respect.

4.3 Red Teaming and Wargaming

Since the structures in companies and companies' institutional capacity generally do vary considerably, it is extremely difficult to develop and implement a method for the integration of management board members as a universal blueprint. Customization is what is required here, especially for large companies, which tend to have more complex structures. The question is whether and how the management board can be incorporated in a cybersecurity strategy using military approaches such as red teaming and wargaming.

4.3.1 Red Teaming Defined

Red teaming or alternative analysis is a specific method used to review plans, strategies, and hypotheses (see Fryer-Biggs 2012; Herman et al. 2009; Lauder 2009; Longbine 2008; Sabin 2012). Two teams are formed, a Red Team and a Blue Team (see Wood and Duggan 2002). The Red Team assumes the role of the attacker, while the Blue Team focuses on defense (see CSO 2008). This method has been successfully employed by the military for decades (see Lauder 2009; Longbine 2008) and has also been applied in civil activities for a number of years (see Lauder 2009). It is explicitly not restricted to acting out physical attacks. The methodology can also be used to investigate theoretical issues from different angles and with varying emphases – reaching as far as intangible constructs such as a legislative draft (see Gercke 2014).

Red teaming can be particularly useful when developing cybersecurity strategies, since the attack situation reflects the real threat situation. However, strategies are mostly developed from the defense angle. A change or expansion of perspective enables a company's own strategies to be examined more critically.

4.3.2 Wargaming Defined

Wargaming is the dynamic simulation of genuine threat situations (see Herman et al. 2009; Sabin 2012; Perla 1990; Oriesek and Schwarz 2009). Using simulated situations like this, strategies can be safely tested under realistic conditions. What makes this approach special is its dynamic nature, which is frequently lacking in conventional strategy developments. Another major advantage of simulations is the fact that they create a more realistic environment. In other approaches like the table desk exercise, discussion does take place, but factors such as stress and strain are not taken into account. It is things like this that can generate realistic simulations.

It is therefore not surprising that simulations and wargaming are used not only in a military environment but also in preparing non-military decision-makers (see Herman et al. 2009; Oriesek and Schwarz 2009; von der Gathen 2014). Wargaming offers numerous advantages, particularly in the field of cybersecurity. In cybersecurity incidents, important information about the scope and effects is often unavailable initially. An analysis of attacks also shows that such incidents are becoming increasingly complex. Decision-makers therefore need to come to grips with the situation that decisions must be made rapidly and in some cases on the basis of not very reliable facts.

4.3.3 Differences Compared with Methods Currently in Use

Up to now, companies have often fallen back on theoretical approaches when developing strategies in general and integrating decision-makers in particular, with advisors normally stating where they personally see vulnerabilities and

potential for improvement. In many cases, the effects of vulnerabilities are also underpinned by specific examples. However, it is unusual and unnecessary in these formats for the people involved to adopt the perspective of an attacker and consciously attempt to exploit the weaknesses of a strategy for attacks. In traditional approaches, a change in perspective like this is often regarded as counterproductive and not expedient.

The potential of red teaming can be explained using the following example: Is it possible to improve draft legislation through red teaming? At first glance, attacks and legislative procedures appear to be rather incompatible concepts. In a state under the rule of law, however, statutory limits serve as a very important reference point that guide the actions of individuals or organizations and companies. Testing the legal boundaries is often of paramount importance for companies in particular. Loopholes in the law can mean that certain behaviors in exactly this relevant peripheral area might pass unnoticed. Putting oneself in the position of an attacker who is specifically searching for vulnerabilities can make precisely these consequences visible.

This example may sound highly theoretical, but practical experience has been gained with this very concept. Some years ago, red teaming was used as a strategy for the improvement of legislation in the area of cybersecurity in connection with an EU/ITU-funded project for over 50 countries in the Caribbean, the Pacific, and Asia (see Gercke 2013). It was shown that red teaming often brings other vulnerabilities to light than those brought up in round tables with experts. The point was clearly made that possible vulnerabilities in a law can be specifically used for attacks. This was far more impressive and generated a great deal more support in the legislating target group than an academic discussion of dogmatic and legislative problem areas (see Gercke 2014).

Similar experience in connection with cybersecurity has already been gained in the area of wargaming. For example, the dynamic approach of making the practical effects of cyberattacks identifiable was used in 2015 and 2016 at the Munich Security Conference to show participants the threat posed by present-day attacks. While the focus was on members of government and decision-makers from the military and security sector, there are also comparable developments in industry, where management board members use wargaming to prepare for decision-making in the event of an attack (see van Zütphen 2013).

4.4 Use of Red Teaming in Combination with Wargaming at Companies

As noted above, red teaming is designed to improve an organization's planning, operations, and responsiveness. Red teaming reviews the efficiency of existing or chosen strategies by exposing them to a simulated attack. The aim is to find vulnerabilities in existing, ideally field-tested concepts that have been perpetuated and updated over a longer period of time and to anticipate the effects of certain actions. During red teaming, the protagonists explicitly adopt an external

perspective. Seeing things from the perspective of an attacker, competitor or adversary allows vulnerabilities to be identified, avoiding cognitive processes that lead to findings being selectively evaluated or disregarded.

In this respect, red teaming builds on a critical point of strategy development: influencing the critical perceptive faculty of the actors involved in the development process. Vulnerabilities are reviewed each time a strategy is developed, but in traditional approaches this takes place from the perspective of those who were involved in the actual design. This carries the risk of selective consideration, which is unconsciously focused on confirmation of the preceding work. Einstein impressively paraphrased the fundamental problem of the approaches that red teaming tries to circumvent when he said, "We cannot solve our problems with the same thinking we used when we created them."

Red teaming offers particular potential in the field of cybersecurity, which generally involves two opposing parties – attacker and target. Yet it must be remembered that red teaming is usually only effectively deployed as part of the development of an overall strategy, not in isolation. This is because the advantage of a realistic review of processes and strategies is partly offset by the disadvantage that time constraints do not allow all attack vectors to be determined and that the respective report also represents a snapshot (see Furtuna et al. 2010).

4.4.1 Classification

Generally speaking, a red teaming approach can be divided into five phases. A combination of red teaming and wargaming results in the following:

1. Definition of a target
2. Composition of the teams
3. Analysis
4. Wargaming
5. Report

The phases may be part of an iterative process and may vary largely depending on their specific implementation.

4.4.2 Definition of a Target

Red teaming begins with the definition of a target (see Furtuna et al. 2010; University of Foreign Military and Cultural Studies 2002). In relation to the integration of the management board, red teaming can specifically address issues such as overlapping responsibilities within a management board or vulnerabilities in reporting processes from middle management. Defining a specific task is of vital importance, especially because of the range of possible deployment. Usually when

the task is being defined, the simulated attacks are authorized at the same time (see Furtuna et al. 2010).

4.4.3 Composition of the Teams

Depending on the task defined, the two teams are then put together (see Wood and Duggan 2002), with an attacking team normally pitted against a defending team, as described above (see Herman et al. 2009). Depending on the target defined, it is certainly also possible to use just the attacking team in order to identify vulnerabilities independently of a defense or to review internal resources (see Furtuna et al. 2010). However, the combination of an attacking and a defending team allows defense readiness to be reviewed at the same time.

The success of red teaming depends to a large extent on the team's composition. In addition to professional qualifications, the interpersonal skills of the team members are pivotal in this context (see University of Foreign Military and Cultural Studies 2002). Particularly in the area of cybersecurity, it is important to have subject-area experts in the team (see CSO 2008). Depending on the emphasis, teams may comprise members from a variety of disciplines and professions – such as technical security specialists, management consultants, members of the legal department, strategy advisors, risk managers, psychologists, analysts, experts in simulations and operations research, etc. If the internal resources available in the company are limited or very tied up, an external service provider may take on the role of the attacker.

4.4.4 Analysis: Data Collection and Evaluation

The third phase, which focuses on the collection and evaluation of data (see University of Foreign Military and Cultural Studies 2002), forms the core of the red teaming. By collecting available data on the target of the attack, the attacking team develops its strategy. Task definition can focus on a specific area. The methods used to collect data also vary considerably: Either the necessary information can be supplied to the attacking team or the team has to procure this itself. When it comes to verifying the security of information systems, the measures may range from peer reviews to ethical hacking, where the hacker is hired to actually attack an information system (see Lauder 2009). When integrating management board members into a cybersecurity strategy, developers mainly concentrate on the evaluation of responsibilities, the focal points of delegation and on reporting. In general, making information available to the attacking team prior to the exercise not only saves time, but may be a prerequisite for effective deployment of external experts in particular (see IBM 2005). However, supplying the data radically limits the scope of action for the attacking team.

The decision as to which techniques will be used to collect and evaluate data depends on the task previously set. Typical questions include the following: Have

all options and the consequences of a certain approach been considered? Which alternative courses of action exist? Which effects do the actions of others have on a company's own actions? How flexible is the company's own planning? Which of the company's own courses of action has the highest probability of success? Specifically in relation to the integration of management board members, one question could be whether the correct parameters establishing management board responsibility have been chosen.

4.4.5 Wargaming

Red teaming is most effective when it is not solely limited to an analysis of vulnerabilities but is combined with a simulated attack. The method can only be used to its full effect if the Red Team takes the external perspective of an attacker and the typical approaches of an attacker can be applied. In an ideal scenario, the attacking team benefits from its extensive experience in the selection and use of critical, creative methods for the analysis of complex issues and the assessment of different courses of action and is therefore not confined to the mere identification of vulnerabilities.

Developing vulnerabilities into attacks forces attackers not to confine themselves to theoretical concepts but to actually implement attack scenarios based on the identified vulnerabilities. Practical experience shows that nowhere near all vulnerabilities can be automatically transformed into an attack scenario. For example, external attackers may be unable to exploit a vulnerability in an internal system. In this respect, validating that vulnerabilities can actually be used to carry out an attack is a key component of the red teaming process (see Furtuna et al. 2010). Yet in many cases an actual attack is neither possible nor expedient. Using the wargaming methodology, the attack is carried out in a controlled environment in which the actual attack situation is recreated realistically. If the technical side of an attack on information systems is simulated, this may require replication of existing technical structures in a laboratory environment. However, if the decision-maker's basic defense strategies are to be reviewed, the focus is more on the provision of realistic reporting structures rather than on the replication of a technical system.

The simulation approach has proven particularly effective in interaction with members of the management and supervisory boards of large companies. For this approach to work, the decision-making structures in companies need to be depicted realistically. Decision-making processes can then be simulated in both management and supervisory boards. This has the advantage that in just two or three hours the participants can not only be shown the bandwidth of attacks, but the decision-maker's defense readiness can be reviewed and the consequences of decisions can be demonstrated at the same time. Simulations can also provide concrete assistance in process improvement via additional measures, such as language analyses or the recording of data that tracks stress levels.

4.4.6 Report

The last phase involves documenting the entire process. Recommendations for action are often included. The resulting overview of the situation can be used immediately to improve plans and strategies.

4.5 Conclusion

Whereas in the past red teaming and wargaming were primarily used in a military environment and by large companies, the methodology can be easily transferred to the optimization of companies' cybersecurity strategies, particularly the integration of management board members.

References

Bürgers, T., & Israel, A. (2014). *Kommentar zum AktG, 2998, § 91, Rn 12*, in Bürgers, Tobias; Körber, Torsten: Heidelberger Kommentar zum AktG, 2998. C.F. Müller.

CSO (2008). *Red team versus blue team: How to run an effective simulation*. Accessed June 20, 2016, from http://www.csoonline.com/article/2122440/emergency-preparedness/red-team-versus-blue-team–how-to-run-an-effective-simulation.html

Fryer-Biggs, Z. (2012). *Building better cyber red teams*. Accessed June 20, 2016, from http://www.thecre.com/fnews/?p=944

Furtuna, A., Patriciu, V.-V., & Bica, I. (2010). *Considerations about red teaming usage in assessing information assurance*. Bucharest.

Gercke, M. (2013). *Cybersecurity strategy, why it is necessary to move from cybersecurity philosophies to true cybersecurity strategies*. CRI 5, 15 ff.; 136–142.

Gercke, M. (2014). *"Red Teaming" Ansätze zur Effektivierung von Gesetzgebungsprozessen? Die Übertragbarkeit einer klassischen, militärischen Methodik auf Gesetzgebungsprozesse im IT-Bereich*. CR 5, 344–348.

Gercke, M., Laschet, C., & Schweinsberg, K. (2014). *Cyber-Risiken als Teil unternehmerischer Leistungsverantwortung*. PHI, 76.

Herman, M., Frost, M., & Kurz, R. (2009). *Wargaming for leaders: Strategic decision making from the battlefield to the boardroom*. New York: McGraw-Hill Education.

IBM (2005). *Red teams: Towards radical innovation*. Accessed June 3, 2016, from http://www-935.ibm.com/services/us/imc/pdf/gt510-6190-red-teams.pdf

Lauder, M. (2009). *Red dawn: The emergence of a red teaming capability in the Canadian forces*. Canadian Army Journal, 12(2), 25–36.

Longbine, D. F. (2008). *Red teaming: Past and present*. Fort Leavenworth: Kansas.

Oriesek, D., & Schwarz, J. O. (2009). *Business Wargaming: Unternehmenswert schaffen und schützen*. Wiesbaden: Gabler Verlag.

Perla, P. P. (1990). *The art of wargaming: A guide for professionals and hobbyists*. Annapolis: US Naval Institute Press.

Sabin, P. (2012). *Simulating war: Studying conflict through simulation games*. New York: Bloomsbury Academic.

Securitymagazine (2013). *$1.5 Million Cyberheist Ruins Escrow Firm*. Accessed June 3, 2016, from http://www.securitymagazine.com/articles/84617-15-million-cyberheist-ruins-escrow-firm

Trappehl, B. (2009). *Arbeitsrechtliche Konsequenzen von IT-Sicherheitsverstößen*. NZA, 18, 986.
Tsukayama, H. (2012). *Report: Chinese hackers breach Nortel networks*. Accessed June 3, 2016, from https://www.washingtonpost.com/business/technology/report-chinese-hackers-breach-nortel-networks/2012/02/14/gIQApXsRDR_story.html
University of Foreign Military and Cultural Studies (2002). *Red team handbook*. Accessed June 6, 2016, from http://www.au.af.mil/au/awc/awcgate/army/ufmcs_red_team_handbook_apr2011.pdf
van Zütphen, T. (2013). *Vorstandsthema Cyber Crime? So sicher wie der nächste Angriff*. Best Practice, 3, 45.
von der Gathen, A. (2014). *Das große Handbuch der Strategie Instrumente*. New York: Campus Verlag.
von Holleben, K. M., & Menz, M. (2010). *IT-Risikomanagement – Pflichten der Geschäftsleitung*. CR, 1, 63–68.
Wood, B., & Duggan, R. (2002). *Red teaming of advanced information assurance concepts*. In DARPA Information Survivability Conference and Exposition, 2002. DISCEX 00 Proceedings (Vol 2, p. 112 ff).

Marco Gercke is one of the world's foremost experts in cybersecurity and cybercrime, having given over 500 papers in more than 80 countries. Gercke is Director of the Cologne-based Cybercrime Research Institute and teaches media criminal law and European criminal law in the Law faculty at the University of Cologne. He is also an external lecturer in the master's program in information law at the University of Oldenburg and visiting professor in international criminal law at the University of Macau (China). His work focuses on advising international organizations – in particular, the United Nations, UNODC, ITU, UNICEF, UNIDIR, UN-CTITF, the European Union, ECOWAS and the European Council – as well as national governments, ministries, experts and large corporations on legal and political issues in connection with cybersecurity. The performance of simulations is a material aspect of this work. Gercke is the author of over 100 publications and has given many expert opinions in comparative law. His most recent monograph was published in six languages.

The Law and Its Contribution to IT Security: Legal Framework, Requirements, Limits

5

Klaus Brisch

Technology is the main way of ensuring that IT security meets perpetrators on a level playing field with weapons of a similar caliber. But technology cannot solve the problem alone. The law can also play a part in IT security, although it is misguiding to assume that legal sanction mechanisms will keep criminal hackers from infiltrating IT infrastructures and harming companies.

In fact, criminal prosecution is quite a blunt instrument, and international legal systems for the prosecution of criminal activities are out of tune with high-tech reality. The level of sophistication possible with technology far exceeds the bounds of our current legal framework. For this reason, legislators concentrate on those who have something to protect and something to lose, i.e., IT users in companies and households. By focusing on users, there is a reasonable expectation of success: They are likely to obey the law and implement the required technical and organizational measures.

From a legal policy perspective, the question then arises as to whether the law and its control mechanisms can possibly address the risks adequately. Can legal responsibility and liability in fact create incentives for IT companies, users, and service providers to effectively combat IT risks?

Are questions of

- duties (who must implement which measures?),
- liability (who is liable when risks materialize, and to what degree?), and
- evidence (who must prove which facts in a dispute?)

asked in a way that aligns with the approach taken by the German Federal Office for Information Security (see BSI 2007)?

K. Brisch (✉)
DWF Germany Rechtsanwaltsgesellschaft mbH, Habsburgerring 2, 50674 Cologne, Germany
e-mail: klaus.brisch@dwf.law

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_5

5.1 Key Features of the Existing Legal Framework

Prior to the entry into force of the German IT Security Act, the only comprehensive IT security regulations in effect for companies of various sizes in various industries stemmed from data protection law or involved the implementation of IT security standards. Since the IT Security Act only applies to companies of certain sizes in certain industries, and merely supplements the general legal framework instead of replacing it, this regulation will be outlined first.

Broadly speaking, the law first and foremost calls for corporate IT suppliers and users alike to set up and maintain data protection systems and to define IT risk management procedures. The focus here is on following IT compliance rules, not least to prevent a company's management board and executives from being held personally liable.

5.1.1 IT Compliance: A Challenge for Management Boards and Executives

According to the definition of "compliance" in the German Corporate Governance Code, "the management board is responsible for ensuring that the applicable statutory provisions and internal company policies are followed, and must work toward adherence by group companies." (Regierungskommission 2015).

Technical standards pertaining to IT are particularly relevant and include the applicable ISO 27001 standard and the IT Baseline Protection Manual (*IT-Grundschutzkataloge*) published by the German Federal Office for Information Security (BSI). These must be complied with although they are not specifically "statutory provisions" or "internal company policies:" Technical standards come into play when the courts need to get to the bottom of statutory standard of care requirements or resolve liability issues. Typical examples are data loss in businesses or a lack of IT availability leading to production or other losses. That is when courts review whether "customary" standards were followed. These standards are considered generally accepted technical guidelines which carry what is known as a "presumption of conformity." According to this concept, a release from liability is justified if such guidelines are adhered to.

5.1.1.1 The Cornerstone of IT Compliance: IT Security

Documenting IT risks is paramount to IT security. A distinction is drawn here between

- organizational,
- infrastructural, and
- application- and process-related risks.

Organizational risks include situations where an IT department is not sufficiently integrated into the corporate structure as an independent entity. Often, the IT organization's responsibilities and requirements are not assigned appropriately in terms of knowledge and skills. Moreover, sensitive data may not be adequately protected to prevent unauthorized access.

Infrastructural risks include the use of heterogeneous or legacy operating systems, data, backup systems, or software packages. This category also includes the technical systems in buildings required to safeguard IT operations, such as suitable protection against water and fire damage, as well as access controls. Finally – and this is pretty much a classic – it is an infrastructural risk when a company has no method of data backup in place or when data backups are only performed sporadically. In practice, users often overlook the fact that backing up data alone is not enough. Rather, it must be possible to seamlessly restore backups to the original IT platform.

Application- and process-related risks can amplify organizational or infrastructure-related risks if a company runs legacy or standalone applications. For example, developers who previously customized off-the-shelf software often leave a company to find other employment. If the customization is not documented, the modified applications can no longer be updated.

5.1.1.2 Liability of the Management Board and Executives

Discussions of IT risk bring up the issue of liability risk for management boards and executives. According to section 93 I of the German Stock Corporation Act (*Aktiengesetz – AktG*) and section 43 of the German Private Limited Companies Act (*GmbHG*), managers of companies are liable for the resulting loss if they breach their duties. To prevent this from happening, they must safeguard the company's interests and protect it from damage while acting within the law and the articles of incorporation, and taking into account the interests of the public. Management must therefore ensure that IT-related legal requirements, particularly data protection regulations, are followed. What's more, if the technical standards relevant to IT security are not adhered to in a corporate setting, the courts consider management personally liable.

5.1.2 Who Is Responsible?

Aside from the question of who is responsible for setting up a fully compliant corporate structure, the division of responsibilities for IT security in the IT value chain is also critical.

5.1.2.1 Requirements for Software Manufacturers

The main laws relevant to software manufacturers are those regarding product liability and product safety. A unique aspect of product liability is that neither a contract between the producer and the user of the product, nor a finding of fault (intent or negligence) is required for producer liability to apply. However, the problem is the unsolved issue of whether software can be classified as a product

in the sense of product liability law, in which case intent or negligence would indeed not be conditions of liability. The same problems as with product safety law arise in general tort liability where, in contrast to product liability, the exact crucial point is a finding of fault due to intent or negligence. After all, financial losses are only determined in exceptional cases and a broad interpretation of the concept of property – not yet handed down by the highest courts – would be required to determine damage to data records or databases.

In practice, the company suffering the loss bears the burden of proving that the software is defective, just as it does for proving a link between a defective product and the violation of a legally protected interest as well as the losses in question – an immensely difficult task to accomplish. The complexity of IT systems and infrastructure in companies and the interplay between various products and IT services often do not permit determining one distinct cause of error. In addition, installation or operating errors by the business suffering the loss must be ruled out.

5.1.2.2 Requirements for Network and Platform Operators

Although they enjoy broad liability privileges provided by the German Telemedia Act (*Telemediengesetz – TMG*), network and platform operators must fulfill extensive duties to secure their own IT systems. Section 44a of the Telemedia Act provides those operating their own electronic communication networks to provide telecommunications services with additional liability privileges.

However, these liability privileges do not apply with respect to third parties who suffer losses via the operator's networks. That is because there is no contractual relationship between them, which section 44a of the Telemedia Act requires.

5.1.2.3 Legal Framework for Providers of IT Services

Businesses that provide IT services or manufacture products with the help of IT systems must fulfill numerous duties of protection arising from specific requirements. An example here is online banking, where a comprehensive set of administrative instructions by the German Federal Financial Supervisory Authority (BaFin) stipulates extensive Minimum Requirements for Risk Management (MaRisk) at German banks.

The IT Security Act

Since July 25, 2015, the IT Security Act has been established in Germany. It provides the Federal Republic with a head start regarding a solid legal basis for cyber security. According to the law, operators of critical infrastructure are required to notify the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik; BSI) of any IT security breach. After evaluation by the BSI, these notifications are processed and made available to all operators.

The IT Security Act focuses on seven branches and about 700 facilities (see Borchers 2016) including but not limited to: information technology and telecommunications, as well as the energy sector, the food industry, the financial and insurance sector, as well as the sectors regarding health and water. These branches are now obligated to orientate themselves to minimal standards for IT security and to notify the BSI of any incidents. The decision as to which attachments

fall under the obligation of notification lies with the Federal Government and is based on the "500,000 rule" which claims that as soon as there is a benefit for at least 500,000 people, the corresponding attachment falls under the notification obligation. The actual usage is converted into a threshold value for easy handling.

Most attachments regarding IT security with a notification obligation are found in the energy sector. There are a total of 320 attachments and companies in this sector which reach the following threshold values:

- Electricity generation (or storage): 450 MW per year
- Gas supply: 5,190 GW per year
- Refinery: 620,000 t of fuel oil per year
- Gas station network: 335,000 stations

The **water sector** (including drinking water and sewage drain) comes in second place with 230 attachments. In this sector, sewage treatment plants (that supply about 500,000 people) and water supply companies which are responsible for allocation, processing and distribution of 21.9 million cubic meters of water per year, do have a notification requirement.

Regarding the **food industry** there are currently 70 attachments that are obligated to give notification, namely those that produce, store or distribute 334,000 t of foods a year. Regarding liquids there is a threshold value of 274.5 million beverages.

The **information technology sector**, with its data centers, trust centers and server farms, constitutes the smallest sector that is affected by the notification obligation of the IT Security Act. The 500,000 rule only applies to the trust centers in this sector and refers to the number of registered person-based certificates. In addition to this, every trust center that gives out more than 10,000 TLS certificates becomes obliged to give notification. Regarding the data centers, the notification obligation refers to all installations that have a yearly average of 5 MW. In case of content suppliers, the new rule applies to those that deliver more than 75,000 terabytes a year. Server farms are obligated to notification after an average of 25,000 instances running.

For operators of **telecommunications** that deal with communication and data networks, the notification obligations are already established in the telecommunications law, so that there are only few additions implemented by the IT Security Act. The established threshold value for networks and transmission services lies at 100,000 participants or rather 75,000 terabytes per year. For DNS servers the value lies at 2.5 million IP queries-a-day or accordingly at 250,000 domains, for which the server is responsible. It is currently determined, how many attachments are subject to the reporting requirement.

A threshold value regarding the **health, finance and insurance sectors** is foreseen for the end of 2016. Debates are currently being held.

5.1.3 Regulation on Determining Critical Infrastructure

A legal regulation determines who has to give notification in IT security matters (see Bundesministerium des Inneren 2016). The operators of critical infrastructures

can review whether the IT Security Act is applicable with the help of quantifiable and comprehensible criteria for their own company. If that in fact is the case, the operator has to make a contact available for the BSI within six months. Furthermore, the operator has to provide proof that the minimal standards of IT security are being followed within two years. Up to now the regulation refers to the critical infrastructures in the sectors of water, food, energy, information technology and telecommunications. A regulation change foreseen for 2017 includes the sectors of transportation and traffic, as well as health, finance and insurance.

5.1.4 Controversial: Changes Affecting Telemedia Services

An easy-to-overlook requirement of the IT Security Act affecting nearly every business is the amendment to the Telemedia Act implemented in article 4. The key here is section 13 (7) of the Telemedia Act: To the extent technically and economically feasible, service providers must take technical and organizational measures to ensure that no unauthorized access is possible to the technical facilities they use for the telemedia services they offer. In addition, these facilities must be protected against disruptions and unauthorized access to personal information, as well as attacks from outside. The precautions taken, such as data encryption, must be state of the art.

This provision is particularly relevant to companies because in the sense of section 2 of the Telemedia Act a "service provider" is any individual or legal entity offering or providing access to its own or third-party telemedia. In the case of audiovisual media services on demand, a "service provider" is any individual or legal entity effectively controlling the selection and configuration of the content offered. Ultimately, any company that operates its own website for business purposes falls under the security requirements laid down in the IT Security Act. Businesses must therefore immediately begin intense investigations on how to prevent unauthorized access.

5.2 International Issues: The European Union's Directive on Security of Network and Information Systems (NIS Directive)

According to the proposal by the European Parliament and the Council for a Directive on the Security of Network and Information Systems (NIS Directive), operators of network and information systems are expected to do more to ensure network and information security. Because security of information and network systems is of utmost importance for the home markets and is necessary for their smooth proceeding. System malfunctions therefore have to be prevented at all times. In order to achieve this, uniform EU guidelines for the water supply, health, energy, transportation and traffic, internet and finance sector will be enacted. Germany already complies with the planned regulations thanks to the IT Security Act.

The EU member states are required to establish a central base for NIS-notifications so they can inform each other easily and to provide the European Union Agency for network and Information Security (ENISA) with updates for eventual incidents: "The international NIS-notification centers that get the information through these channels are to pass this information on to the companies in their jurisdiction. Reactions to NIS-threats are coordinated by the NIS-authority and the ENISA Europe-wide" (Lepper 2014).

The recommended guideline would provide a minimal security level regarding digital technique, networking and services for all member states alike. These requirements as well as standardized measures in risk management and clear regulations regarding notification will lead to a more stable and trustworthy IT system in the respective sectors.

5.3 Data Protection and Data Security in the United States

There are no comprehensive federal laws governing data protection and data security in the United States. US law governing the collection, use, distribution, and protection of personal information is based on overlapping, and in some cases contradictory, regulations at federal and individual state level. At the federal level, a sector-based approach is taken with data protection guidelines and regulations focusing on industrial sectors such as healthcare and the financial industry. Government agencies such as the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the Securities and Exchange Commission (SEC) issue additional rules and regulations that affect the collection, use, and storage of personal information. Finally, US states such as California exercise their right to impose additional requirements – for instance, the obligation to report incidents where the personal data of citizens is threatened.

The amount of questions each individual incident can bring up in the US can be demonstrated by the example of the conflict between the FBI and Apple regarding the data de-codification of a smartphone owned by a potential terrorist (see Martin-Jung 2016). The FBI unlocked the smartphone without the help of Apple, against the court's decision. The reason was simple, that no help was needed from the manufacturer, Apple. Even though the de-codification of the iPhone ended the disagreement between Apple and the FBI, the question remains, if technology companies and other organizations should be obligated to integrate the possibility that in case of investigation, the codified data should be made available to the authorities.

5.4 Data Exchange Between EU and US Companies

The answer to the question of how personal data can be exchanged legally between companies in the EU and the United States is complicated. But one thing is certain: Transferring data without considering the European legal framework unavoidably

raises the issue of liability for the company transferring the data as well as the responsible individuals within the company, particularly management.

5.4.1 Safe Harbor

In 2000, the European Commission established a safe harbor arrangement for the purpose of creating legal certainty. It was supposed to facilitate the transfer of personalized data from the EU to the US – and in compliance with the European Data protection regulations.

However, the safe harbor decision was declared invalid by the European Court of Justice on October 6, 2015. Since then, there has been considerable legal uncertainty about whether and on what basis such data can be transferred.

5.4.2 Privacy Shield

The solution for the legal uncertainty is now based on the so-called Privacy Shield, a covenant between the United States and the European Union for the regulation of transatlantic data transfer. Since its announcement on February 2, 2016 the Privacy Shield was fiercely criticized. It was especially complained about the US governments right to collect information on a large scale for purposes of national security. In this form, the agreement would not be upheld by the European Court of Justice (see Beiersmann 2016). According to the European data protection officer, who advises EU institutions, the Privacy Shield must fulfill the requirements of the new EU Data Protection Directive, whose entry into force across the EU is anticipated in May 2018. This directive also applies to the transfer of data to the United States.

Irrespectively of all opposition the EU-Commission established that the new framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers (see Europäische Kommission 2016).

Independently of this development numerous cloud providers, such as T-Systems partners Salesforce and SugarCRM, have moved to regional data centers to be on the safe side.

5.5 Conclusion: Many Legal Issues to Consider

IT security is complex in more than just a technical sense. The legal framework underlying it is laced with widely diverse laws, guidelines, rules, and technical standards. Business leaders face a huge challenge if they wish to comply with all of the relevant requirements and limit the risk of personal liability.

The law can shed light on various risk scenarios to which IT providers and users, and network and platform operators are subject. The IT Security Act does not make the general rules on liability obsolete. In fact, they have been enhanced for certain industries.

In the European Union, the harmonization of regulations is proceeding – and the Directive on the Security of Network and Information Systems is pointing in the right direction. Germany is ahead of others in this matter because passing the IT Security Act already implemented large pieces of the directive.

Ensuring security in data exchanges with the United States is a challenge for companies: Legal certainty in the transfer of personal data is currently somewhat questionable due to the rejection of the safe harbor concept despite the implementation of the Privacy Shield. But caution should be exercised because the legal framework in the United States is heterogeneous, and the legal situation in the European Union is fluid. It may be awaited eagerly what judgements the courts will render in the future, especially Court of Justice of the European Union (CJEU).

There is no getting around the fact that companies and their management must clearly see to every aspect of IT security. It cannot simply be seen as a cost factor. In truth, IT security is complex. IT security is expensive, risky and mission critical. IT security must therefore be a top-level management issue. What else could it be?

References

Beiersmann, S. (2016). *Auch EU-Datenschutzbeauftragter lehnt Privacy Shield ab*. Accessed August 16, 2016, from http://www.zdnet.de/88270732/auch-eu-datenschutzbeauftragter-lehnt-privacy-shield-ab/

Borchers, D. (2016). *IT-Sicherheitsgesetz: Wer was wann zu melden hat*. Accessed August 16, 2016, from http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Wer-was-wann-zu-melden-hat-3096885.html

BSI (2007). *IT-Sicherheit und Recht*. Accessed June 6, 2016, from https://www.bsi.bund.de/DE/Publikationen/Studien/ITSicherheitUndRecht/index_htm.html

Bundesministerium des Inneren (2016). *Kabinett beschließt erste Verordnung zur Umsetzung des IT-Sicherheitsgesetzes*. Accessed August 16, 2016, from http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2016/04/kabinett-kritis-vo.html

Europäische Kommission (2016). *Europäische Kommission lanciert EU-US-Datenschutzschild: besserer Schutz für den transatlantischen Datenverkehr*. Accessed August 19, 2016, from http://europa.eu/rapid/press-release_IP-16-2461_de.htm

Lepper, K. (2014, August). *Bericht aus Brüssel*. Accessed August 16, 2016, from http://www.bdsv.eu/data/8aae7b7bc3cebbc67ea7aecfbed47bceb9a494cdb9dca0cdc7b798bac7b778d8c3b7b3b88aae957cc2b9d1847dddd093.pdf. In: Newsletter des Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. Edition 03.

Martin-Jung, H. (2016). *Datenschutz – Apple trotzt dem FBI*. Accessed August 16, 2016, from http://www.sueddeutsche.de/politik/datenschutz-apple-trotzt-dem-fbi-1.2925671

Regierungskommission (2015). *Deutscher Corporate Governance Kodex*. Item 4.1.3. Accessed June 22, 2016, from http://www.dcgk.de/de/kommission/die-kommission-im-dialog/deteilansicht/kodexaenderungen-2015-beschlossen.html

Klaus Brisch LL.M. (USA), is a partner at DWF Germany Rechtsanwaltsgesellschaft mbH, where he specializes in information technology law. A consultant to national and international companies in the information technology and telecommunications sectors on industry-specific issues relating to commercial law, he also advises end-user companies on the interpretation of IT law. His work focuses in particular on data protection, data security, IT security and cybersecurity in both a national and international context.

Brisch also specializes in providing support for industry-specific acquisitions of companies and shareholdings, as well as the design and management of complex projects in the field of national and international IT and telecommunications, an area that also includes the outsourcing of IT service provision. Other activities include consulting work in the field of IT compliance and e-commerce law.

IT Security: Stronger Together

6

Ralf Schneider

Modern CIOs handle a multitude of roles within their companies, from deciding the strategic orientation of the IT environment to keeping data centers and devices running smoothly. As if this wasn't enough in terms of responsibility, CIOs also bear ultimate responsibility for the security of data, applications and the IT infrastructure. Although ensuring the safety of the company's digital assets has long been one of the core elements of a security strategy, new adversaries such as government-backed hacker groups, cyberespionage teams out for a quick profit and politically motivated activists have resulted in a "red alert" status for digital assets. And yet, while the current threat from these numerous attack vectors should be taken deadly seriously, many companies still believe that antivirus software, a firewall or simply taking a hush-hush approach are adequate precautionary measures. Antivirus software and firewalls are of course essential, even though both systems only form building blocks of an overall security model. But the time has really come to drop the idea of seeing security as a taboo topic not to be discussed in public. "Security by obfuscation" used to be considered a legitimate security strategy: If we don't publish any information on a topic, then we're not giving away any useful data – right? Wrong! Pretty much every proprietary software or hardware has now been hacked, simply because attackers found a loophole that manufacturers had overlooked. Which is why open source software is considered more secure: The multitude of auditors and developers picking through the code maximizes the number of vulnerabilities detected and the speed of their discovery. Going at it alone, hidden away behind closed doors, is not how IT security works. Attackers recognized this a long time ago, of course. Since hacking is a collaborative, team-based effort, why shouldn't the good guys do the same?

R. Schneider (✉)
Allianz SE, Königinstr. 28, 80802 Munich, Germany
e-mail: ralf.schneider@allianz.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_6

6.1 The Trinity of IT Security

CIOs must accept the current situation: Observations made by the security company FireEye show that some 95 percent of companies have been victims of cyberattacks for many years without being aware of it. In Germany, the number of attacks against companies and government agencies observed in the second half of 2015 was almost double that of the previous six months. One noticeable trend is the phenomenal rise in attacks made via ransomware across the entire EMEA region (see FireEye 2016a). The threat situation is prodigious. In addition to attacks made at network perimeters, there is the fact that every employee has a couple of tools in daily use capable of routing attacks directly into the heart of the network: the email client and the web browser. If an employee mistakenly clicks on a phishing link, he or she opens Pandora's Box – bypassing firewalls, intrusion detection systems and other perimeter barriers. The same applies to the browser. Drive-by infections by legitimate websites nonetheless polluted with malware dump the poisonous handiwork of clever but criminal hackers directly onto the PC and company LAN. There are no quick remedies to such problems. We live and work in an information society that is becoming increasingly internetworked. Employees without email and with highly-restricted Internet access (or none at all) are unproductive employees. Highly restrictive approaches can really only be deployed in extremely sensitive areas – most office jobs will require a broad range of communication options with the outside world. Nor should one forget that the holy trinitiy of IT security is expressed via the "CIA" principle: Confidentiality, Integrity and Availability should each be given the same level of attention. Plugging every hole also seals off the availability pipeline.

Some protection is of course needed. While it's true that a successful attack doesn't always merit a front-page headline – even if the victims are household names – the consequences of a cyberattack can still be catastrophic. The TalkTalk hack in fall 2015 caused revenue losses of around 60 million pounds and resulted in the UK cellular network provider losing over 115,000 customers (see Wired 2016). And around 61 percent of German consumers would take legal action if their personal data was exposed in a hack (see FireEye 2016b). So it's important to find the right balance between policing and productivity.

But how can one protect a 280,000-node network like the one operated by the Allianz Group? The right hardware and software is of course important, but so is an appropriate model that takes a nuanced approach to threats while conceding that a company has a better chance of mounting a successful defense as part of a team rather than doing it alone. The lion's share of hacks now run as automated processes without a specific target, a simple case of poking around in the dark long enough to find someone who has failed to apply a patch or overlooked a PC backdoor. Once the backdoor is found, there's a good chance that more than one company is affected by it. Often, however, this same vulnerability has already been identified and resolved by another organization. If companies shared this kind of information, everyone would benefit. While this would not offer a remedy against targeted attacks, it would be an effective suppressor of the aggressive "background noise"

of digital hackers. Accordingly, the news that cooperative initiatives are now springing up in the traditionally rather close-mouthed sector of IT security is to be welcomed. As just one example, over two dozen companies and organizations have now signed the "Coordinated Vulnerability Disclosure Manifesto." The manifesto declares support for collaboration between companies and the cybersecurity community to find and resolve vulnerabilities in information and communication technology. This kind of cooperation requires a high level of trust between stakeholders. Simply for practicably reasons, only a more exclusive club can be considered for very large firms, whose assets at stake – both in a financial sense and in terms of the company's reputation – are immensely valuable. The role of the partner network for Allianz is played by the German "Cyber Security Sharing and Analytics" (CSSA) association. Within the CSSA, 12 large businesses now work not as partners in crime but partners against cybercrime.

6.2 CSSA – Security Through Collaboration

The founding concept of the CSSA is the peer-based sharing of information about cybersecurity between organizations. Major corporations have other requirements than SMEs, especially in terms of the operating models they use for IT security. The CSSA currently counts 12 heavyweights of German business among its members, including Allianz, BASF, Bosch, Deutsche Bank, Deutsche Börse Group, SAP, Siemens and Deutsche Telekom. United by their strong interest in IT security, they have also recognized that the cooperative approach today is the better option. A non-profit organization, the CSSA develops models that enable the rapid and highly-scalable sharing of information about cyberattacks without compromising the confidentiality of the business transactions involved. The CSSA refers to itself – only half-jokingly – as a kind of "neighborhood watch," warning each other against the digital equivalent of leaving the front door unlocked.

The initiative arose as the logical next move following a meeting of several CIOs. In their meeting, the CIOs not only discovered that they were plagued by similar problems but that each of them also had access to information that could be useful to their counterparts. Companies had previously been prevented from sharing this data due to the lack of a secure and efficient framework. Accordingly, the CSSA was formed in November 2014 as a registered German association with seven founding members, one of whom being Allianz. Membership of the CSSA was and continues to be assessed on the value or information that a new applicant can bring to the group. Participating organizations must contribute both expertise and knowledge and already have a stable security system in place featuring key basic components such as a CERT – and ideally a SIEM, etc. The sharing of information about threats and vulnerabilities would be pointless if a company lacked the tools for implementing protective and counter-measures.

While the CSSA does prioritize the importance of a small, effective group, it is not a static club. New members are welcome if they can meet the acceptance criteria. This includes considering Europe to be the main focus of their business.

6.2.1 Targeted Interaction

"Actions speak louder than words" is the CSSA's unofficial slogan. With it, the CSSA's 12 member companies have mutually agreed their commitment to being active members of the association, i.e., to providing a budget and experts to ensure that the volume of available data can actually be turned into tangible results. All of this is made possible by a manageable number of participating organizations, clearly-defined contacts, and dedicated resources both in the CSSA and member companies.

CSSA members see their most important activity as being the sharing and analysis of actual incidents, threats and vulnerabilities with the aim of improving protection against potential attacks. Weekly conference calls at a technical level plus regular meetings ensure a constant flow of information. By sharing threat intelligence, a joint database is being established. Lessons learned and threat indicators from actual attacks are collected as Indicators of Compromise (IoCs) together with strategic information, while analyses of recently-discovered malware are distributed as Malware Reports. Member companies can import this information into their own systems, thereby enabling them to block potential threats or check infections. At some companies, this process is almost fully automated, while others are still working on integrating the CSSA platform into their security infrastructure.

Since the members are active across a spectrum of industries, the CSSA is generating a large dataset that covers a huge range of threat vectors. This enables information to be isolated from its industry-specific context and to be used to create connections that would be beyond the capabilities of a single company.

Nor does this merely sound good on paper – the reality proves that it's also bearing fruit in the real world. Details from companies about attacks happening on their own turf have been already shared at a strictly technical level with other CSSA members, who were then able to prepare and adapt their defense systems accordingly. A number of those participating had never experienced this level of transparency – some not even within their own company.

The sharing of warnings also plays an important role in the CSSA. A good example of this is last year's wave of "DDoS for Bitcoins" blackmail attacks. One CSSA member was affected early on and warned the other organizations almost a week before the BSI issued a corresponding advisory. So CSSA members were well prepared and able to fend off actual attacks they then experienced.

6.2.2 Network of Trust

Trust is the most important basis for the collaboration within the CSSA: trust that information about individual members is not misused, and that information about a discovered vulnerability or even a wave of attack is passed quickly to the other members. The very founding of the association already involved the definition of policies and processes to ensure the optimum sharing of data among members, with only specific contacts requiring access and nobody else. All individuals involved with

the work of the CSSA must sign personal confidentiality statements. The statement includes a version of the Traffic Light Protocol (TLP) adapted for the CSSA. Different levels of confidentiality are shown using the colors green, yellow and red. For publicly-available information, "TLP White" has been introduced. Only green material may be forwarded unencrypted. From the yellow level onwards – which is the default classification within the CSSA – encryption is mandatory. Material at the red level may be shared only within the information's original context. The material is "X eyes only," i.e., only for a specific set of "X" individuals.

Thanks to the small-scale setup of the CSSA, confidentiality breaches are unlikely and have indeed not yet occurred. Furthermore, since the association is based on trust, a breach of this kind would also be treated very seriously. Secure exchange is also naturally essential for the collaboration. In addition to defining a set of general-purpose security rules, the association also deploys specific tools with which information can be distributed securely across multiple media and formats (encrypted email, Secure Data Room, Secure Chat, etc.).

For the future, the CSSA is clearly working towards becoming a competence center and expert panel for its members. Through the network of trust formed between participating organizations and individuals, a database packed with highly relevant and up-to-date information is being established. Here, the trust model is decisive, which is primarily based on personal relationships and designated contacts having direct responsibility. Sharing the database or parts of it with other organizations might be an option for the future, although this is seen only a potential scenario at present. Governmental institutions are currently not granted access as well.

6.3 The Six Elements of an Integrated Defense Strategy

Even when helpful partners are at hand, the primary burden of IT security is borne by a well-configured security system that is correctly dimensioned and monitored on a continuous basis. Past experience has shown that a multi-layered architecture offers the best level of protection and is also the simplest to manage – even for very large networks. In the ideal situation, attacks are intercepted before they even reach the network perimeter. If an attack does slip through, then it is blocked by the subsequent layers. The approach resembles an onion with its several consecutive layers and is capable of handling both a range of attack vectors and heterogeneous corporate structures. At Allianz, a six-level system is deployed that has proven its worth in practice and is undergoing continuous expansion. Virtually every level has been deliberately designed to benefit from information shared between peers and, in turn, to enable the forwarding of information to these partners. Of course, this doesn't automatically work from the outset – this is not an "off-the-shelf" solution. By redesigning its IT processes, however, Allianz was able to streamline many of its processes, adapting them to better suit the needs of its business departments and ultimately its end users.

6.3.1 Prevention Is Better Than the Cure

But how can an attack be blocked before it even happens? Doing so requires neither a crystal ball nor superhuman powers. As the **first layer of protection**, prevention is a crucial strategy, not least because errors that are avoided before hardware or software is even deployed cannot become security holes. Vulnerabilities avoided by prevention can also be beneficial to partners in the information network because the chance that they have also failed to discover the same vulnerabilities is high, given the standard configurations typically applied to devices in company use. From operating systems to applications, no code is error-free. This fact is powerfully illustrated by the monthly "Patch Tuesdays" carried out by Microsoft – although Microsoft is only one prominent example of many, as the problem affects any software development company. In 2015, the US National Vulnerability Database (see National Vulnerability Database 2016) listed 8,822 vulnerabilities – almost 2,000 more than in the previous year. In pole position with 314 entries was Adobe's Flash Player, followed by Microsoft Internet Explorer (231), Firefox (178) and Java Runtime (80).

Another problem is self-inflicted vulnerabilities caused by configuration errors. One recent survey from security company F-Secure (see F-Secure 2016) discovered thousands of cases of incorrectly configured systems and outdated software in use at companies. Indeed, some of the most common vulnerabilities in corporate systems had been caused by misconfiguration issues. In recent months, SSL in particular has proven to be something of a Pandora's Box: Errors made in implementation coupled with careless administration had thrown company gates wide open to attackers, and the confidentiality of SSL-encrypted connections had been compromised. Yet these vulnerabilities were easily avoidable, which would have drastically reduced organizational exposure to attacks.

Surveillance guards against the kind of errors described above. You cannot take the right precautions until you're aware of what needs protecting in your network. Network management/analysis and documentation are key factors that decide whether an IT unit has its network under control or is constantly put on the back foot by a never-ending stream of new problems. And end users are not making life any easier for CIOs and administrators. The words "shadow IT" have now become a feared moniker describing IT systems set up outside official channels. Wi-Fi access points from the local electrical goods store used to be the classic example of shadow IT. Employees frustrated by the speed of the company Wi-Fi network simply took the rough-and-ready approach of installing their own access point in the office – naturally without taking any of the necessary security precautions and without informing the IT department. What was then a minor headache for IT and not without its risks – if an open Wi-Fi network was also accessible outside the building – has now escalated into something else entirely. Cloud services are very popular with employees and even entire departments, and are sometimes used as a DIY solution without official approval.

A survey conducted by the Cloud Security Alliance (CSA) showed that IT management staff receive ten applications for cloud service usage every month

on average (see Cloud Security Alliance 2016). The only problem is, they also need about 18 days to process and evaluate an application. This mismatch in time frames can provide dangerously fertile ground for shadow IT, warns cloud security provider Skyhigh Networks. A recent analysis of actual cloud usage in European businesses reveals that a large proportion of the some 1,000 cloud services used on average per company takes place without the knowledge of the IT department (see Skyhigh 2016). If the IT department doesn't know what's being used, it can't protect it – and finding an unauthorized cloud service is more complex than tracking down a rogue access point. This is why proper surveillance of the network and a clear idea of the protocols, services and applications that should run in a specific segment is so important in order to detect changes.

Patching is another aspect of prevention. While it should be self-evident that resolving problems in products with updates, patches and fixes is a good idea, practice tells a very different story. Sometimes, the reasons for this are sound: Not every patch is safe to apply – all too often, updates are well-meant but poorly executed. Even if only one percent of the 280,000 user devices connected to the kind of networks that Allianz runs are taken offline by incompatibilities with other programs, losses in terms of productivity and (indirectly) revenue are nonetheless dramatic. Despite this, patch management is here to stay, and there are now numerous strategies designed to ensure that rollouts proceed smoothly (even in large networks) and side-effects are contained.

6.3.2 Knowledge Is Power

As has already been shown by the very real danger of shadow IT, prevention is only one side of the coin – the status quo must also be reviewed in addition to the desired status. Logically, the **second layer of IT protection** encompasses everything already underway in the company. Surveillance, monitoring, early warning – plenty of security models are available. Above all, however, the collection of data must be automated as far as possible. The 280,000 network nodes at Allianz generate an inordinate amount of data every second. Only an intelligent and largely autonomous filtering system is capable of evaluating the data by relevance and urgency, and correlating it to events. A single failed login to a resource does not by itself indicate the network is under attack. But if the same user also fails to access five other resources in a short space of time, a response is required.

Ideally, a Security Information and Event Management (SIEM) system acts as a high-level information clearinghouse, fed by log files, warnings issued by security software such as IDS/IDP and antivirus systems, as well as the valuable data provided by CSSA members. Normally, a SIEM system merely collects data and prepares it for display. In especially large networks, however, it is also possible to let the SIEM setup or underlying security systems react autonomously. Returning to the above example of the multiple failed logins, the account of the user in question could be locked out or, if a subsequent login succeeded, the user might then be granted only limited rights. While this is technically possible, the consequences at a

personal level are rarely thought through in many companies. Should this arrangement also apply to CxO-level accounts? Have staff been properly informed about the people they need to contact to restore login permissions? And is this unit available 24/7 – in the event of an employee being accidentally locked out while working in a different time zone? While a lot can be handled by a SIEM setup and its associated infrastructure, it is often advisable to have a SIEM focus primarily on collection, evaluation and correlation, and leave the job of active system defense to human IT resources.

6.3.3 IT Security Is Not an End in Itself

This brings us to **layer number three** and the employees for whom IT security has been established in the first place. Administrators – and especially those entrusted with security tasks – should not forget that the daily work of the company's employees must be the focus of any security efforts. IT security is not an end in itself but serves to facilitate the productive output of products or services. Accordingly, an IT security strategy must provide answers not only to the issues of securing the working equipment but also to questions about guaranteeing the productivity of members of staff. Although a PC without network access, USB ports or a CD drive is practically impregnable, it's not particularly useful for day-to-day work. While the topic of staff awareness was hyped to breaking-point a few years ago, things have calmed down again since then. Many of the "awareness training" firms that sprang up overnight have vanished again just as quickly. But this doesn't mean that staff are now security-savvy. Quite the opposite, in fact: As network perimeters become increasingly hardened, attackers are becoming increasingly dependent on insider help from within the network. And their chances of success aren't too bad, either. Verizon's Data Breach Investigations Report shows that the number of users opening a phishing email in 2016 has actually risen from 23 percent last year to 30 percent in the current year. A full 12 percent then proceed to click the dangerous link itself – so a certain amount of work still appears to be necessary on the subject of security awareness in the years to come (see Verizon 2016).

Of course, company staff are not solely to blame here. Employees are coming under increasing pressure, as larger workloads are shared among dwindling workforces, and – crucially – proficiency is required in an ever-increasing number of technical and organizational tools. The topic of "password security" alone is met with eye-rolling from users and exasperated groans from administrators. Passwords should be secure, complex and dynamic. And a new password should be set every three months. And a separate password should be used for important services. But it's hardly surprising that employees often sabotage this strategy. The much-loved Post-It under the keyboard, stuck to the monitor or kept handy in a desk drawer bears mute witness to the difference between well intentioned and well implemented. Forcing employees to follow security rules doesn't achieve anything – except less security. Password security problems could have been defused a long time ago by

two-factor authentication, for example. As more and more services and operating systems such as Windows 10 support multifactor authentication, this perennial nuisance could perhaps be passé very soon. Interacting with one's staff on awareness and other matters is a highly individual business as every company and department will need to identify and follow their own strategy here. That said, the experience of other partners in similar situations, as gained by CSSA members on a daily basis, can provide help in the form of best practices.

6.3.4 It's Only a Matter of Time: Incident Management

Only a rookie would believe it's possible to stay ahead of the dangers of the digital world. Anyone actually meriting the title of CIO understands that a successful attack will inevitably take place. So the sensible approach is to set up the **fourth layer of the security model** and prepare for this eventuality before it is too late. The time for lengthy discussions is not when the alarms already start to sound. Moreover, the natural response to an attack in progress tends to be panic, nervousness and quite possibly ill-considered responses. Just as it is helpful to regularly rehearse emergency procedures, a detailed code of conduct also helps defuse an ongoing crisis. Knowing the game plan means steps can be taken more quickly. Sometimes it's easier said than done, however. When corporate security is at stake, decisions can have far-reaching consequences. As one example, if a data leak is stopped by effectively cutting network access for more or less the entire organization, this can affect the company's bottom line at the end of the year. If the success of the data hack is unknown, then a sensible precaution might be for everyone to change their passwords. While no one enjoys making such a decision, it needs to be clear that the decision can be made if the risk is serious enough and that the decision-maker also has the backing of company management to do so. Incident Management is also frequently associated with forensic analysis, when the aim is to discover the attack vector and close it against future attacks. Generally, this involves external service providers who then gain access to critical company systems. For a company whose membership in the CSSA means that it is used to confidentiality and the highly selective sharing of information, a fact-finding mission of this kind should only present a low risk of the undesirable disclosure of company internals.

A successful attack on a fellow member is naturally no reason to celebrate for the partners within the CSSA. The organizations can nonetheless benefit from the attack and its attendant circumstances by closing the very same attack vectors within their own networks. Those aware of events in partner companies are better prepared, can take precautions and may even be able to help by providing resources. While it is clear that market forces require two companies to follow their separate objectives, preventing them from simply sharing everything, the clear-cut categorization of the CSSA's Traffic Light Protocol unambiguously clarifies which data can be shared with whom. As a result, the necessary data – and only this data – is provided to take appropriate action.

6.3.5 Fitness Training: Prepare for Emergencies

"Attack is the best form of defense" is a claim made since the Middle Ages. IT security also applies this principle as **another layer of security** – although it does not mean that we attempt to infect hackers with their own malware. At times when there are no acute situations that require an immediate response, the company's own defenses can be put through their paces by simulated attacks. Penetration testing, awareness campaigns using fake phishing mails and social media attacks performed by security service providers are just some of the many strategies with which real-world emergencies can be rehearsed and prepared for. Closer collaboration with the company's ISP can also be a productive strategy against Distributed Denial of Service (DDoS) attacks. Rapid-response defense measures against ongoing attacks require seamless communication, clear-cut competencies and detailed knowledge of the company assets needing protection. Those with the necessary know-how and resources can also try hanging out with the hackers themselves. Many of the underground forums frequented by professional hackers are well-known. Alongside antivirus software makers and other security companies, IT departments of large organizations are often to be found lurking here in the hope of getting tip-offs about forthcoming attacks and the latest malware trends.

6.3.6 Stronger Together

This brings us to the **sixth layer** in our security stronghold. Depending on your viewpoint, this is either the easiest or most difficult level to implement. It involves collaborating with others, implementing insights from one's fellow victims and, naturally, sharing the company's own data. If, like the CSSA members, you have included your partners in the information network for the five security strategies outlined above, then you can draw on a solid, shared repository of data. This helps day-to-day operations with a large volume of data that is fed directly into the SIEM, simplifies trend monitoring thanks to the size of the dataset and spreads the workload across multiple virtual shoulders.

6.4 Conclusion

For a single company, replicating the CSSA's achievements for its members in the months since its formation might be feasible but would certainly be harder. Many companies will (hopefully) rethink their approach in the near future. While discussing IT security was once considered bad form – one might let something slip – the regularity of successful hacks has shown that we all have weaknesses, some of which are already being exploited by attackers. Those who refuse to see IT security as a task that demands integration – as a combination of products, strategies, processes and (above all) partners – are ultimately doomed to fail. But

in a world where digital information is used to control trade flows, money transfers, opinion and soon the very cars that drive us, failure is not an option.

References

Cloud Security Alliance (2016). *Website*. Accessed May 24, 2016, from https://cloudsecurityalliance.org

FireEye (2016a). FireEye-Studie: *Doppelt so viele Cyberattacken in Deutschland – starker Anstieg bei Ransomware*. Accessed May 24, 2016, from https://www.fireeye.de/company/press-releases/2016/fireeye-report-finds-almost-twice-as-many-cyberattacks-in-germany.html

FireEye (2016b). *FireEye-Studie zeigt: 61 Prozent der Deutschen würden rechtliche Schritte ergreifen, wenn ihre persönlichen Daten gehackt warden*. Accessed May 24, 2016, from https://www.fireeye.de/company/press-releases/2016/fireeye-consumer-survey.html

F-Secure (2016). *Schwachstellen zu schließen ist eine der wichtigsten Maßnahmen, um Attacken erfolgreich abzuwehren*. Accessed May 24, 2016, from http://www.pressebox.de/inaktiv/f-secure-gmbh/Schwachstellen-zu-schliessen-ist-eine-der-wichtigsten-Massnahmen-um-Attacken-erfolgreich-abzuwehren/boxid/796096

National Vulnerability Database (2016). *CVE and CCE statistics query page*. Accessed May 24, 2016, from https://web.nvd.nist.gov/view/vuln/statistics

Skyhigh (2016). *Cloud adoption and risk in EU Report Q1 2016*. Accessed May 24, 2016, from http://info.skyhighnetworks.com/WPCARRQ12016EU_Download_White.html

Verizon (2016). *Verizon DBIR 2016 shows we haven't learned how to improve security*. Accessed May 24, 2016, from http://searchsecurity.techtarget.com/news/450294161/Verizon-DBIR-2016-shows-we-havent-learned-how-to-improve-security

Wired (2016). *TalkTalk Hack Toll: 100k Customers and £60m*. Accessed May 24, 2016, from http://www.wired.co.uk/news/archive/2016-02/02/talktalk-hack-customers-lost

Ralf Schneider has been Group CIO at Allianz SE since 2010. From 2010 to 2016, he was also responsible for IT as a member of the Management Board at Allianz Managed Operations and Services SE. Schneider was previously CIO at Allianz Deutschland for four years.

In the course of his 21-year career at Allianz, Schneider has worked in several senior IT roles and was always the youngest to hold these positions. His past responsibilities included heading the Information Systems Sales department as well as managing the unit for E-Business and Project Management Accounting Germany. Complementing his successful work at Allianz, Schneider also holds various offices in a number of cybersecurity organizations, such as Cyber Security Sharing and Analytics (CSSA), the German Cybersecurity Organization (DCSO) and the Digital Society Institute of ESMT Berlin.

Schneider studied mathematics and obtained a doctorate in informatics before beginning his professional career at Allianz in 1995.

The German Security Market: Searching for the Complete Peace-of-Mind Service

7

Markus a Campo, Henning Dransfeld, and Frank Heuer

7.1 Challenges for IT Security Managers

Data privacy has a very high priority in Germany. And yet data security is threatened by numerous factors – both internal and external. The typical external trigger for drives towards better security in corporations is an attempt – often successful – by third parties to gain access to IT systems or company data. In recent years, this type of threat has seen fundamental changes, since attacks have become increasingly professional. One reason for this is that advances in security technologies have resulted in a countertrend that has raised attack techniques to at least the same level of sophistication. In addition, state-backed agents and political activists have been joined by organized crime, which has discovered cybercriminality as a lucrative and low-risk source of profit.

Supplementing conventional threats is a new risk that is now spreading rapidly: the "hijacking" of things or machinery controlled by IT systems. Contemporary attacks are about much more than simply hacking IT to steal or disable data or systems. Rather, the term "security" now includes the concept of "safety" – in the sense of security against hazards to life and limb. In the age of the Internet of Things and the steady advance of automation, serious dangers are posed by the unauthorized control of networked industrial robots, control systems – and even cars. The relentless march of progress hugely increases pressure on those responsible for

M. a Campo
Försterstr. 25, 52072 Aachen, Germany
e-mail: markus.acampo@experton-group.com

H. Dransfeld
St. Ursulagasse 19, 61440 Oberursel, Germany
e-mail: henning.dransfeld@experton-group.com

F. Heuer (✉)
Experton Group AG, Königstor 23, 34117 Kassel, Germany
e-mail: frank.heuer@experton-group.com

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_7

security, not least because the theft or manipulation of data in the context of industrial espionage is now practiced on an increasingly larger scale.

A key internal driver for the new requirements faced by corporate IT security professionals is the transformation of the working world, championed by tech-savvy employees at all levels of the hierarchy, who require policy answers from IT units on topics such as Bring Your Own Device (BYOD) and social media. As a result, boundaries between personal and business use and between identities are now increasingly blurred, making the simultaneous fulfillment of existing corporate requirements for business on the one hand and data privacy legislation for employees on the other a growingly complex task for security managers. The intermingling of employees' business and personal lives already began a few years ago, and there are no indications that the trend is set to lose any momentum in the future.

Alongside internal and external threats, corporate IT security managers also see themselves confronted with additional external and internal factors that significantly influence the range of options available to them. These include legislative and regulatory requirements that mandate compliance with applicable security standards (ISO 27001, "IT Baseline Security" from the German Federal Office for Information Security (BSI), etc.) from service providers in sectors such as financial services, energy and telecommunications. Pressure on some segments of German industry is also set to increase still further due to the new IT Security Act (ITSIG). An estimated 2,000 companies will be affected. As operators of critical infrastructure (energy and water supplies, financial services, etc.), they are compelled to comply with a defined minimum standard, and – this is a crucial new requirement – to submit proof of this compliance to the BSI every two years. Once a company has been formally notified that it is now required to comply with ITSIG, it has two years to achieve this compliance.

As can be seen from the range of possible sanctions, this request is not to be taken lightly. In the event of non-fulfillment of the minimum requirements for IT security, the BSI can simply order appropriate measures to be taken. Operators of critical infrastructure are not the only ones affected by ITSIG requirements. The minimum standards specified by the law also apply to relationships with suppliers and service providers. As these are also indirectly affected by ITSIG, the need for security services will increase exponentially in the years to come.

In times where CIOs are increasingly reporting to their CFOs, one extremely significant internal (and limiting) factor is cost pressure within companies. As a consequence, digitization and standardization are now increasingly prevalent, and both business processes and infrastructure are being partially or completely outsourced. CIOs in large companies and corporations in particular are under a lot of pressure to justify their IT expenditure. A report published by the Experton Group discovered no change to the downward trend in dedicated security budgets that has lasted for some years now, finding that outlay for security is either included in the IT budget – itself now an embattled resource – or in the budgets of business departments. As a result, security – viewed as neither productive nor adding value by the business units – is directly competing with current business requirements.

7.2 Choosing the Right Protection in a Fragmented Market

The manifold issues raised by security requirements are matched by a wide choice of solutions and services. In the following sections, we introduce a number of key solutions and note the scenarios in which outsourcing services to a provider can be advantageous. Whether these benefits can actually be realized in practice must of course be assessed on a case-by-case basis.

7.2.1 Data Leakage/Loss Prevention (DLP)

The Experton Group uses the term DLP (Data Leakage Prevention, also Data Loss Prevention) to refer to solutions deployable by the user company for the identification and monitoring of sensitive data. The aim is to ensure that this kind of data is accessible only to authorized users and that no data leaks occur. One technique used here is to identify critical data as it is moving out of the company and to block it if necessary (preventing data loss). Other approaches monitor the infrastructure necessary to gain access to data in order to make the flow of data out of the company more difficult in the first place (preventing data leakage).

In cases where corporate data is stored in the cloud (e.g., Dropbox), there are benefits to be had by outsourcing DLP to a service provider. DLP service providers use specialized interfaces (APIs) to access a wide range of cloud implementations and can therefore offer customers considerable flexibility.

7.2.2 Security Information and Event Management (SIEM)

The Experton Group uses the term Security Information und Event Management (SIEM) to refer to analysis solutions that collect and evaluate security information and events. Some solutions make use of Big Data features to improve their ability to identify hazards for personal and other kinds of confidential data. The particular challenge with SIEM consists of standardizing data from a range of sources and in various formats, and then to analyze this data so that even complex attacks can be identified.

While on-premise solutions in the SIEM field primarily collect and analyze in-house data, SIEM service providers can also use attack patterns identified in data recently harvested from other customers in their analyses.

7.2.3 Email/Web/Collaboration Security

These security solutions offer protection from spam, viruses and malware associated with the use of the Internet and email/collaboration solutions, monitor data traffic. They also protect confidentiality, particularly by means of encryption.

Solutions that guard email against Internet-based attacks are still the "workhorses" of information security. One potential advantage in outsourcing security services in this specific area is the rapid propagation of information about new viruses or spam attacks. Within a provider network, this information is effectively distributed in real time.

7.2.4 Endpoint Security

The protection of user devices against malware is one of the first and oldest themes in IT security architecture. Endpoint Security is one of the key components of a successful defense strategy – both for the safety of the company in general and for cyber security in particular. After all, the first step is crucial for a successful attack on the infrastructure of a company: The attacker must get a foot in the door and set an anchor within the company's systems. Safety experts have, therefore, always been focused on avoiding such initial infections with, for example, Advanced Persistent Threats (APTs).

A key problem with endpoint security occurs in the event of attacks en masse, when the response time for the analysis and distribution of protective measures (e.g., patterns for virus scanners) is very short. Here, outsourced services can offer advantages as providers are able to use the entire customer base to collect data about suspicious files and activities, which can then be analyzed with the aid of Big Data methods to drastically shorten response times. This also applies to sandbox techniques, whereby suspicious files are first executed in a virtual environment (and often within a purpose-built appliance). Here too, centralized data collection by the provider shortens the response time for new attacks.

Another advantage of outsourcing endpoint security to the service provider is flexibility in the integration of new user devices, such as tablets or smartphones. While on-premise solutions often first require the purchase of new software packages that manage and protect these specific devices, service providers typically have most if not all popular user devices in their portfolio.

7.2.5 Identity and Access Management (IAM)

Identity and Access Management (IAM) is the term used by the Experton Group to refer to solutions and services (solution implementation and operation) for the input, logging and management of user identities and their associated access permissions. IAM solutions and services ensure that access permissions are granted in accordance with predefined policies.

The outsourcing of IAM to a service provider is especially advisable in cases where a company operates internationally and therefore needs access to corporate data from a variety of user devices and locations around the world. In this setup, user identification and authentication is handled by the provider, who grants access to the data once users have authenticated themselves successfully.

7.2.6 Mobile Security – Are Employees Really the Biggest Risk?

Employees are now increasingly mobile. Their need for secure access to sensitive data from any location (via tablet or smartphone) demands comprehensive protection for a growingly heterogeneous infrastructure and device landscape. Mobile security is an increasingly important topic. Modern smartphones are now as easy to infect with malware as a traditional PC. In many cases, they are also connected continuously to the Internet ("always-on"), which constitutes an additional security risk. Rapid progress in mobile apps is also generating a broader spectrum of threats. Mobile security is increasingly moving from protection of the user device alone to ensuring end-to-end protection for content, regardless of whether employees are accessing a company application on the go, from a secure office environment or from the much less secure structure of a public Wi-Fi network. In an age where company applications follow the "mobile first" design, integrated models are required to protect user devices, applications and company content from attacks. Here, IT departments are moving to shift company content to a container solution or a virtual application from the cloud. The last option reduces the danger of third-party interference or misuse, as the data is no longer even copied to the user device. The disadvantage of this kind of model is that mobile users have to be online to actually get any work done.

The question often arises as to whether employees themselves are the biggest threat when it comes to the misuse of company data. In the relevant literature, a phrase often heard in this context is that of the "disgruntled employee" – i.e., the members of staff with an ax to grind, who take entire filing cabinets full of corporate secrets home with them on their USB pen drives. How does this kind of mistrust gel with the era of mobility and the promise of "any time, any place, any task, any device" – with the simple freedom of choosing how and where one wants to work, depending on the task at hand? Isn't it the case that these flexible options are actually reducing the numbers of "disgruntled employees" – and thereby lessening the overall risk? Of course companies in the digital age need to protect the data of their business partners and customers in addition to their own. But there is an increasing number of technical measures that can prevent employees with a grudge (identified by the mobility system in use) or staff leaving the company from making off with company secrets. In fact, there are more such measures than ever before. Employers who have implemented a proper process to deal with members of staff leaving the company and their access to mobile user devices or information can eliminate this threat at the touch of a button.

Elsewhere, things are more difficult. Alongside the "disgruntled employee," we also have the "careless employee" – members of staff who take a lackadaisical approach to policy implementation in their company. As the following considerations show, the consequences of such carelessness can be very serious. Attacks from outside are successful only if those attacked are sufficiently vulnerable. Viruses and worms need to discover a vulnerability of this kind in software or hardware in order to deliver their payloads. Security holes need to be identified and

patched. Speed is of the essence here to avert the risk of damage. Two factors limit success in this context:

1. **The manufacturer must first identify and respond to the vulnerability**. This isn't always straightforward, as the example of Android and Stagefright has shown. Three months after it became known, a security hole was finally patched – only for a second vulnerability to appear three months later.
2. **Employees need to keep their work devices up-to-date**. Essentially, this only means that they need to have the latest firmware. Everything else can then be centrally deployed to devices with Mobile Device Management. But devices must be enabled and embedded in the system. In the real world, this requirement often implies a good deal of time and effort spent chasing up the last 10 percent of the "careless employees." CSOs and CIOs all agree that one of the most significant security holes is the one created by mobility.

Stopping employees taking information with them when they leave the company is a job that HR and IT must tackle together. Equally, identifying and motivating "careless employees," and encouraging them to upgrade their devices in time, are tasks for the management team. Even the best CIO in the world cannot master this challenge alone.

Due to the wide variety of mobile platforms and the various options for their secure administration, mobile security is a sound business model for a service provider. Everything we have said about endpoint security is especially pertinent in the mobile field. Service providers offer a single, standardized platform to manage and secure a huge variety of devices – a factor that hugely simplifies the work of in-house administrators in the context of Bring Your Own Device (BYOD).

7.2.7 Network Security

Contemporary corporate networks are exposed to a multitude of threats. Alongside unauthorized access to computers by external parties, attacks may also take the form of bringing the target company's servers to their knees (DoS, DDoS) or may simply involve dangers arising from the reckless behavior of the company's own staff. For "lucrative targets," hackers also invest a great deal of effort and an increasing amount of sophistication, penetrating deep into the network infrastructure and using these cyberattacks (Advanced Persistent Threats) to spy on sensitive data undetected for extended periods of time. Effectively countering these threats is a task for network security solutions. In the sense used in this section, "network security" refers to the securing of physical network structures, including wireless LANs.

Protecting against DoS or DDoS in particular is not something achievable by an individual company, since the network bandwidth available is generally insufficient to mount a defense. Accordingly, Internet providers frequently offer the option of providing this type of protection for their customers. Other network security

services are also good candidates for outsourcing: For example, firewalls or systems for intrusion detection and prevention can also be configured and supported by a provider. Outsourcing such traditionally internal security services will result in major changes to the nature of the associated admin positions. Staff who have perhaps spent decades running firewalls and configuring their policy files will now need to deal directly with a contractor and monitor the quality of the service provided. When outsourcing conventional network security, a very cautious approach is required if major conflicts are to be avoided.

7.2.8 Conclusion

To protect the company's valuable data, those responsible for IT security can draw on a comprehensive range of on-premise solutions and external services that address a broad spectrum of scenarios. While this situation has the advantage of offering tailor-made solutions for specific needs, the security market seems unnecessarily fragmented for the many security managers who simply need to secure their data and lack the time, know-how and budget to consider specialist solutions. The problem of finding the right package is aggravated by the fact that so many providers and products are essentially offering the same solution.

7.3 Security from a Single Source: Managed Security Services

On the one hand, decision-makers in mid-sized companies in particular are now facing security threats that present multifaceted, highly dynamic challenges. On the other, they have to cope with limited resources in terms of information, time and financing. Security specialists are also in short supply on the labor market. Accordingly, increasing numbers of security managers are now looking for providers who are able to offer a managed security service as a one-stop shop. As with the IT market in general, security is also gravitating towards outsourcing. For the client company, this brings a wide range of benefits, including a lower level of capital outlay coupled with reduced management effort – as a specialized provider (Managed Security Service Provider, MSSP) simply takes over both the operation and the monitoring of security solutions. The customer also benefits from the up-to-dateness of the service provider's expertise, which is hugely advantageous especially in terms of ever-changing cyberthreats. As a service provider that hosts and manages security services, an MSSP operates dedicated IT security infrastructure for one or more customers.

To lower costs, core security functions are often retained within the customer's own company, while day-to-day security business is either partially or fully outsourced as a managed service to an appropriate service provider. This has the advantage of keeping existing expert knowledge about security within the company and enabling more extensive control of security operations. Alongside conventional software licensing and bespoke managed services, standardized "as-a-Service"

offers are also becoming increasingly popular. This segment is likely to see disproportionately high growth in the future.

7.3.1 Managed Service or Cloud Solution?

When deciding to outsource security, one question that must always be answered concerns the "distance" permitted between outsourced services and the company's own infrastructure. With a managed service, for example, the equipment running the services usually continues to be based at the client, while the MSSP is responsible for installation, configuration and support. In a cloud solution, on the other hand, network traffic is routed via the provider, who renders the services using in-house systems before ultimately transferring the data back to the customer.

Decisions about the exact variant to choose are made as part of a sourcing strategy, which needs to consider a series of impact factors, including:

- Security and data protection;
- Service flexibility (on the part of the provider);
- Flexibility in handling customer requests;
- Effort required to manage the service (governance);
- Cost;
- Standardization;
- Effort needed to integrate the service into company infrastructure.

Regardless of the sourcing strategy, the two options also come with their respective fundamental advantages and disadvantages:

- Cloud services often offer a broader feature set than managed services. A sandboxing system, for example, which executes and analyzes suspicious files within a self-contained environment, may be offered for any possible operating system variant within the cloud. With a managed service, where the sandbox appliance sits in the client's network and is supported by the MSSP, a decision must generally be made for a single OS environment.
- Cloud services are also easier to integrate into Big Data analyses than managed services, since all of the customer data is already in the cloud and doesn't need to be collected first. This enables new kinds of attacks to be detected more quickly and communicated to the protective systems.
- With cloud services, unencrypted data is first sent to the provider – where it can in principle also be read.
- In addition, encrypted data cannot be analyzed in a cloud solution without first being unencrypted by the cloud provider.
- With a managed service, the risk of unauthorized eavesdropping on data is lower, since the data never leaves the client's own network.

Most of the security features described above are available as a managed service, a cloud solution or a hybrid version of the two. Only protection from DDoS attacks is generally handled exclusively by the cloud, since only a specialized provider can offer the kind of network bandwidth that is necessary when defending against this sort of attack.

7.3.2 Selection Criteria

As the market for MSS now starts to mature, customers are also becoming more demanding. Faced with increasingly sophisticated threats, they are looking for improved service readiness, end-to-end SLAs, on-premise operation where possible – all at affordable prices. Considering these requirements, the Experton Group views the following aggregated criteria as especially relevant for providers of managed security services:

- Breadth of security service portfolio offered, scope of security solutions operated by the provider (see 7.2)
- Range of support strategies intended to secure availability and confidentiality (e.g., failover protection, hotline availability, segregation in multitenancy)
- Security Operations Center (SOC) in Germany or Europe
- Own network (provider offers end-to-end responsibility)

7.3.3 Assessment of Deutsche Telekom/T-Systems as a Managed Security Services Provider

The Experton Group published its second Security Vendor Benchmark in 2015. In this major review of the provider market, the Experton Group also analyzed and rated providers for managed security services based in Germany (see Fig. 7.1). A large number of individual criteria was used to evaluate the providers. These individual criteria were weighted to reflect the respective product category, and used as the basis for assessing the appeal of the security offering ("portfolio attractiveness") and the provider's position in the market ("competitive strength"). These two dimensions form the two axes of the "Experton Market Insight Quadrant." Each of these axes is itself dichotomous, so that the Experton Market Insight Quadrant contains four segments into which providers can be categorized. Providers characterized by a combination of a highly attractive portfolio and high competitive strength are placed in the "Leader" segment. Leader companies can draw on a highly attractive product and service portfolio, plus a strong and well-established competitive presence in the market, and therefore fulfill all of the requirements for successful market development. They are to be viewed as strategic trendsetters and opinion leaders.

In the 2015 Security Vendor Benchmark, Deutsche Telekom (T-Systems and Telekom Deutschland) was placed in the Leader segment for Germany. In the

German market for managed security services, Deutsche Telekom is truly the provider to beat – both in terms of portfolio attractiveness and in competitive strength. Deutsche Telekom's portfolio extends across the entire MSS spectrum, and is supported by an end-to-end service program for securing availability and confidentiality (e.g., failover protection, hotline availability, segregation in multitenancy). One key feature of the portfolio is the inclusion of managed services for network hardening. Internet Protect Pro is just one of Telekom's services in its MSS portfolio, for example. This should be seen in the context of Telekom's view of security as an integral component and basic precondition for its entire product and service portfolio. With T-Systems and the Telekom Deutschland Business Customer Unit, Deutsche Telekom addresses the entire spectrum of industry – from small- and mid-sized enterprises to multinationals. An increasingly powerful argument for Deutsche Telekom – not only in terms of SME customers (cf. the overturning of the Safe Harbor agreement) – is that services are provided from Germany and are governed by the provisions of the German Data Protection Act. As a network operator, Deutsche Telekom can also offer end-to-end responsibility, from the data center/SOC to the customer.

Source: Experton Group AG

Fig. 7.1 Positioning of Managed Security Service Providers in Germany

7.3.4 Specialized Managed Security Services

Managed services is a strong growth market in mobile security, with many companies now utilizing service providers to reduce administrative costs and ensure that the protection of their mobile data is entrusted to experts. Alongside traditional software licenses and bespoke managed services, a firm footing has also been established by Security-as-a Service (SECaaS). For smaller companies in particular, SECaaS offers comprehensive protection from external cloud providers. Advantages include faster antivirus provisioning, continuous and automated virus definition rollouts (saving users from constantly having to update antivirus software themselves) and the outsourcing of tasks such as log management to the external provider. This model is especially attractive for companies with only a limited budget for overall IT security who require an adequate level of security for a large mobile user base. For mobile users, the solution is always a compromise between mobile freedom, the costs for a mobile solution and ensuring optimum protection for corporate data.

Many leading providers now also offer Mobile-Security-as-a-Service, and the Experton Group expects this segment to continue to grow. However, users of this model should always remember that the security of their confidential company data now lies in the hands of an external service provider. Accordingly, steps must be taken to ensure that the SaaS provider is an established company, which has been audited and certified by the German Federal Office for Information Security (BSI).

Markus a Campo works in the Experton Group as a Senior Advisor, specializing in information security with a particular focus on the analysis of IT architecture and IT security models. Other aspects of his work include network security, security audits, incident response, secure smartphone deployment, web application security, payment system security, as well as the ISO 27001 standard and the Baseline Protection Catalogues from the German Federal Office for Information Security (BSI).

As an Advisor, a Campo organizes workshops that address key information security topics of particular interest to customers and works with the customer to develop prospective solutions for meeting these requirements. A Campo studied computer engineering at RWTH Aachen University and received his doctorate in 1991. Following a position in the IT department of a large aluminum company, he has worked since 1997 as a consultant, author and trainer/lecturer in the field of information security. He also is an officially appointed and sworn appraiser for the Aachen Chamber of Industry and Commerce, with his field of expertise being "Information processing systems and applications with a focus on IT security." He is also an ISO 27001-certified Lead Auditor and Lead Implementer.

Henning Dransfeld works for the Experton Group as Manager Advisor and Program Manager Mobile Enterprise, where he specializes in advising ICT users and providers in the field of mobile enterprise on client strategy, mobile productivity, security and staff motivation. Dransfeld is a recognized expert in the analysis of ICT trends, the evaluation of provider strategies and competitive positioning, with over 18 years of experience in the industry. Before moving to the Experton Group, Dransfeld was responsible for Mobile Enterprise in Europe at Forrester Research, where he published a series of analyses on current mobility topics, including "Demystifying BYOD in Europe." Previously, he spent eight years in a number of roles at T-Systems, working as a project manager in the fields of marketing, distribution strategy and corporate strategy. Most recently, he was responsible for Solution Marketing for Mobile Enterprise and Workplace Services. Before moving to T-Systems, Dransfeld spent six years as an analyst at Ovum in London, where he headed the Advisory Service for IP communications services, with responsibility for numerous study reports and forecasts on topics such as IP communications services, and a post as Research Director for ICT Network Strategy.

Dransfeld is an experienced speaker at international conferences such as the European VPN User Association (EVUA) and the European IPQC Mobility Exchange. He is a graduate of the Henley Business School, the University of Wales and Université 1, Institut de Gestion Rennes.

Frank Heuer works at the Experton Group as a Senior Advisor and Lead Advisor for Social Business. He specializes in social business, communications services and solutions, unified communications and cloud computing, with a particular focus on communications-as-a-service. Heuer has worked in ICT market analysis and consulting since 1999. His fields of interest include ICT provider consulting on the topics of strategic and operational marketing, as well as sales. He has overseen go-to-market study reports and analyzes for leading providers on topics as varied as social business, unified communications (as-a-service), cloud computing, IT Security, telecommunications services, convergent solutions and next-generation networks.

Until 2011, Heuer worked at techconsult GmbH as Head of the Competence Center for Communications and Cloud Services. He co-authored the BITKOM Cloud Computing Guide, and is a regular speaker at conferences and webcasts in his fields of expertise. Heuer holds a degree in business administration from the University of Trier.

CSP, not 007: Integrated Cybersecurity Skills Training

8

Rüdiger Peusquens

Whether mid-sized enterprises or corporate giants: In a survey of senior management, 92 percent of respondents stated that IT security has "high" or "very high" priority in the organization (see Telekom 2015). And for good reason: In the Industry 4.0 era, with the growing intelligent networking of humans, machinery and production processes the risk of security attacks also increases simultaneously. Alerts, cyberattacks and other threats must be countered successfully on a daily basis – in a matter of hours, minutes and even seconds. The key challenge here is that IT systems alone cannot win the cat-and-mouse game between the hacker and the target. Well-qualified IT security experts are urgently required; but from where? The market for specialists in this segment is modest – not least because Germany has yet to provide dedicated vocational training and university degrees for defense and security experts. The handful of experts available is much sought-after and therefore very expensive. Long-winded tender procedures also cost time and money – and only provide mid-term solutions to the problem.

8.1 The New Profession of Cybersecurity Specialist: From IT Worker to IT Security Expert

What can be done? Our solution: ensure an adequate skills base within the company, build up expertise and train employees to meet your needs. As a large multinational, Deutsche Telekom employs well over 100,000 people. Among the 9,000 apprentices also working at Telekom are IT experts whose training is of great concern to us; but not necessarily with a focus on security. We need a bridge that leads from vocational training to future employment as a security expert.

R. Peusquens (✉)
Deutsche Telekom AG, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany
e-mail: ruediger.peusquens@telekom.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_8

The challenge in the process: A cybersecurity expert effectively requires two occupational training courses, namely a solid standard of education in IT or networks plus dedicated security training. This is where our specialized security advanced training is making a difference: A program that comprehensively, strategically and in a structured manner teaches cybersecurity. The concept emerged in mid-2013 and was formulated thus: We need an entirely new job profile, and a curriculum of advanced training that qualifies IT experts into IT security experts.

In cooperation with the Cologne Chamber of Industry and Commerce (IHK), Telekom developed an advanced training program: The prerequisite is a successfully completed IT-specific vocational training or equivalent dual studies. After two and a half years and successful completion, participants may carry the IHK-certified, nationwide-valid title "Cybersecurity Professional." In addition, the program also partners with the university federation "Open C3S" (Open Competence Center for Cybersecurity) – the largest vocational and further training initiative in the field of cybersecurity in the German-speaking market. The future IT security experts complete appropriate courses there as part of their training.

The IT security positions created especially for graduates of the course attracted over 230 applications. The first development program started in late September 2014.

8.2 Hands-on Experience in All-Round Security

A central element for the advanced training to become a Cybersecurity Professional is hands-on activity in the profession's task area, i.e., practical work in the professional departments. These include all departments that have relevance for IT and network security, and which therefore require employees with sound IT expertise – from the Cyber Defense Center to units working with application security, security-on-access networks and user devices, as well as groups working on fraud detection.

By dealing with the daily requirements from the departments, typically handled in a project format, course trainees develop their expertise step by step. This process is supported in parallel by a modular subject-specific and cross-subject advanced training. Trainees also develop their expertise in a range of formats, from face-to-face seminars to online courses and e-learning. The skills and abilities acquired in these modules can then be immediately applied and further developed directly in workplace projects. In this way, the program integrates practical occupational requirements with the targeted reflection of academic and scientific content, enabling the new IT security experts to apply the latest research in order to resolve challenges in their profession.

To ensure that the course offers both maximum quality and current relevance, the acquisition of specialist professional expertise features strongly in the curriculum. To secure the learning progress, each participant receives support from a subject coach as well as from a course learning process supervisor during the vocational training program. The subject coach is an employee in the department where the trainee also works. This person acts as a mentor to the student and is the first point of contact for day-to-day issues and problems. To avoid hierarchical

conflicts from the outset, subject coaches must not be immediate supervisors – e.g., team leaders or managers. The learning process supervisors, however, can be consulted on any general topic concerning the program and also organize communication and networking within the student body. For this purpose, regular face-to-face meetings and workshops are held, in which the budding Cybersecurity Professionals tackle work together on common projects. These events add up to around 40 days of the total time spent in the two-and-a-half-year program. To qualify for the final IHK examination, participants must have an attendance record of 80 percent or more for these classroom-based units.

8.3 Cybersecurity Expertise for Managers, too

At the end of the advanced course, participants must demonstrate their acquired knowledge by autonomously processing and solving a project task. Those who successfully complete this exam receive IHK "Cybersecurity Professional" certification. Once trained, the new specialists can then be deployed to tackle any relevant task areas within the Group. In addition, course participants have the option of taking individual exams for the study units scheduled as part of the program, and thereby acquiring six undergraduate certificates as well as the associated European Credit Transfer and Accumulation System (ECTS) accreditation.

Yet the Cybersecurity Professional course is actually only one of many strategies that Deutsche Telekom is using to combat skills shortages in the field of IT security. In addition, all employees regularly attend security training and are made aware of the issue with a variety of security awareness measures. In addition, modules for managers are also planned, designed to provide management staff with specialist knowledge of selected important IT security topics. These skills will enable prompt and competent decision-making by managers on security-relevant aspects of their day-to-day work.

8.4 Conclusion

Deficiencies in IT security are the Achilles heel of our society, in which humans and machinery are now increasingly networked via the Internet. To achieve greater security in the network, stakeholders need to work together far more closely to create transparency and to establish clear responsibilities and advanced expertise to provide better protection for data and infrastructure. An understanding of the need for IT security must also be established and maintained – both for employees at all levels of the corporate hierarchy as well as for customers. Cybersecurity must stop being seen as an annoying "add-on" for IT: It needs to be presented as a truly critical aspect of day-to-day life until everyone recognizes the hugely important role IT security now plays for us all. In the process, however, security must be simple and easy to obtain and to use – otherwise it will not be implemented.

The great interest of organizations and companies outside the Group in our program confirms the high relevance of the topic in the whole industry. Thus, currently industry associations and the Federal Institute for Vocational Education – the recognized center of excellence for research and development of vocational education and training in Germany – are discussing how specific IT security content itself could be integrated into existing training occupations; and how it could be possible to establish a separate occupational profile such as "IT Security Specialist."

All of this shows just how well the topic resonates with the industry. The major challenge for the future now consists of not resting on one's laurels but instead working to continuously expand the program. As described at the outset, in (cyber) security often a few hours, minutes or even seconds are decisive as to whether an attack is averted or causes damage – and new, entirely novel and unprecedented threats now arise on a daily basis. Looking to the future, one of the primary tasks will therefore be to review the content of this two-and-a-half-year program and adjust the curriculum to the current threat situation – possibly even during ongoing courses.

Reference

Telekom (2015). *Cyber security report 2015*. Accessed July 28, 2016, from https://www.telekom.com/static/-/293656/2/Cyber-Security-Report-2015-si

Rüdiger Peusquens is Vice President Cyber Defense and Situation Management at Deutsche Telekom AG. After receiving his doctorate in nuclear physics, Peusquens began his career as an IT security consultant at debis Systemhaus. During this period, he set up a vulnerability reporting service and completed white hat hacking work for customers in the form of penetration tests.

With the takeover of debis Systemhaus by T-Systems, Peusquens moved to Deutsche Telekom AG, where he used his six years of consultancy experience to contribute his considerable expertise to Group security work. He took on the setup of the internal penetration testing team for quality assurance work in technical security. His most recent work now involves attack detection and defense. His current position brings together the responsive forces of cybersecurity and business security to focus on early detection and rapid countermeasure deployment for security incidents at Deutsche Telekom and its customers.

Human Factors in IT Security

9

Linus Neumann

Imagine you are a hacker suddenly faced with an insurmountable technical challenge: Your target's email server has been well configured, its publicly known vulnerabilities have been eliminated and an as-yet undisclosed vulnerability is either unobtainable or much too expensive. Do you give up? No, you just ask for the password.

One of the most common myths about hacking attacks is that they usually require a high level of technical sophistication. However, you really don't have to possess special technical skills or secrets to be a hacker. In reality, the opposite is often the case: Criminals can successfully gain access with little or no technical knowledge. Most of them make use of "off the shelf" hacking tools which are available either as open source software or from underground online marketplaces. The inconvenient truth is that you – yes, you – are much less secure than your computer. And no attacker wants to do more work than is actually necessary.

9.1 IT Security Is Just Not Very People-Centric

Most people know very little about the inner workings of their computers. Their complexities are indeed quite difficult to fully grasp. It is just as difficult for us to appreciate the principles of computer security. Our understanding is often hampered by something much more basic: IT security does not work the way we intuitively expect it to. It makes assumptions that we often find difficult to fulfill.

L. Neumann (✉)
c/o CCCB, Marienstr. 11, 10117 Berlin, Germany
e-mail: kontakt@linus-neumann.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_9

9.1.1 The Thing with Passwords

We have all been there. We need to create a new password for our business account. It should have more than eight characters. It should comprise letters, numbers and special characters. We must not write it down anywhere. And we need to change it after three months. How annoying that we can't just use our standard password: the one we've always used whenever we opened a new account. For our personal email account, for Facebook and for that small online store that had a special offer on some really stylish shoes last year. It's much more convenient to use the same simple password for everything.

We are warned all the time that we have to vary our passwords – but how are we supposed to remember them all? Anyway, how would anyone possibly guess our password? We might have used our partner's name but we were careful to replace the A with a 4. How could anyone figure that one out?

What we tend to forget is that the password is potentially known to every single website on which we use it. How securely it is stored there is anyone's guess.

In fact, reusing the same password for different services is one of the biggest IT risks that we expose ourselves to on a regular basis. A single unauthorized access or a single security hole at one of the many services we use is all it takes to give an attacker control of all of our accounts.

But how are we supposed to remember all these different passwords? Nobody can memorize them all – especially if they have to be totally "random" (i.e., cryptic) and long. And what is all this about anyway? "At least eight characters?" Why not just six?

The exponential relationship is not obvious to us because we cannot imagine how anyone could "crack" a computer password simply by guessing (although sometimes the guessing is far from simple). You start with 'a' and finish with 'ZZZZZZZZ' – if you ever get that far. While you can try all possible combinations of six characters in a few hours, eight characters require months and nine characters years, even with the computing power provided by a modern PC. It is hard for us humans to grasp the two aspects – to imagine, on one hand, how quickly a computer can rattle through all possible combinations; systems optimized for password cracking can easily achieve several million or even billions of attempts per second.[1] And yet on the other hand, it can still take quite some time to guess a few letters, numbers and special characters.

Unfortunately, our desire for ease of use leads us to undermine the very mathematical principles upon which our password protection depends. A "password" is an intrinsically perfect concept: Just a few bytes of information are sufficient to provide us with effective security protection. But our large number of password-protected accounts makes it impossible for us to remember a different password for them all. This is why we resort to simple, popular passwords like "password123," which make it very easy for attackers to penetrate what may have otherwise been a technically secure system.

Our simple, everyday needs make it impossible to reconcile IT security with ease of use, as our first example has demonstrated.

[1]The actual speed at which passwords can be cracked depends on whether the cracking takes place locally or remotely, the latter being significantly slower. The technical characteristics of the security system – the hashing algorithm – also make a difference.

9.1.2 The "Security versus Productivity" Dilemma

If you ask the people working for a large company what they see as the biggest brake on their productivity, they are quite likely to say "IT!" They cannot swap files easily and quickly because USB sticks are banned and are not recognized by their computers anyway. Before they can read their emails at a hotel, they first have to set up a complicated VPN connection. And they cannot even configure their company account on their neat new tablet.

There are good reasons for all of these restrictions, but what they have in common is that in reality they hinder users more often than they protect them. This is dangerous in two respects: It decreases satisfaction with and confidence in IT, and it encourages users to find ways to circumvent the restrictions. Instead of carrying out work on their secure corporate laptops, staff use their personal devices – because they will accept USB sticks. Important emails are simply forwarded to a private Hotmail account so that they can be read easily and conveniently on a tablet during a flight.

This causes sleepless nights for the company's IT security professionals because these users are completely outside their control. A common reaction is to impose even stronger restrictions, warnings and prohibitions, thereby antagonizing users even more. The result is an even lower level of security than was the case before the restrictions were introduced.

What those responsible for IT security regularly ignore is that their coworkers really do want to make use of IT in order to carry out their work more efficiently. The last thing they want is constraints on the way they do their work, especially if those constraints don't make any sense to them.

This brings us to IT security's second fundamental problem: A computer either works or it doesn't. It is not able to distinguish between good and bad actions. Users either have permission to open, copy or even overwrite files – or they don't. If users are empowered to do something, that privilege can sooner or later be exploited during an attack. If they are not allowed to do that thing, they will try to circumvent what they consider to be an unnecessary restriction.

9.2 Social Engineering

Attackers know that people are often the weakest link in the security chain. They would have to invest many man-hours to track down and exploit new security vulnerabilities without any guarantee of success. With people, they can be confident of discovering any number of vulnerabilities as long as they employ a little creativity.

In addition, as Fig. 9.1 demonstrates, the organizations and businesses that really need to protect themselves against attacks, often have a wealth of resources at their disposal with which to protect their IT. These massive resources bear no relationship to their investment in "hardening" their staff against hacking attacks.

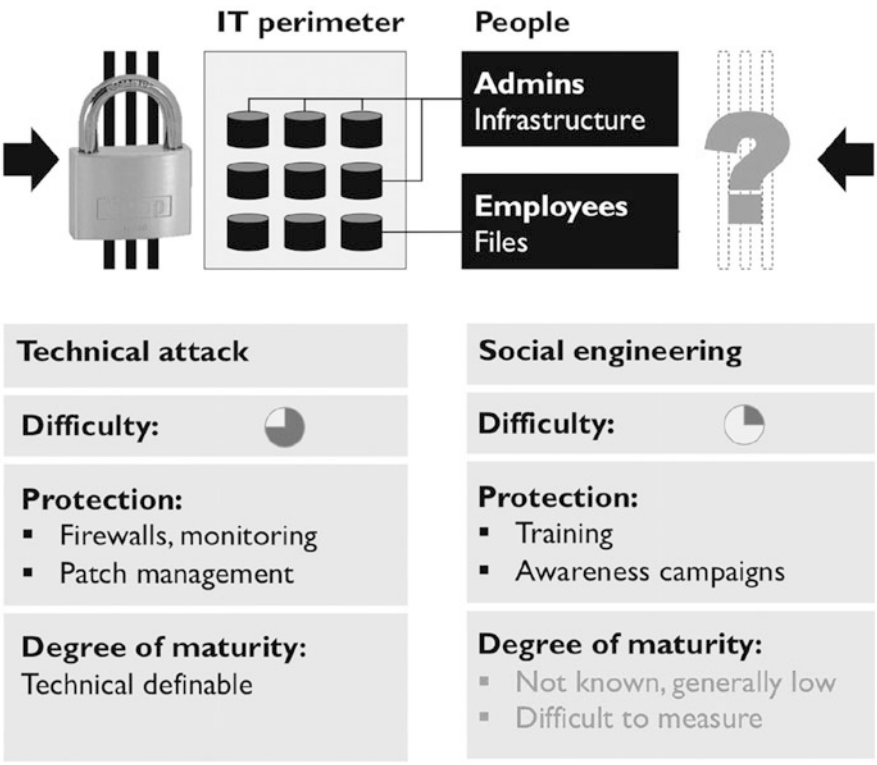


Fig. 9.1 IT Is Often Much Better Protected than the Person Who Uses It

A typical attack can be divided into five phases, which are summarized in Fig. 9.2. Without some sort of vulnerability, an attack is not possible. We also need an "exploit" for the vulnerability, or a way of manipulating the target system so that it does what we want. The actual "manipulating" is done by the "payload," which could, for example, be a trojan horse secretly lurking on an infected computer. Finally, we have the access rights that will allow us to carry out whatever attack we have in mind.

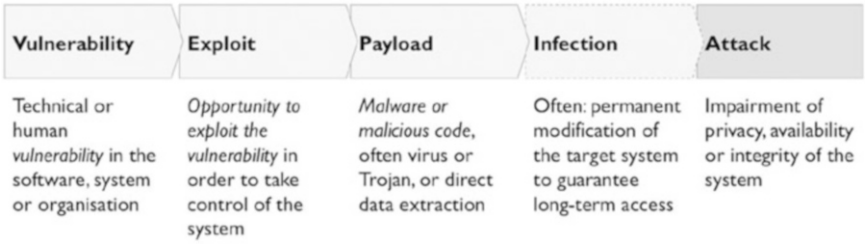


Fig. 9.2 The Phases of a Typical Attack

The human factor is particularly important in the first phase, as attackers are rarely in a position to automatically plant a targeted "drive-by" trojan infection. They have to rely on their victim opening and executing the file. The same is true for passwords: Attackers usually lack the ability to remotely crack a password and depend on their victim's willingness to reveal it to them. But how exactly?

9.3 Human "Weaknesses" Are Often Social Norms or Simple Instincts

Many of these human weaknesses would be strengths in another context. Characteristics such as helpfulness and friendliness are fundamental to our social relationships, just as curiosity is fundamental to our ability to solve problems. Hackers regularly exploit these character traits to get us to infect our own computers or to reveal our passwords.

9.3.1 Would You Mind Installing This Malware on Your Computer?

In early 2016, many people in Germany received one or more email reminders about an unpaid invoice from a company they were not familiar with. The details, it read, were to be found in the attached Word file. "That's just not possible," the recipients thought. "I'd better take a closer look." When they opened the file they saw a blank document, along with a warning from Microsoft Word that the document had "active content" that was currently disabled. The advice – please click on the "Activate content" button to see the active content – might not sound unreasonable to someone staring at a blank page.

Those who accepted this advice would become one of the many victims of the "Locky" cryptotrojan. The "active content" was a macro embedded in the Word file that downloaded the blackmailer's software from the Internet and ran it on the computer. This would be followed by a ransom demand of about 250 euros to restore the files that had been made unusable.

As we see in Fig. 9.2, each of the various stages of the attack is distinct and separate: The vulnerability is the user. He reads his messages without a second thought and opens those that he considers of interest. The covering email seeks to exploit this vulnerability. The curiosity and concern aroused by this seemingly unwarranted reminder can prove irresistible. Clicking on the "show content" message overrides the technical protection measures in place to prevent the running of active content. So the user downloads the cryptotrojan – the payload – onto his computer and runs it.

From a strictly technical standpoint, no technical vulnerability has been exploited here; the attackers are simply exploiting the gullibility of the victim. It did not take long for a considerable number of these infections to occur. Everyone was talking about "Locky" – and not just the specialist IT press. The attackers therefore needed to come up with something new. So they sent out emails with the subject line "Official warning about the Locky computer virus," which asked the recipients to follow the instructions contained in the attachment (see Fig. 9.3). Opening the attachment resulted in a nasty shock.

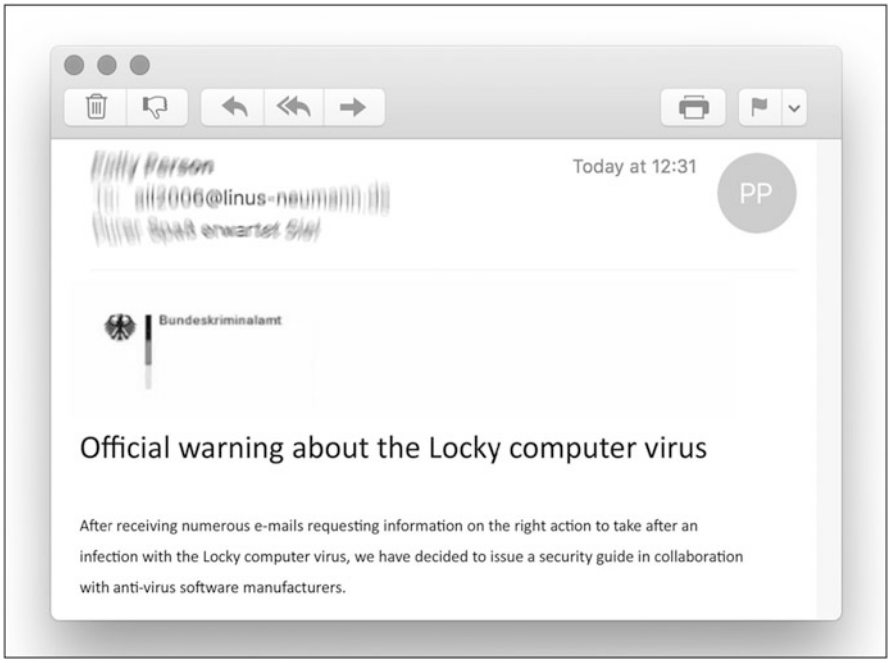


Fig. 9.3 Phishing Email Claiming to Be a Warning from the Police

Another way of getting unsuspecting victims to run malicious software is to deliberately "lose" USB flash drives. These contain a small number of files, named to give the impression that they contain confidential data. Also on the stick is another file, prominently positioned and named "To the honest finder." In reality all the files contain malware configured to attack the systems of curious and honest finders alike.

Some remarkable hacking successes have been achieved at a cost of a few euros for each stick left somewhere on the company's parking lot.

9.3.2 Excuse Me, What Exactly Is Your Password?

Even today, the holy grail of remotely executed espionage and sabotage remains the email password, because this is the gateway to everything else: It enables the intruder to monitor business communications down to the very last detail, to impersonate the victim in communications with third parties, and for good measure, it allows the intruder to reset most other account passwords through email verification. This potentially gives the attacker access to Facebook, Paypal or business bank accounts. But the most dangerous aspect is that the attacker does not even have to use malware, which could be detected by a virus scanner.

Many email servers – particularly those in companies – disconnect after a few failed login attempts and insist on renewed personal authentication. Attackers therefore cannot keep guessing as often as they would need to, but must instead convince victims to reveal their passwords voluntarily.

One popular method is to get a victim to go through the process for changing the password – something users in companies are required to do regularly. The target person receives an email telling them to renew their password. If they fail to do so, access will be disabled within the next few days. The email includes a link to carry out the request immediately. When the target clicks on the link, they see the usual login page, and once logged in, they are presented with an input field in which to change the password.

What likely went unnoticed, is that the linked login page is a near-perfect malicious clone crafted by the attacker. Preparing such a clone does not involve much more than saving the original page and then adding a few additional features to it. The old password is received and stored. The new password will also be stored and automatically changed on the real server. The attacker finally chose a domain name for the malicious website that looks very similar to the real address.

Merely substituting the letter L with the number 1, for example, would change the address https://mail.linus-neumann.de to the deceptively similar https://mail.1inus-neumann.de. Reversing or omitting letters towards the end of the domain name is another popular trick (https://mail.linus-neumnan.de). The human brain doesn't always read words right to the end once it has "recognized" them. It is therefore unlikely that victims would notice the difference.

Following this brief visit by the victim, the attacker is now in possession of both the old and the new login data. He can also see if the victim follows a particular pattern when changing the password – just changing one letter, for example, or

incrementing a number. Armed with this knowledge, the attacker does not have to be too concerned if the victim changes his password again. Now, the next thing the attacker does is to download all of the victim's emails and sift through them before deciding how to proceed.

If you are anything like me, you get a couple of dozen emails like this every day. They are often poorly written and are rejected by the spam filter anyway. But all it takes is for you to let your guard down for a second – and an attacker who is skilled at his craft.

Indeed, there is a world of difference between an expert and an amateur, and between mass phishing and a carefully targeted spear fishing attack. With the former, hundreds of thousands of emails are sent indiscriminately to multiple recipients and quickly end up in spam filters, while the latter target specific individuals. These emails refer to their recipients by name and provide faultless instructions in the language they expect to read. A familiar footer with the company logo and callback number also helps to convince the victim of the legitimacy of the request. And spam filters? They are not too worried about a single email; they are trained to detect and block mass mailings. Consequently, most spear-fishing attacks manage to stay completely under the radar.

A recent attack targeted a steelworks in Germany. The 2014 Management Report of the Federal Office for Information Security (see BSI 2014) describes how the attackers tried to use spear fishing emails to get their foot in the door. Over time, they managed to gain access to a number of the plant's control components, causing parts of the plant to fail. They finally caused a furnace to end up in an undefined condition that prevented it from shutting down properly, resulting in massive damage to the plant.

9.4 Would You Please Transfer Me a Few Million?

Most attackers generally have one goal in mind: making money. There are various ways of doing this – making money from an attack they carry out themselves or getting a third party to pay them to carry out an attack. But why make it difficult for yourself – when you can simply request a large transfer of funds?

The boss is out of the office attending an important meeting with business partners. It promises to be a quiet day at the office. But a frantic email causes disquiet. The deal is likely to fall apart because a vital transfer of funds has not taken place. The boss is angry and piles the pressure on his staff: "Please transfer the funds without delay. If the money doesn't arrive tomorrow, all our work has been for nothing. How could this happen?"

The amount? A six- or seven-figure sum payable to an offshore bank account – a run-of-the-mill transaction for a large business. Overwhelmed by a mixture of guilt and indignation, the boss's PA gets to work. Has the boss really not mentioned this payment before, or had it just got stuck in the accounts department? Anyway, something needs to be done about this urgently. The transfer is completed within a few minutes. A short click on "Reply" and the boss sends a friendly thank-you message: "Just in time, thank you."

When the boss returns from his business trip a few days later, his PA thanks him again and asks him if it all went well. “But of course, what could possibly have gone wrong?”

It slowly dawns on the victim. The email claiming to be from the CEO was a well-crafted forgery – and by now the money will have been transferred by a circuitous route from the offshore account to anywhere in the world.

This scam, known as the “Fake President Fraud,” relies entirely on the psychological blind spots of the victims. It is usually based on exploiting the universal values professionals live by: authority, speed, trust, and often secrecy. Variants of this method base their approach on the offer of a secret deal that may not yet be public. The employee who receives the message is one of a select few who are being taken into confidence – and is required to keep the matter confidential.

These cases, which are more common than you might think, often end with the employee’s dismissal and with a company reluctantly swallowing its losses.

9.5 Defensive Measures

The work of an IT security engineer within an organization is never done. Every day, new vulnerabilities are discovered and have to be dealt with. The IT security engineer has one advantage, however. Once a vulnerability has been eliminated, it is not likely to return soon.

This is not the case when it comes to “human” IT security, where a one-time “immunization” often only has a specific and temporary effect. Even slight variations in attack patterns can increase the chances of finding victims and the odds improve steadily over time.

Many organizations try to warn their staff by sending out regular mass mailings about the risks from such attacks. In practice, however, these warnings have a barely measurable effect that makes them of little practical relevance.

Therefore, hardening an organization against social engineering attacks requires ongoing programs that not only deliver a flow of information about the methods used by the attackers but also include mounting simulated attacks against the users themselves. If they click on the fake phishing messages, they receive an immediate warning and advice.

These simulated attacks should cover the whole gamut of scams employed by hackers. At the same time, the campaigns should be used as an opportunity to strengthen trust between the IT department, IT security and the employees. Allegations and heavy-handed lecturing are unlikely to encourage employees to contact the security specialists if they come across something suspicious.

Since most attacks take place via email and simulated phishing attacks are easily scalable, the principles involved are explained below, based on a typical phishing campaign. By regularly repeating a variety of different attacks, it is possible to evaluate the success of the campaign in terms of the two main learning objectives: Is the number of successful attacks going down? And are attempted attacks being reported more quickly and more often?

9.5.1 Recognizing Social Engineering

Due to their diversity, it is not really possible to devise a technological means of recognizing social engineering attacks. The cover stories are so diverse and the fabricated scenarios are too close to real-world situations. Yet, they often have one thing in common that a trained eye is able to identify: Social engineering attacks usually contain small cues designed to switch us into action-oriented mode without thinking about it much. This can be achieved in two ways: through boredom or excitement.

Familiar, run-of-the-mill situations that we don't think about too much can be exploited. Classic examples are holding open a door for the person in a hurry behind us, getting rid of a familiar warning by clicking on it, or – as described earlier – regularly changing our passwords.

We are just as careless when we are excited: A task must be carried out without delay or else bad things will happen. Classic examples are the software that is supposed to remove what is claimed to be a virus from our computer, the sum of money that must be transferred as a matter of urgency, or the unwarranted payment reminder that we want to refute.

When we are excited or bored, we often do not stop to ask ourselves whether a request is credible or sensible. If we want to immunize organizations against social engineering, we must therefore instill a healthy degree of suspicion. Unfortunately, we have to ensure that this level of suspicion is not so high that it impacts normal working relationships too strongly.

The relevant mechanisms are best demonstrated with some concrete examples. The best time to think about what you have just done is right after you have logged into a phishing site. Users can be alerted to suspicious details that they would normally overlook and can be advised on what they should do in the future. The teaching materials used for this purpose should be memorable and attractive. Specially produced video shorts, no more than two or three minutes long, are particularly effective at getting the point across.

9.5.2 The Learning Objective: Reporting Suspicious Activity

To create a solid defense against attack, an organization must ensure that all targets of a phishing or spear-phishing attack immediately report suspicious messages to the responsible department, usually the IT department or IT security department. Appropriate countermeasures should be taken without delay.

Responses to a phishing email could include the following:

1. Access to the phishing server that is hosting the fake login page is temporarily blocked in the internal network. If the structure of the organization permits, it may also be advisable to temporarily prevent access by external IP addresses to the mail server in question.
2. A warning is sent to all users requesting notification if they have clicked on the link.

3. Affected users receive a detailed debriefing explaining the process and the risks posed by the attack.
4. Working closely with employee representatives, it might be possible to identify the targets of the campaign from the mail server logs. This would make it easier to approach those individuals in order to warn them of the possibility of further attacks, and could also help to explain the motives for the attack.
5. A password reset will be needed for the targets, and in case of doubt, for the entire organization. Steps must be taken to ensure that only reauthenticated users can perform the reset. It is recommended that all affected accounts are frozen until the passwords have been changed. This must be done strictly from within the internal network.

IT should be prepared to take the appropriate measures and to react to the attack quickly but in a calm and collected manner. At the same time, it should expect an increased volume of false alarms as a result of raising employee awareness about the issue. A friendly and encouraging response will help retain the willingness of staff members to report problems. "Rather one report too many than one too few" should be the maxim.

The reporting rate should be evaluated in detail as part of the next simulated attack. How many users fell victim to the attack before it was reported to IT? Experience has also shown that it makes sense to look at whether employees reporting suspicious activity were previously victims themselves and have therefore already seen the teaching materials and the appeal to report anything suspicious. Because attempts to paper over one's own past mistakes can distort the analysis, these reports should not be counted as successes.

9.5.3 Practice Makes Perfect

The first time an organization systematically evaluates its susceptibility to social engineering, the results are often alarming. While the susceptibility of employees to phishing typically lies in the high single-digit percentage range, the success rates achieved with spear phishing normally reach mid to high double digits. It should be assumed that targets who have not proved susceptible have simply ignored or forgotten about the message – because reports of suspicious messages are extremely rare.

But that is not all. These evaluations regularly discover that some employees have not only been unaware that an attack was taking place, but have even gone so far as to establish a cooperative relationship with the attacker. In one particular case, support questions were still being sent by the employees of the targeted organization to the attacker's email address months later. The printer wouldn't print, attachments were too big to send via email, new employees needed to access certain accounts – the problems that the employees communicated to what they believed was the company's IT department were many and varied. Each of these messages gave the hackers another opportunity to compromise the organization all over again.

9.6 Conclusion: IT Must Work for and Not against Users

Social engineering attacks are not just a very effective means of infiltrating an organization; they are another long chapter in the ongoing battle between IT and users. Vulnerability to these attacks can be reduced only by conducting regular campaigns and simulated attacks. These campaigns provide a welcome opportunity to improve relations between users and IT managers.

After all, "normal" users are much more at risk than IT professionals. While the latter are perfectly familiar with concepts such as "email headers" and "spoofing," many users have no idea how easy it is to impersonate an email sender or forge an email.

In an ideal world, the IT department works hand in glove with the rest of the workforce. But often this is no more than wishful thinking. When it comes to defending against social engineering attacks, it is helpful if both sides are able to speak openly. The IT department should therefore think twice before publicly venting their frustration about mistakes users make. The users, for their part, could be more open in discussing their needs with the IT department and more appreciative of the advice they receive – because ultimately, they both share a common goal: making sure that the company and its sensitive information remain secure.

Reference

BSI (2014). *Die Lage der IT-Sicherheit in Deutschland 2014*. Accessed June 6, 2016, from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

Linus Neumann is a psychologist and hacker. While studying to earn his degree in psychology at Humboldt University in Berlin, he also showed an interest in political science and forensic psychiatry.

He consults German and international organizations on IT security issues and talks about the political and social ramifications of digital transformation in his "Logbuch: Netzpolitik" podcast.

Neumann has appeared as an expert for hacker organization Chaos Computer Club before committees of the German Parliament, contributing his expertise on e-government and the IT Security Act, for example.

Secure and Simple: Plug-and-Play Security 10

Dirk Backofen

These days, companies from all industries and of all sizes – but primarily small and medium-sized enterprises (SMEs) – are required to deal with pressing questions. To remain competitive, they need to introduce and implement new technologies and take account of the demographic trend, globalization, and the continuing shift in the focus of industry to the services sector. This can only be achieved with the aid of digital processes. Digitalization provides a whole range of new possibilities for companies. In particular, the cloud is a cost-effective, simple, and more flexible option for competing successfully.

Yet companies' IT environments are being bombarded – with almost incessant cyberattacks on corporate networks. These, in turn, are ill-protected: Only last year, Germany's National Initiative for Information and Internet Security (NIFIS) said there was a lot of catching up to do in the area of security, especially with regard to securing the Internet of Things. This is especially true for SMEs, says NIFIS (see NIFIS 2015).

Likewise, there is an urgent need to provide greater security for mobile devices such as smartphones and tablets, as techconsult's latest "Security Bilanz Deutschland" shows. In this security poll, 50 percent of German companies stated that they had not found good solutions for identifying viruses and malware. When it came to solutions for mobile devices, this figure increased to as much as 66 percent (see techconsult 2015). Companies are keen to protect themselves better but lack the IT security experts to do so.

For example, a report by the Federal Office for Information Security showed that only one in two companies has the expert capacity to appoint an IT security officer (see BSI 2011). We can see that security is emerging as the final obstacle to digitalization.

D. Backofen (✉)
T-Systems International GmbH, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany
e-mail: dirk.backofen@t-systems.com

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_10

One solution could be an approach that initially sounds paradoxical: In the age of digitalization, the best protection against attacks from the Internet might also come from the Internet. With what are known as managed services, customers receive an easy-to-use all-round protection package from the cloud that secures their industrial networks, data and applications, and gives them early warning of cyberattacks.

10.1 Data Security in the Danger Zone

German companies of all sizes are successful worldwide and often market leaders, yet they worry about security. If the Bundestag (German parliament) and other large organizations are vulnerable to hacking, how, then, are small and medium-sized enterprises in particular supposed to protect business-critical data and applications? Reports of new attacks and infections by computer viruses appear daily. According to Bitkom, Germany's digital association, approximately half (51 percent) of all German companies were victims of digital industrial espionage, sabotage or data theft between 2013 and 2015. The resulting losses to the economy amount to around 51 billion euros per year, with SMEs being hit the hardest (61 percent of the attacks). The sectors that are attacked the most are the automotive industry (68 percent), followed by the chemical and pharmaceutical industry (66 percent), then banking and insurance (60 percent) (see Bitkom 2015b).

What we also know is that cyberattacks are becoming increasingly frequent and more refined. This forces the companies affected to repeatedly invest in new security mechanisms and possibly pay ransoms for stolen data. What is more, such attacks lead to a loss of image and trust, which in turn causes greater customer churn and a drop in revenue. Experts therefore put the global losses resulting from cyberattacks at between 400 billion and 2.2 trillion US dollars (see A.T. Kearney 2015). In most cases, companies are unable to keep pace with criminal IT development. The consulting firm Roland Berger estimates that 250,000 new malware programs are discovered daily (see Roland Berger 2015). The number of programs that actually exist is likely to be significantly higher.

Company managers are well aware of the seriousness of the situation but lack the skills, manpower and easy-to-use solutions to close the lines of defense. How could it come to this, especially as security has always been one of companies' top priorities? A poll conducted last year by Matthias Zacher, senior analyst at IDC, revealed that improving security – especially the security of mobile devices – is one of the three most important initiatives this year for 62 percent of companies. However, techconsult's "Security Bilanz Deutschland" study showed that there are major problems even with relatively simple solutions such as antivirus programs or firewalls for smartphones and tablets. Only one third of the SMEs surveyed professed to be satisfied with the implementation of corresponding solutions at their companies (see techconsult 2015).

This is highly significant because companies feel they are at risk from a whole series of attackers with different objectives ranging from cyberwars, advanced persistent threat (APT) attacks and cybercrime to e-espionage, hacktivism, and

e-vandalism. Companies especially do not accord APT due attention, say experts (see IDC 2013). According to a study, one in five companies have not implemented any APT-specific defense mechanisms.

The attacks, aimed at data theft and encryption, have different objectives: extortion, interrupting operations, causing loss of image, and misusing the company's own IT systems for criminal purposes. In a worst-case scenario, the companies involved may end up having to cease operations.

As expected, companies have mainly focused on protecting their data centers and business-critical applications. However, this is not enough. There is now a bewildering number of tablets and smartphones at the periphery of company networks. These are the least secure elements in an enterprise's information technology landscape. This is even more the case when private devices are used for business purposes ("bring your own device").

IT security officers face the task of adequately considering old challenges and new requirements in equal measure (see IDC 2013). This is because cyberattacks are currently only discovered in companies after an average of 230 days, giving the attacker a long time to cause damage unhindered. What companies therefore need are easy-to-use solutions that are able to identify the attacks promptly and initiate defense mechanisms immediately. Malicious code, cyberattacks, and data theft need to be blocked as quickly as possible and, at the same time, suspicious files should be detected through "sandboxing" – by executing them in a protected environment.

A sandbox is a separate area in which processes can run without affecting the software environment. For example, a virus can be safely activated there and its mechanisms can be studied. It is shielded from the rest of the system, just like a child in a sandbox, where it can "play" safely. At the same time, the system time can be accelerated so that system processes can run faster than usual and anomalies such as viruses can be identified within minutes – not after an average of 230 days.

Sandboxes traditionally look like an operating system that builds on a virtual machine or runs in a container. What may sound trivial is actually very tricky, although nowadays even browsers like Google Chrome have built-in sandboxes where they test code on websites to determine whether this is harmful and warn the user if necessary. Solutions for SMEs are naturally far more sophisticated because the attack scenarios are also more complex. In addition, a sandbox must not impact network performance or work.

A sandbox therefore ensures in a simple manner that harmful activities are executed in a closed environment rather than in the company's network. In a closed area, it is possible to study the functioning of a software package that was previously unknown. This was how the cryptolocker "Locky" was detected in March 2016, for example.

Locky and its multitude of variations are what is known as ransomware, to which companies are increasingly exposed. Advanced versions encrypt documents and files on computers and hard drives that are connected on the same network. This enables cybercriminals to paralyze entire organizations and extort money from the victims in bitcoins. One of the companies affected at the beginning of 2016 was a

research institution where, in the space of an afternoon, Locky had encrypted the files on a central server and made them unusable (see Heise.de 2016). Many public authorities and companies in smaller communities were also affected during the same period.

Cybercrime has evolved into a separate branch of industry – the underground economy. Trojans like Locky can be purchased on disguised websites, known as the dark web, for a three-figure sum. The suppliers of such harmful code even offer their criminal clients support. And using such ransomware is lucrative: According to calculations by US security specialist Tony Robinson, online criminals can generate over a million dollars per day with it (see T-Online 2016).

In Germany, security experts and the police generally advise companies not to pay ransoms to online extortionists, telling them to focus their efforts on prevention instead. However, in practice many companies and local authorities are obviously unable to cope, because very often the ransomware infects computers through an infected attachment, be it an Office document, a PDF file from the fax machine or even JavaScripts on which the recipient unsuspectingly clicks.

In reality, Trojans and worms are currently the biggest hazard on the Internet, says Bitkom, Germany's digital association, with a reference to a report by the European Network and Information Security Agency (see Bitkom 2015a). Ranking second among the biggest hazards on the Internet are attacks using Web-based software, also known as "drive-by downloads." Visiting an infected website is enough to download harmful code unnoticed. Other hazards are manipulated smartphone apps, remote-controlled computers (called botnets), infected emails, often sent in huge quantities as spam, and attacks on sensitive access data – the dreaded "phishing." All of these hazards continuously keep appearing in new guises.

Here, easy-to-use big data analyses can be of great benefit. They analyze the behavior of data in the system, identify anomalies, and block further exchange where necessary. "Honeypots" have also proven to be very helpful, enticing potentially harmful code with seemingly interesting data and incapacitating it.

In addition, security apps for devices are highly effective: An algorithm capable of independent learning can also identify unknown risks through a real-time analysis of thousands of parameters in the operating system. These include zero-day exploits that target previously unknown gaps in security. Compromised devices can be excluded from the company network as soon as threats arise. They raise the alarm at the system's control center and send forensic data there for a detailed analysis of the attack.

To be able to react in an appropriate manner to all of the attack scenarios outlined, companies have two options: They can either develop and implement their very own security concept or get external help. The first case is anything but trivial – and, as seen, often fails due to the scarcity of experts who can build a powerful defense. In the second case, solutions exist that excel on the basis of their simplicity and come as a bundle from the cloud.

10.2 Digitalization Needs New Security Concepts

All of the problems known to us today relating to the securing of corporate networks can only be understood if we take recent developments in information and telecommunication technology (ICT) into account. Digitalization today is reflected in four major megatrends:

1. "**All is Mobile**:" Knowledge work in the twenty-first century is not possible without electronic aids. Almost every professional now carries a smartphone or a tablet to use for both work and leisure. Although laptops and desktop PCs are still the terminals preferred by 60 percent of users, smartphone use in Germany increased to 29.6 percent at the end of 2015 (see Webtrekk 2016). These days, users are accustomed to being able to access their applications on mobile devices. Needless to say, these applications must be up to date and synchronized at all times. For this, they need to be stored in a central location. This takes us to the second major digitalization trend.
2. "**All is Cloud**:" For centralized storage of applications and data, the PC or server has become obsolete. A centralized, highly secure cloud solution in a data center is what is needed to collect, store, and process the vast quantities of data. Cloud-Monitor 2015 found that 44 percent of companies in Germany deploy such solutions, while a further 24 percent are planning or discussing their use. As many as 74 percent of companies hope that using a private cloud will improve their access to IT resources, while three-quarters of users confirm that this goal has already been achieved (see Bitkom and KPMG 2015).
3. "**All is IP**:" The Internet Protocol (IP) has become the universal language of all communication processes. Instead of the devices of the relevant participants being connected directly as before, communication content is routed in data packages in an IP network. This conserves network resources and makes communication highly efficient. The packages may contain all manner of content – images, texts, videos; in effect, anything that can be digitalized. However, communication no longer solely takes place between people. In the Internet of Things, objects communicate with one another. Here, technology and usage are only in their infancy: Of the some 1.5 trillion objects on Earth that could in principle benefit from an IP address, just one percent are connected to the Internet, according to Roland Berger. It is not only smartphones and computers that use IPs; consumer electronics, communication devices, household devices, clothing, wearables, vehicles and many more objects can also speak this universal language. When the number of devices connected to the Internet reaches the 50 billion mark in 2020, just 17 percent of these devices will be computers or cell phones (see Kückelhaus 2015).
4. "**All is Secure**:" It is a fact that the number of devices connected via an IP is growing on an unimaginable scale. So, too, is the number of possible gateways for data thieves. The fourth aspect of digitalization has thus become the most important: What use is this promising new IP world if it is not secure? This has made the topic of security even more important for company managers.

No business owner can escape this trend. Whether digitalization is in fact worthwhile is no longer the issue – there is simply no way around it now. In this case, it is not the usual situation of large companies swallowing up the small ones; it is about the hare outstripping the tortoise – those who take too long to digitalize will lose out. For user companies the question is therefore not whether they need to digitalize but rather when, where and how securely they will digitalize. These are the decisive issues in the progressive process of connecting all the different devices in companies' distributed networks.

Given these exponentially growing potential gaps in security, how can a user company protect itself from unauthorized access? For providers of security solutions it is vital to understand users' concerns, anticipate them where possible and provide companies with solutions that are genuinely easy to use. What form do the user's digital processes take – a booking process, for instance? Generally speaking, many complex digital processes and mechanisms are used that need to be understood to give attackers no chance.

10.3 Digital Identity Is the New Currency

In the Internet age, the all-important currency is no longer money, but personal data that people divulge online and with which they then "pay" on the Internet, either consciously or unconsciously. But things can even be taken one step further: In the age of the insecure Internet the new currency is one's personal digital identity. Digital identities can take many different forms, and nowadays most people actually have a series of digital identities. People can reveal their identity in the digital world in the same way as in the real world. When users transfer money online, make online purchases, log into forums, social networks or email accounts, they authenticate themselves using a variety of methods. This is where mechanisms that assign individual attributes to a specific person come in. The user name/password combination is a common example (see Bundesdruckerei 2015).

Nowadays, even objects and companies have digital identities. This allows them to be clearly assigned in different process steps and to be traceable, for example in logistics or in Industry 4.0. They must be secured so that they cannot be falsified, manipulated or stolen – by criminals being able to gain access to them, for instance.

As a consequence, the protection of digital identities is closely intertwined with the protection of company data, because access to digital identity is what makes it possible to gain access to the heart of a company. The mechanisms for protection must be equally sophisticated. But how can non-experts know how best to protect themselves? This requires proven experts who ensure the protection of company networks including digital identities and business-critical data.

All-round protection like this is highly complex. However, the experts must not pass this complexity on to users. Their job is to dispel the users' fear of the apparently obscure technological steps in the background. Users should only become aware of the complexity – if at all – when switching a device on or off and as a plug-and-play approach – similar to the electricity that is fed to an

appliance unnoticed. SMEs in particular need "plug-and-play security" that is available at all times, quickly and easily. Comprehensive protection for data, networks, applications, and digital identities must ultimately be possible with just a small number of settings. This is the only way data protection can work.

10.4 Does Absolute Protection Exist?

Anyone who has ever had anything to do with security is guided by two ambivalent objectives. On the one hand, they want to get a comprehensive view of a system including all its possible vulnerabilities and weak points, and do everything necessary to achieve this. On the other hand, they have the feeling – in spite of all the analyses and measures – of being absolutely defenseless against a previously unknown threat at the decisive moment. This is the conflict that practically all security experts experience. How can the best possible protection for a company be provided if the company is expanding at the same time and constantly adding new IP connections? After all, it is not only the data and applications that must be made secure, but also the networks on which these run.

There is one thing that all experts can confirm: No security expert in the world can ensure absolute – in other words 100 percent – protection, even with the most sophisticated methods and mechanisms. The reason for this is obvious: Hackers and intruders are constantly competing with the security experts, both sides racing to find solutions or counter-solutions, ideas or opposing ideas. Progressive security experts have therefore proceeded to use intelligent mechanisms not only to identify the patterns that make an attack successful, but also to select the patterns that were atypical or unknown up to now, and to study their harmfulness.

Conventional security technologies, comprising virus scanners, web proxies, and similar mechanisms, perform what are known as deep package inspections, sweeping the network traffic for known threats. If they find such a pattern, the relevant data package, such as an email attachment, is disallowed. These procedures reach their limits as soon as an unknown pattern appears. Using conventional technologies would unleash this potentially harmful pattern on the company. It is important to prevent this in every case, which is why experts have developed processes such as the sandboxing explained earlier. Preventive defense mechanisms must move away from pattern-based analytical procedures that look for known patterns toward mechanisms that hunt for unfamiliar code. In the process, the analysis is expanded to include all elements that are incorporated into the network.

One conceivable approach in this environment is continuous monitoring of mobile devices such as cell phones or tablets – somewhat along the lines of a continuous electrocardiogram for human beings. This would involve compromised devices raising the alarm at the system's control center and sending forensic data there for an analysis of the attack. Other responses to a threat such as notification of the user or other countermeasures via mobile device management solutions can be set up on a case-by-case basis.

Such "continuous ECG monitoring" of a cell phone draws on a great many different vectors and sounds the alarm when, for example, the battery discharges surprisingly rapidly, there is a sudden spike in the CPU load or an excessive amount of storage is used. Whenever something happens that is not in keeping with regular operations, the cell phone is blocked.

Ultimately, the aim is to develop an analytical method that identifies anomalies without initially defining these in more detail. While this still does not provide 100 percent protection, the monitoring of a system increases it to the maximum level possible. And what is possible for smartphones must also be feasible in corporate networks, even though the access scenarios there are considerably more sophisticated and distributed.

10.5 This Is What Attack Scenarios Look Like Today

Denial-of-service attacks show just how elementary an intelligent analysis is. The attack deliberately overloads the computer systems of companies and other organizations. The hacker world generally launches distributed denial-of-service attacks whereby the attack is executed by many different servers previously hijacked by the attacker. These are referred to as zombie hosts. The victim is besieged by large numbers of inquiries, leading to the use of defective IP packages, for instance, and then terminates the service due to overload.

Individual PCs that point the way to a larger, higher-level network are often interesting as a gateway for these attacks. If, for example, the network of a large online mail order company were to malfunction, losses running into millions of euros would be incurred within half an hour. The data stolen from customer bank data could be used to extort a significant amount of money.

Another example is "phishing," the aim of which is to obtain, among other things, online banking login data or other types of passwords. Here, attackers generally use emails that guide the victim to a malicious website or encourage them to open an infected file. Incidentally, according to the Advanced Threat Report by security experts FireEye (see FireEye 2016), malicious code is sent in zip files in over 90 percent of cases. Malicious code like malware has now also started to appear in seemingly harmless email attachments such as ".doc" or ".pdf". This may signal the beginning of an APT attack in which attackers attempt to gain access to corporate networks, identities, and data in several steps, sometimes over a period of several years. DLL files are also increasingly being used instead of the more usual EXE files as they ensure that infections remain undetected for longer.

In the case of malware, attempts are also made to circumvent the sandboxing. For example, incidents are known in which the malware only became active when the mouse was moved – it effectively hid behind the pointer. In addition, there is increased proliferation of malicious code that can identify virtual environments – if the virus believes itself to be in a sandbox, it simply remains inactive.

Attackers and defenders thus continue the hare and tortoise race described at the beginning – like in the case of the aforementioned ransomware "Locky" that caused

a furor: This encryption Trojan even captured data from hospitals – both in Germany and in the United States – and tried to extort money from them. It could have been even worse: Not only had results to be communicated by telephone or fax for a while, but patient data could also have been manipulated or deleted – with really serious, i.e., life-threatening, consequences for those affected. Here, too, increased networking of (medical) devices – the Internet of Things – has beneficial goals, but also provides cybercriminals with a growing number of possibilities to access data.

With advanced persistent threat protection, which also prevents more complex access scenarios, the type of malicious code that had been unknown until that point could have been fished out and made harmless. This demonstrates that organizations which considered themselves secure in the past now need to revisit their security situation because the protection they established three, four or five years ago is now obsolete. IT managers and company directors are responsible for keeping the company's safeguards updated at all times and focusing on simplicity of use.

10.6 In Need of Improvement: Security at SMEs

Given the complexity of attacks these days and the defense mechanisms employed to counteract them, only specialists can keep on top of things. And specialists are now in short supply. SMEs and large companies alike are desperate to find suitable staff with the right skills to operate security systems under their own direction. However, these people are very difficult to find.

In many cases, SMEs therefore have little option but to outsource security to a trusted partner. In this respect, it has been found that the best protection against attacks from the Internet likewise comes from the Internet. With what are known as managed services, companies receive the all-round protection package from the cloud – for all targets in the company including the safeguarding of industrial networks and applications as well as the early identification and aversion of attacks. And they acquire all this without specially trained staff having to look after it – again, as quickly and easily as "plug-and-play security."

The mechanisms with which companies of any size protect themselves are nearly always the same. This is because the difference lies not in the attacks themselves, but in the size of the bandwidth of Internet traffic to be inspected. A set of tools comprising virus protection, firewalls, intrusion prevention, load balancer, web proxy, advanced persistent threat protection and some other procedures is generally used for this.

It is not uncommon for managers of SMEs to be overwhelmed by the complexity of the task. They are afraid to take the wrong step at a decisive moment. This often gives rise to security architectures that come in a variety of shapes and forms, are overly complex and heterogeneous and not always very efficient. It would be efficient to use security solutions that constitute "plug-and-play security" or solutions from the cloud. These can be ordered at the push of a button, are delivered as a package, preconfigured and self-installing.

10.7 Expensive Does Not Necessarily Mean Secure: Gaps in Security at Large Companies

Large companies have generally spent significant sums on their protection and therefore frequently consider themselves to be secure. After all, they opted for state-of-the-art technology. But for how long does technology remain state of the art? There is always an even better product out there, and so managers in these corporations spend their time trying to keep up with the latest international security trends. This takes effort and uses up resources.

Another challenge for large companies is that applications have often been written internally and are hosted in their own data center. These applications have always been called up in the company's internal network – because up to now the Internet has only been used for research purposes.

Back at the beginning of this century, security policies focused primarily on safeguarding the transition points from the corporate network to the Internet. Today, this situation is completely different. The Internet has gained immense importance and any number of business applications are available for use in the public cloud. A few of the many examples are the Telekom Cloud, Open Telekom Cloud, MS Office 365, Salesforce, and the Cisco InterCloud. Were companies to host such applications in their own data centers, a variety of measures would be needed – for secure access alone, a corporate security hub would have to be installed between the application and the workforce, for example. The security hub is a security solution that protects mobile devices from attacks and malicious code from the Internet; for this, all data traffic is analyzed in real time. Since large numbers of employees tend to access such applications, the hub must ensure appropriate bandwidth. Encryption of communication also requires a substantial investment and use of resources. Then there is mobile device management, mobile application management, and mobile content management.

Alternatively, companies can simply procure business applications that have been specially developed for their needs as services from the Internet. Users are given direct access to the applications. However, a smart security element from the cloud is installed in between, making the functions of a security hub available for bigger and more diverse user bases and for larger, more complex applications in big firms. This also lays the foundations for more sophisticated security projects.

10.8 The "Made in Germany" Stamp of Quality

It is clear that in the age of the digital transformation the cloud and security are inextricably linked. For a long time, the cloud had an image problem – not necessarily because it would be easy for hackers to break into, but rather because

many offerings, particularly from the United States, are not immune to industrial espionage. This was found by the study entitled "IT-Sicherheit und Datenschutz 2016" presented by Germany's National Initiative for Information and Internet Security (NIFIS) (see NIFIS 2016) in the run-up to CeBIT 2016: "The study revealed that 87 percent of companies in Germany attach the greatest importance to their data not being stored on the servers of companies with parents or subsidiaries in the United States, in order to protect against spying. When contracting cloud services, 63 percent prefer to use German or at least European providers only."

Of the companies surveyed for the report entitled "Mobile Content Management in Deutschland 2016" (see IDC 2015), 82 percent stated that the location of the data center of a cloud provider in Germany had become extremely important to them. Both SMEs and large companies rely on providers that operate highly secure cloud data centers in Germany – and only store the data in Germany and in accordance with German legal requirements. It is generally known that Germany is the best place to protect data against unauthorized access due to the country's strict data protection regulations. Encryption of data is also allowed in Germany in contrast to many other countries.

Under data protection law, there are other essential requirements for highly secure data centers. For example, data centers should always have a redundant design so that the data is invariably stored in parallel – even in the event of a failure uninterrupted access to the data is provided on the twin. In addition, the goal should be the highest possible availability of 99.999 percent – the maximum achievable by today's technical means, which corresponds to around five minutes of downtime per year. All data in the data center flows through secured IP VPN tunnels, isolated from the public networks. This creates a closed system, fully guarded against external access. Ultra-modern encryption techniques ensure that data can be viewed by authorized parties only.

10.9 Companies Want the Cloud – But Securely

Cloud offerings furnish solutions to pressing problems of companies wishing to run their applications at minimal cost but also securely. Outsourcing spares them a lot of effort. In-house developments are expensive and lengthy, and they must also be scalable. Large international providers relieve companies of this burden. They give users access to the applications in the cloud and keep these up to date at all times. They also make investments in software and hardware unnecessary. This is a marked difference to the situation in the past, when administrators had to install the latest version of a software package locally on the employees' PCs, often using stacks of CDs.

The cloud makes life so much easier and flexible for IT departments, which is why it can no longer be halted. However, companies must be assured that their data will not spread there. The big challenge is to keep unauthorized parties from seeing this data. This is not just about secure transport routes, but also about access

permissions, additional encryption of the data inside the cloud and other mechanisms to make unauthorized access as difficult as possible.

Companies are well advised to investigate a potential cloud provider thoroughly before signing a contract. Under what legislation does the provider operate? Is the potential partner company a German one? Healthcare organizations, for example, are not allowed to store their data outside national borders. Users must therefore take a close look at the provider and ask themselves what is particularly important with regard to the handling of the data (generally this is data protection). Last but not least, customers – especially small and medium-sized enterprises – should make sure that the security can be procured as quickly and easily as if it were plug-and-play security – without interrupting business processes and workflows, yet always unobtrusively in the background. After all, the risks and threats are invariably at the cutting edge of today's technology. Company managers would be wise to keep abreast of the risks at the same speed.

References

A.T. Kearney (2015). *Information security: It's all about trust*. Accessed April 20, 2016, from https://www.atkearney.de/pressemitteilung/-/asset_publisher/00OIL7Jc67KL/content/a-t-kearney-cyberangriffe-werden-in-zukunft-haufiger-und-folgenschwerer?_101_INSTANCE_00OIL7Jc67KL_redirect=%2Fnews-media

Bitkom (2015a). *Die größten Gefahren im Internet*. Accessed April 11, 2016, from https://www.bitkom.org/Presse/Pressegrafik/2015/Maerz/150327-Zehn-groesste-gefahren-Internet/150327-Gefahren-im-Internet.jpg

Bitkom (2015b). *Digitale Angriffe auf jedes zweite Unternehmen*. Accessed April 20, 2016, from https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html

Bitkom, & KPMG (2015). *Cloud-Monitor 2015*. Accessed March 22, 2016, from https://www.bitkom.org/Publikationen/2015/Studien/Cloud-Monitor-2015/Cloud-Monitor-2015-KPMG-Bitkom-Research.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2011). *Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen*. Accessed April 11, 2016, from https://www.bsi.bund.de/DE/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.html

Bundesdruckerei (2015). *Was ist eine digitale Identität?* Accessed August 19, 2016, from https://www.bundesdruckerei.de/id-kompass/content/was-ist-eine-digitale-identitaet

Experton Group (2015). *Cloud vendor benchmark*. Accessed March 22, 2016, from http://www.experton-group.de/research/studien/cloud-vendor-benchmark-2015/ergebnisse.html

FireEye (2016). *Annual threat report*. Accessed April 11, 2016, from https://www.fireeye.com/current-threats/annual-threat-report.html

Heise.de (2016). *Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde*. Accessed April 14, 2016, from http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html

IDC (2013). *IDC-Studie: Halboffene Scheunentore – Viele Unternehmen in Deutschland zu sorglos bei IT-Security*. Accessed Aug 19, 2016, from http://idc.de/de/ueber-idc/press-center/56521-idc-studie-halboffene-scheunentorse-viele-unternehmen-in-deutschland-zu-sorglos-bei-it-security

IDC (2015). *Mobile content management in Deutschland 2016*. Accessed March 22, 2016, from http://idc.de/de/research/multi-client-projekte/mobile-content-management-in-deutschland-2016/mobile-content-management-in-deutschland-2016-projektergebnisse

Kückelhaus, M. (2015). *Das Unvernetzte vernetzen – das Internet der Dinge in der Logistik*. Accessed August 19, 2016, from https://www.delivering-tomorrow.com/connecting-the-unconnected-the-internet-of-things-in-logistics/

NIFIS (2015). M2M: *Experten warnen vor erheblichen Sicherheitsproblemen im Mittelstand*. Accessed August 19, 2016, from http://www.nifis.de/veroeffentlichungen/news/datum/2015/07/14/m2m-experten-warnen-vor-erheblichen-sicherheitsproblemen-im-mittelstand/

NIFIS (2016). *National initiative for information and internet security*. Accessed April 11, 2016, from http://www.nifis.de/

Roland Berger (2015). *Cyber-security – managing threat scenarios in manufacturing companies*. Accessed April 20, 2016, from http://www.internetworld.de/technik/cybercrime/cyberattacken-verursachen-milliardenschaeden-909741.html

T-Online (2016). Lösegeld-Trojaner – Geiselnehmer haben das Internet entdeckt. Accessed August 04, 2016, from http://www.t-online.de/computer/sicherheit/id_77197720/trojaner-locky-und-co-das-macht-ransomware-so-erfolgreich.html

techconsult (2015). *Security-Bilanz Deutschland*. Accessed April 11, 2016, from http://www.techconsult.de/studien/mobile-security-verursacht-grosse-probleme

Webtrekk (2016). Press release "Webtrekk Quartalsstatistik 2015 Q4: 49 % nutzen Tablets oder Smartphones für Online-Shopping." Accessed March 22, 2016, from https://www.webtrekk.com/fileadmin/PDFs/Press_releases_News/2016/DE/20160115_Webtrekk_DI_Statistik_Q4_2015_DE.pdf

Dirk Backofen has been Program Manager Portfolio Management, Engineering and Operations at Telekom Security since April 2016. In this role, he is responsible for the development of new security products as well as Magenta Security Portfolio Management at T-Systems International GmbH – a position that also involves the provisioning of products and solutions in line with T-Systems' Zero Impact strategy.

Backofen began his career with Deutsche Telekom in engineering in 1991. From 1995 onwards, he held a number of management positions in marketing at Deutsche Telekom. As Senior Vice President Portfolio Management, Presales and Marketing at Telekom Deutschland GmbH, Backofen was most recently involved in portfolio management for fixed-line, cellular and IT/cloud products for business customers. Dirk Backofen holds a degree in information technology, and is an alumni of Chemnitz University of Technology.

Cybersecurity - What's Next?

11

Thomas Tschersich

Companies hoping to successfully use the IT security technologies of the future need to rethink their strategy and shift their focus from a latent arms race aimed at protection against the outside world to detection within the enterprise. After all, every company needs to remember that an attacker will infiltrate its network sooner or later, as many recent examples have shown. The next step is to identify the attack as quickly as possible and remove the threat. In the future, smart data and artificial intelligence will be needed to provide this protection within organizations. Authorized users must be distinguished from attackers rapidly with easy-to-use or automated tools such as behavior-based analysis systems. Zero impact must be the goal. Yet, to understand how to get their company or any company to this point, executives always need to keep in mind how the current situation evolved.

11.1 The Motives of Attackers Are Becoming More Malicious with Each Passing Generation

From private users to companies to governmental organizations or NGOs, the range of potential data thieves is as diverse as the profiles of the participants in global data traffic. Quite a few of today's victims will be the attackers of tomorrow – although unknowingly in many cases. In spite of all the complexity, one thing has always been certain: Nobody enjoys absolute protection against anybody on the other side of the fence. This is something that US security firm HBGary Federal experienced for itself.

Its CEO Aaron Barr had stated very publicly in an interview in the Financial Times that he had infiltrated Anonymous in a month-long campaign and could now

T. Tschersich (✉)
Deutsche Telekom AG, Friedrich-Ebert-Allee 140, 53113 Bonn, Germany
e-mail: thomas.tschersich@telekom.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_11

identify all leading members of this group of activists for the FBI (see Menn 2011). Less than 24 hours later, Anonymous retaliated with the theft of 60,000 emails by HBGary's management, disclosing a thorough list of the company's appalling gaps in security. In addition to technical vulnerabilities, these included simple behavioral errors – for example, even the top brass at HBGary such as CEO Aaron Barr and his Chief Operations Officer always used the same, very simple passwords not only for their private email, Twitter, and LinkedIn accounts, but also for the company's key systems (see Schmidt 2011).

Up until about fifteen years ago, when cybercrime or, more precisely, IT security was still in its infancy, hackers were motivated by fame and glory, along the lines of "Look what I can do!" or "Look what I found!" Back then, hacking was not yet about online crime per se, though the foundations for this had been laid. It is only in the last decade or so that we have seen this adaptation of cybercriminal behavioral patterns by, in many cases, organized groups or hacker collectives who are in it for the money on a massive scale. In other words: There has been a commercialization of cybercrime. Phishing emails, DDoS attacks on online shops or the dissemination of SPAM suddenly became the tools of choice in "areas of business" such as fraud, extortion or money laundering.

In the third wave, about five years ago, came the hacktivists, who for politically motivated reasons turned into cyberattackers. DDoS attacks against banks that had blocked the accounts of the whistleblowing platform Wikileaks and attacks paralyzing companies' data traffic in the form of "digital sit-ins" are some of the instruments they use to spread their social, economic or broadly political messages.

Recently, attention has been drawn in particular to state actors, not least as a result of the Snowden leaks. While intelligence agencies have also moved around in cyberspace from year one, in terms of public awareness one can definitely consider the youngest "generation" of cybercriminals to be those who scour the Internet in search of potential targets for acts of sabotage or for the procurement of information under orders from the state or for the purpose of industrial espionage. "Stuxnet" (see New York Times 2016) and "Red October" (see Kaspersky Lab 2013) are just two examples of attacks – allegedly by intelligence agencies or state-controlled organizations – that made headlines around the world.

Admittedly, none of the types of crime and attacks described above are new. But in their order of appearance corresponding peaks have formed. In short, the following assertions can be made:

- The motives and characters of the attackers have changed.
- The attacks are leading to higher and higher financial losses at companies each year. According to security experts, these may currently be as much as 575 billion US dollars and are therefore causing more damage than global drug-related crime (see Bauer 2014).
- The methods and tools used by all groups of perpetrators have remained very similar.
- Yet the resources and the effort in the background differ substantially.

The last point was clearly illustrated by thefts of data such as in the case of Wikileaks or, more recently, the Panama Papers, as compared with attacks like Stuxnet. While in one case it was employees with administrator rights who facilitated the data leak, in other cases attacks use special software that has been developed for this purpose over many years. It is all a question of opportunity, specifically of funding. Using the example of state agencies, there is the telling fact that (according to Wikileaks) the budgets of the five US secret services – CIA, NSA, and Co. – were 45.2 billion US dollars for 2013 alone (see Zeit online 2013). It is a sum that significantly exceeds the annual revenue of quite a few German blue chip companies.

Just how much funding is available to all cyberattackers worldwide does not bear thinking about. The following fact also shows the clear disparities between the concerns of potential attackers and those of their possible victims: A company like Deutsche Telekom must protect over 3,000 proprietary systems directly connected to the Internet in Germany alone, whereas a hacker needs to crack only one of these systems to be successful.

The attacks will become more radical. In the beginning, most attacks were intrusive, with the unwelcome perpetrators simply being satisfied with penetrating the company's line of defense. However, ever since the start of this decade attacks have become increasingly disruptive, compromising the availability of the systems attacked and generally interrupting, blocking or sabotaging their traffic. Digital extortion combined with a ransom demand is the objective of many of these attacks. Attack scenarios in the future, however, will increasingly target the integrity of the data. In other words: While up to now groups of attackers always sought to exploit data in its present form or to impede its availability or communication, the attacks of the future – which scarcely feature today – will be aimed at modifying the data. This will completely transform the risk landscape.

Interference with road traffic is just one example. Remote attacks on cars, their braking performance, sudden failure of wipers or the lighting system – not to mention self-driving cars – could have fatal consequences. The same goes for the manipulation of data in the healthcare system, where, for example, a patient's blood group could be changed in the course of the transfer of the patient's data shortly before an operation. It is very easy to imagine the potential consequences of malpractice during attacks on several hospitals in the German federal state of North Rhine-Westphalia at the beginning of 2016. The worst were only averted because the perpetrators were solely interested in a ransom. As the State Office of Criminal Investigations reported, physicians were unable to continue treating their patients due to data not being available (see Polizei/Landeskriminalamt Nordrhein-Westfalen 2016).

Security homework – or the worst mistakes made by companies. One of the first and most important things that companies need to change is their defense policy, followed by their ecosystem. The next step is to consider everything that needs to be protected in the future. The vast majority of companies protect PCs and servers, and most users also have virus protection, at least for their PCs. The first gaps in security appear when it comes to installing software updates, because this is

seen as overly complicated and time-consuming. Although operating systems may actually be updated regularly and promptly, companies often fail to update application software, which may have equally critical security issues. What is more, the update cycles at companies are frequently far too slow. This enables attackers to exploit new gaps on a massive scale just hours after they become known, as companies frequently only implement manufacturers' updates weeks or months after their release. Not to mention that there is also a whole series of other IT systems such as cell phones, system controls, etc., most of which are still left out of the equation entirely. Such carelessness, once discovered by cybercriminals, is almost an invitation for attackers and makes one thing clear: Security and laissez-faire are two irreconcilable worlds.

The fact that this understanding has still not become entrenched in people's minds is one of the main reasons why – in 84 percent of the cases investigated in a study last year by the US telecommunications group Verizon – it took attackers only a few hours to prepare an attack and subsequently reach the actual target system. By contrast, in 62 percent of the cases the attacks were not identified by the companies themselves until months later (see Verizon 2016).

Significantly larger gaps in corporate security will be caused in the future due to the fact that we still regard the smartphone as a telephone rather than a computer. In this connection, people still completely underestimate how quickly smartphones can be turned into remote-controlled cyberweapons to be misused as a listening device, to access photos and videos or to serve as a Bluetooth interface to the user's peripheral application systems.

Cell phones are an even more attractive target for hackers who harness these devices for botnets, for instance, in order to launch automated attacks against third parties from a network of externally controlled devices or computers. Botnets are used for distributed denial of service (DDoS) attacks against websites or other services, for example. Ultimately, hackers can thus paralyze any e-commerce platform with just ten captured smartphones. One of the methods used for this is the NTP reflection attack (see Akamai Technologies 2015), in which the Network Time Protocol standard used to synchronize the time of computer systems is abused to prompt one server to attack other servers in the Internet with NTP packages (see NTP 2016).

What do attackers need to carry out such attacks? – High bandwidth and a low level of protection. Very few smartphones these days have security software, but they have far superior bandwidth to most PCs. What also plays into the hands of criminals is open architectures such as in Google's Android operating system. Owing to the Americans' business model of monetarizing user behavior and user data in advertising, for which a lot of content is generated from any number of sources, Android, the smartphone operating system with a market share of over 80 percent, is becoming an open invitation to any criminal. It took around 14 years for 450,000 malware versions to be identified in the Windows operating system, but not even 10 months for this to happen in Android.

Companies that give their employees iPhones for work purposes should not feel any safer. Even though Apple's operating system is more homogeneous and its

architecture affords better protection because the business model works differently from Google's, it is not perfect either. One of the reasons for this is the ever-popular practice of jail breaking, which involves removing the restrictions imposed by a cell phone manufacturer – in this case Apple – in order to download software to an iOS phone from alternative marketplaces instead of using the Apple Store.

Tests we performed showed that a jailbroken iPhone connected to the Internet suffered around 300,000 automated attacks in one year. About 330 of these attacks were so successful that the attackers were able to move around freely in the system of the phone we had designed as a honeypot. But especially in the areas of jailbreaking and rooting, not everything is black or white: By obtaining elevated privileges to their device, experienced users can also raise their level of security – if they know what they are doing. In addition, there is a lively CustomRom scene that also develops operating systems with the latest security updates for many of the popular models.

Yet even iPhones that have not been jailbroken are not immune to being hacked. In an analysis of Operation Pawn Storm, which has been running worldwide for four years now (see Trend Micro 2014), Security company Trend Micro (see Trend Micro 2015) discovered a tool that was specially designed for iOS phones (see iPhone Ticker 2015). This extensive malware campaign is directed at companies as well as at the political organizations and the military in different countries. The target persons are never attacked directly. Instead, the hackers attempt to initially infect the communication devices of other people from their target's personal or business environments, obviously based on the idea that a subsequent attack or the transmission of malicious software via news or emails from trusted sources has significantly greater chances of success. That is why this approach is called "pawn storm" after the chess strategy.

Cheap smartphones, put on the market by the manufacturer at a particularly reasonable price but not receiving any further security updates, constitute a fundamental problem, not just for companies. Here, what is needed is a policy that requires all manufacturers to ensure security updates throughout a phone's life, which generally lasts at least two years.

In the future, gaps in our defense will also show that we underestimate the growing risk of increased networking. Be it air-conditioning systems and elevators in companies or household appliances such as fridges, televisions etc., many of the devices that can be networked today were not originally designed for this purpose at all. In most cases, the software is installed in these devices during production; interaction with the user – e.g., for update installation – is not envisaged or not possible. Consequently, protection for these devices must come from the network. Going forward, security solutions that are incorporated into network infrastructures will therefore have even greater significance than today.

The traditional perimeter approach adopted by companies of building their castle walls increasingly higher, wider and thicker led to companies continuously investing in security. Ultimately, though, they were only ever able to maintain the status quo and therefore hardly able to achieve their goal of increasing the level of protection. Instead of being forced to spend money on repairing damage, they

should free up resources whose investment actually improves their own security. But how does this square with the growing need for security from the network? As easy as it may sound, the first step is finally to do our old, but perennial homework and to continue to do this without fail.

11.2 Cybersecurity – The Sleeping Giant in the Company

A successful defense against cybercrime is based on three pillars: prevention, detection, reaction. I would go so far as to say that at least 95 percent of the millions upon millions of cyberattacks that are carried out around the world each day would come to nothing if companies took the basic rules of prevention to heart. The fact that end users and unfortunately also companies (because they dread the effort involved in testing) do not implement software updates as quickly as possible and, after putting them off several times, eventually end up letting things slide is by far the greatest vulnerability.

In addition, most of the attacks that exploit the gap created by missing software updates follow a set pattern: The fundamental principle of the protection concepts in the company is based on the fact that there is an internal (trusted) infrastructure and an (untrusted) outside world. Broadly speaking, these worlds are separated using firewalls. The principle governing these firewalls is simple: Everything coming from outside is "bad" by definition and is blocked, whereas everything that comes from within the company is good and is allowed to happen. This is where attackers begin. Using social engineering, the environment of potential addressees is spied out using enticing emails which successfully function as bait – if not on the first or second attempt, then on the third or fourth attempt – essentially by awakening the recipient's interest so that they read the email and open the attachment that is generally enclosed. This may be a PDF that looks completely normal but immediately executes malicious software in the background, downloading a Trojan from the network and installing it automatically.

Unfortunately, neither of these steps raises any suspicions for conventional firewalls. This is because emails per se are treated as a communication channel that is always kept open to the outside world. Moreover, a Trojan is downloaded by means of an action that is initiated by the computer from the inside and is therefore classified as "okay" by the firewall, as would be expected from it. Having penetrated the castle walls in this way, every attacker has free access to the system. Getting from the attacked computer to the file server, where data is spied out, exfiltrated, and the attacker's tracks are obliterated, is a process that in some cases takes no more than a few minutes. With one fatal consequence: While the firewall as the "castle wall" continues to defend the perimeter, the attacker is now in the house and can move around freely.

APT detection solutions provide help here. APT stands for Advanced Persistent Threat, effectively a permanent individual vulnerability. Solutions like Fire Eye, which review the behavior of all incoming emails and any attachments enclosed, provide protection. If the behavior of the emails being examined is inconspicuous,

these are effectively waved through after being checked in a virtual machine. However, if the file being examined suddenly starts to develop unexpected activities such as wanting to install software updates or change the operating system or the configuration, Fire Eye assumes that this file has been manipulated by malicious functionality and blocks it. The entire check is performed in milliseconds without causing a perceptible delay in email traffic for the owner of the mailbox. In terms of functionality, the safeguards that will be needed in the networks in the future are vastly different from the long-established "castle walls." Future security models will be based on the behavior of software rather than on the principle of admission control at the wall.

A second new way of protecting company networks is by using sensor technology like in alarm systems. All PCs could also be fitted with sensors, just like every smartphone today – for example to receive GPS signals or capture data on health or environmental data. These sensors can continuously review incoming and outgoing data traffic and attachments, files, etc. for conspicuous behavior, identify anomalies immediately, and report them to a central instance. In many company networks, for example, there is no direct client-to-client communication. If a PC starts contacting another PC directly without going via the email server or group shares, this can only mean one of two things for a security officer who has been alerted by an alarm triggered through corresponding sensors: Either an employee introduced a service and forgot to tell anyone about it, or an attacker is moving sideways in the network from one PC to the next.

Although such sensory solutions for detection purposes are unable to reverse the attack, which may have taken place long before, they can minimize its effects. This is no mere small comfort, because these days no company should assume that it can permanently protect itself against attacks. Today, every security officer's goal must be zero impact, in other words, reducing the repercussions of attacks to zero. To this end, a logical step, which at the same time entails a radical change in IT security overall, is to move away in the future from a purely preventive approach and to equally divide capital expenditure on security between detection and reaction.

Before this happens, however, it can be assumed that the preferred (and simple) method among attackers of exploiting the fact that software updates have not been installed will remain successful for quite some time – simply because users lack the necessary awareness, be it at work or in their own personal environment. This, in my opinion, may be the main reason why cybercriminals always seem to use Formula 1 cars, while the security experts – usually unnecessarily – trail after them in Bobby cars.

In the past, it normally took months to find out which vulnerability was closed by an update and then to develop an exploit (attack tool) for this. Through reverse engineering, which makes the original program code and therefore also the measure implemented for its improvement easier to extract, this now takes the underground economy not even half a day. On average, only a few hours elapse between the supply of a patch for the vulnerability and the large-scale, fully automated use of tools that can exploit an identified vulnerability. For companies and the providers that protect them, this means that the time frame for an appropriate reaction is

relatively minute. Speed is of the essence here. Relying on the virus protection installed on each company PC does not provide adequate assurance, as this only recognizes threats that are already known to it. However, when criminals use an exploit for the first time – or possibly once only – the chances of this being detected are virtually zero. This is because virus protection works along the same lines as a police fingerprint file. If a method, a line of attack or a perpetrator has already appeared, the virus protection will be able to identify it. Otherwise, there is not a chance. This means that malicious software of which the antivirus industry is not yet aware may "work" for months before being exposed. When the update is installed at some stage and sounds the alarm – "malicious software on this computer" – it is often far too late.

This makes it very important for companies to be able to keep track of how long malicious software was actually active. It may require a great deal of time and effort to eliminate all of the damage because attackers naturally know that their "break-in" through the front door – via email access – will be discovered sooner or later and be blocked by the software update. This is why they generally use the time to set up their own back entrances and exits. Identifying these is extremely time-consuming and nearly impossible in some cases. In the attack on the German Bundestag, in which hackers gained access to 14 parliament servers in May 2015 (see Zeit online 2016), the computer system had to be set up again from scratch (see Holland 2015). In cases of doubt, this is actually the last remaining useful measure to at least bring the traditional hare-and-tortoise game between attackers and victims back to the starting line.

Unfortunately, in the reality of business every update is considered a brake, true to the motto "never touch a running system." The real message should be that people who do not install software updates promptly only have themselves to blame. To put it plainly: it is a worthwhile investment. This is because simple updates are the key to foiling virtually all attacks with the exception of zero-day exploits.

11.3 What Will Protect Us?

The first step is to create a much better awareness of threats. In many companies these days, investment decisions about IT security are made by managers who throughout their career – apart from using their PC – have had nothing whatsoever to do with IT, never mind IT security. IT security is normally studied as part of a computer science degree – but is actually an interdisciplinary topic spanning all sectors, i.e., all courses of study. A mechanical engineering contractor who installs remote maintenance modules in his equipment is taking a quantum leap in terms of servicing. This is called predictive maintenance. The only thing he is generally unable to guess is how the module will function and what scope for attack his equipment will provide at any given time.

However, as IT security is an issue that affects everybody, from the janitor up to the CEO, and as everyone will be a link in the security system of their future

employer, this subject should already be firmly anchored in school curricula. It not only hones people's security awareness, but also trains them to keep in mind at all times that every hacked PC is a potential cyberweapon against third parties. Continuously sharpening this awareness, also in employees' personal spheres, will need to become an important part of companies' defense strategy. The effects will be twofold: Companies will reduce the possible scope for attack against themselves and will increase the motivation of employees to address this issue – even more so when those employees see there is something to be gained in their private IT lives, too.

When it comes to concrete solutions, a whole series of solutions can be identified. Encryption will be the technology of choice in the future for protecting the integrity of data. It effectively provides secure transportation for the data. It would never occur to the central bank to transport pallets with gold bars or the latest generation of freshly printed 20 euro bills on flatbed trucks on the public highway. However, this is precisely what we do in the digital world. What applies to virtually all security applications also applies here. When their use is to be mandatory – keyword "user acceptance" – defense and protection solutions such as encryption must fulfill three requirements: easy to procure, easy to implement and easy to use – ideally even running automatically.

In order to provide optimum protection for the email gateway, as mentioned before, behavioral analyses in the network or in virtual machines are particularly suitable for advanced persistent threats (APTs) that use malware, possibly individually tailored for just one person. Whether in large corporations, SMEs or start-ups – cutting-edge technologies as potential prey make it worthwhile for criminals to invest a great deal of time and effort in developing tools, even though these might only be used once for one specific purpose.

In the future, sensor technology in the network will also be essential for detecting and remedying conspicuous client-to-client communication, for instance, as quickly as possible through behavioral analyses. Cybersecurity sensors like honeypots will take on greater importance, not only at strategic points in the company network but in all devices (smartphones), computers, and equipment. This is because nobody is capable of analyzing over 400,000 new variants of malware every day, as now registered worldwide by the antivirus industry. For this reason, behavior-based detection will play a key role in the future for initiating fully-automated defense mechanisms. If sensors are to be extensively employed, however, the hardware industry has a particular responsibility to make the first move. "One sensor for each PC" must be the standard in the future.

Rethinking a company's own security practice must also involve systematically keeping critical and uncritical applications apart and fitting each component with sensors and safeguards. The exchange of data between systems should always be authenticated in every case.

A future trend will be that security is set to become a component of the data itself rather than of the infrastructure that transports and processes the data. Digital rights management (DRM) technologies are one example, ensuring that data cannot be viewed or modified during transfer and could thus also be given a kind of digital

best-before date. Data or documents themselves will then contain information as to who is authorized to access and modify them. This will progressively reduce the importance of the infrastructure in guaranteeing security. At least in terms of approach, the photo service Snapchat provides an example of an alternative, deleting a photo once it has been viewed by the recipient. This is a useful feature – and not only for potentially embarrassing selfies.

In addition to all of the new technical possibilities, it is also important to keep the castle walls high, at least to ward off intruders, but to no longer exclusively rely on them for protection.

Otherwise, I believe that two ideas are especially important. Firstly, keeping silent about having fallen victim to a cyberattack should be a thing of the past for companies. Let's rather view it as joining the club. The list of companies already in the club is effectively a Who's Who of international industry. And who believes that any company is unassailable?

This idea leads on to the next one: Why shouldn't potential victims of cybercrime not join forces just like the attackers do? After all, I believe that security is for sharing. Sharing at many different levels, from the Cyber Security Sharing and Analytics (CSSA) platform, on which the largest German blue chips already share their experience and information about new methods and types of attack with one another (see CSSA 2016), to the operations of the cyberdefence centers of major providers. Once these have initially identified the attack and the underlying tool at just one of their customers, the security solution implemented for defense purposes is automatically transferred to all of the other customers. This form of digital neighborhood watch will allow us to implement better defense strategies more easily overall.

One aspect that in my experience tends to be neglected by companies in nearly all security discussions at C-level is the nonetheless obvious consideration of where administrators stand in the company hierarchy and salary structure. This is because the objective of all attacks is to gain administrative rights – giving any attacker "carte blanche." Companies may be making a strategic mistake in keeping the employees with the highest authorization level ("they are allowed to do more than any CEO") and who know every IT secret – in other words, the "Access Almighty" – at the lowest level of the hierarchy in some cases. Here, I would urgently advise checking to what extent it is recommendable for such employees to be promoted in line with their level of responsibility and the value they add for the company. This might keep the scope for attack that vital bit lower.

Urgent need for action – Yet even the supposed all-inclusive package still has gaps when it comes to providing security for the future. Security officers claim to have rightly complained: "If everything were encrypted, it would be impossible to identify malware in the network." Unfortunately, though this is true, who says it will always be the case? Developing technologies that overcome this obstacle should be a future research assignment for IT chairs the world over.

11.4 Conclusion

From my point of view, companies are well advised to stay with what has been proven to work (and also implement it properly), but to implement many new measures and solutions at the same time. In companies' protection concepts, internal sensor technology – the installation of sensors in practically all hardware used – is only in its infancy. However, this technology is necessary to ensure that future security models work and new job norms such as "bring your own device" do not turn into "bring your own disaster."

Where appropriate, small and medium-sized enterprises (SMEs) and other companies should replace their own in-house security operations center with external cyberdefense centers that work with broader analytical capabilities, forensics, hunter teams and anomaly recognition on the basis of sensors and logic; with the objective of deriving preventive solutions and defense mechanisms from these and initiating them immediately.

Companies should seriously consider the benefit of the swarm intelligence amassed by a service provider who protects many systems, has the specialists for this, and averts threats that arise at a given point for everyone in an automated manner. Companies that are not there yet should at least use the knowledge available in their own community – that of the potential victims. This is because, despite all competitive thinking, companies will always remain a community. And, last but not least – patch, patch, patch.

References

Akamai Technologies (2015). *Reflection-Techniken für DDoS-Angriffe*. Accessed May 18, 2016, from http://www.itseccity.de/virenwarnung/statistiken/akamai110215.html

Bauer, H.-P. (2014). Mehr Schaden durch Cyberkriminalität als durch Drogenhandel. Interview in Manager Magazin. Accessed May 18, 2016, from http://www.manager-magazin.de/unternehmen/it/enormes-wachstum-cyberkriminalitaet-ueberholt-drogenhandel-a-976184.html

CSSA (2016). Website. Accessed May 18, 2016, from http://www.cssa.de/

Holland, M. (2015). *Nach Bundestag-Hack: Parlament bekommt neue IT-Sicherheitsstruktur*. Accessed May 18, 2016, from http://www.heise.de/newsticker/meldung/Nach-Bundestags-Hack-Parlament-bekommt-neue-IT-Sicherheitsstruktur-2810587.html

iPhone Ticker (2015). *Operation Pawn Storm: Malware zielt auf iOS-Geräte ohne Jailbreak*. Accessed May 18, 2016, from http://www.iphone-ticker.de/operation-pawn-storm-malware-zielt-auf-ios-geraete-ohne-jailbreak-77204/

Kaspersky Lab (2013). Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage campaign targeting diplomatic and government institutions worldwide. Accessed May 18, 2016, from http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide

Menn, J. (2011). *Cyberactivists warned of arrest*. Accessed May 18, 2016, from http://www.ft.com/intl/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html#axzz490kpLOzQ

New York Times (2016). *Cyberattacks on Iran – Stuxnet and Flame*. Accessed May 18, 2016, from http://www.nytimes.com/topic/subject/cyberattacks-on-iran-stuxnet-and-flame

NTP (2016). *Website des Network Time Protocol Projekts*. Accessed May 18, 2016, from http://www.ntp.org/

Polizei/Landeskriminalamt Nordrhein-Westfalen (2016). *Cybercrime-Angriffe auf Infrastrukturen von Krankenhäusern, Behörden, Unternehmen*. Accessed May 18, 2016, from https://www.polizei.nrw.de/lka/artikel__13193.html

Schmidt, J. (2011). *Ausgelacht*. Anonymous kompromittiert US-Sicherheitsfirma. Accessed May 18, 2016, from http://www.heise.de/ct/artikel/Ausgelacht-1195082.html

Trend Micro (2014). Pawn Storm Espionage Attacks Use Decoys, Deliver SEDNIT. Accessed May 18, 2016, from http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/pawn-storm-espionage-attacks-use-decoys-deliver-sednit

Trend Micro (2015). *Pawn Storm Update: iOS Espionage App Found*. Accessed May 18, 2016, from http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/

Verizon (2016). *Cybersecurity's most comprehensive investigations report*. Accessed May 18, 2016 from http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Zeit online (2013). *Geheimes Budget von US-Nachrichtendiensten veröffentlicht*. Accessed May 18, 2016, from http://www.zeit.de/digital/datenschutz/2013-08/geheimdienste-haushalt-snowden-nsa-cia

Zeit online (2016). *Hackerangriff wurde aus Russland gesteuert*. Accessed May 18, 2016, from http://www.zeit.de/digital/2016-01/hackerangriff-bundestag-russland-nachrichtendienst-bundesanwaltschaft

Thomas Tschersich As Senior Vice President Group Security Service at Deutsche Telekom AG, Thomas Tschersich is responsible both for cybersecurity and all other operational security topics in the Group. Since April 2016, he has also led the Internal Security and Cyber Defense team for the future Telekom Security unit. In this position, he directs high-level services for the new unit and is responsible for strengthening internal hazard control and managing the external launch of the Telekom's cyberdefense portfolio. With Telekom Security, Deutsche Telekom is bringing together security teams from across the group.

Since joining Deutsche Telekom, Tschersich has established a Group-wide security team and held a number of roles, including Senior IT Security and Information Security Officer at Group HQ, as well as managing the Security Strategy and Policy unit in the core Group Security division and the Technical Security Services unit within Group Business Security. In February 2009, Tschersich was appointed Senior Vice President Group IT Security – the cybersecurity unit within Deutsche Telekom. In this role, he has Group-wide responsibility for the security of production and IT infrastructure. Alongside his work at Deutsche Telekom, Tschersich also sits on numerous committees as an advisor to the German Federal Government and the European Parliament.

Conclusion

12

Ferri Abolhassan

12.1 The Internet Has Become Ubiquitous

Within a few short years, the Internet has fundamentally changed the way we live, work and perceive our surroundings. According to the German digital association Bitkom, using the Internet is now more or less a daily routine for most Europeans: "Three out of four EU citizens between the ages of 16 and 74 (76 percent) go online at least once a week" (Bitkom 2016). In Germany, the average is actually 84 percent. The Internet has thus become part of our everyday lives. We surf, chat and play there. We book trips, buy insurance and transfer money. Digitalization has taken hold wherever apps have made services faster, easier and cheaper than conventional offerings.

The advantages of digitalization are even more tangible and extensive in the business world. The Internet of Things alone is revolutionizing entire business models and processes. "Faster, more efficient and more flexible," is the motto when it comes to accessing real-time maintenance data from machines, for example, or logistics data from transported goods. Or when big, traditional, global banks work together with alternative payment providers such as PayPal or new financial services companies – the dynamic "fintechs" – in order to jointly develop offers for bank customers. One thing is certain: Digitalization has led to exponential growth in the volume of data, and thus in the lures of abusing this data – either by hackers and their ilk, or by intelligence services who disregard the right to informational self-determination and preservation of the private sphere.

F. Abolhassan (✉)
Telekom Deutschland GmbH, Bonn, North Rhine-Westphalia, Germany
e-mail: ferri.abolhassan@telekom.de

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6_12

12.2 Good Internet, Bad Internet

John Doe and even corporate employees and executives might like to close their eyes to the hazards of the Internet and ignore the risks inherent in handling digital information every day, but one user group has long been aware of the Internet's value potential: cybercriminals. They have a decisive advantage here. As opposed to crimes in "real life," online crimes are much less dangerous for them. If a theft is discovered at all, it is usually only after some time has passed. And there is no need to fear being apprehended with a loaded gun and thus facing risk to life and limb. As a consequence, the biggest bank robberies these days are digital. For example, the Carbanak gang was able to steal up to one billion US dollars worldwide from around 100 financial institutions in the space of about two years. They committed the biggest online bank heist of all time. And according to the latest information, the criminals have not yet been stopped (see Computerwelt 2016).

After seeing attacks such as these covered by the media, every last user and IT officer must now be aware of one thing: Data is exposed to very high risks online. For this reason, extensive protective measures must be taken to ensure its safety. And yet, most users still do little or nothing. Why is that? For the majority, especially private consumers, security measures seem too expensive and complicated. "Things have been fine so far," they think. So why bother with the latest encryption solution, firewall or a new password? What's even more concerning is that the situation is not much better in industry. Many companies are not sufficiently protected against attacks by cybercriminals. And in companies, too, people are often the weak points. What good is the best firewall if a user reveals personal login data over the phone to someone claiming to be from IT support? Or when someone finds a USB stick at a trade fair and tests it on their office computer, just out of curiosity? In the case of social engineering attacks such as these, the only thing that usually helps is a short, sharp shock – that is, confronting users with their mistakes through simulated attacks, combined with subsequent risk training. But very few companies – not to mention private users – have reached this point yet. Urgent action is needed here.

12.3 Cyberhare vs. Cybertortoise

The high speed and dynamics of digitalization suit the schemes of cybercriminals. Digital transformation moves more quickly than people or the society we live in, and it moves much more quickly than legislation. The law appears very antiquated indeed in the face of the quantum leaps made by digitalization in recent years. And legislators have realized that data protection regulations no longer meet current requirements. Thanks to the IT security law that came into force in July 2015, Germany is a pioneer in cybersecurity legislation, with extensive reporting requirements for the operators of critical infrastructures. However, the EU-wide harmonization of regulations demands even more work from everyone involved. Another set of rules will come into play with the new EU data protection directive,

which is due to take effect in 2018. Here, too, IT officers must keep their fingers on the pulse of development in order to stay abreast of what is required and what is prohibited.

But private Internet users and companies are not the only ones affected. Cyberthreats have long had global political dimensions. We need look no further than the hacker attacks on globally important critical infrastructures, the online recruitment of jihadi fighters, and autonomous weapons systems. Here, too, the barriers to entry for cyberwarriors are much lower than they would be in a traditional battlefield situation. Not just anyone can build an atomic bomb, but anyone can develop a virus or gain access to an insecure password. These possibilities have fundamentally changed the nature of modern conflict. The attack scenarios call for worldwide security alliances, and they are forcing even global organizations to take action. NATO, for instance, recently declared the Internet to be an independent theater of operations, and attacks via data networks are treated in the same way as those by land, sea or air forces. If such virtual attacks were to take place, they could even trigger NATO's collective defense article. The threshold for this has not yet been defined. But there is no doubt that these threats are being taken very seriously.

The German armed forces are also employing more cyberspecialists to protect themselves as well as possible from the continuously growing threat. However, it is not clear where this large number of required cyberexperts will come from because – as if there were not already enough to do in the field of IT security – such experts are in short supply. This affects every industry as well as organizations and companies of every size. But the problems are particularly acute among small and medium-sized enterprises. Though the first security-specific courses at universities are already available, it will take a good deal of time to train a sufficient number of experts in the long run. Additionally, this training is more demanding than other subjects, where the same syllabus can be used for years. Since the threats from cybercriminals evolve so rapidly, security experts must be trained in an equally dynamic way so that they are always up to date.

Security experts and legal regulations are not the only things in short supply. A valid, resilient strategy for dealing with emergencies is also lacking. Very few CEOs or CIOs know how to respond properly to a cyberattack. They would do well to deal with this problem, however, because depending on the legal structure of a company, its management may be held personally responsible if the company's risk management system fails. This in itself gives management the opportunity to hone its responsiveness and cybersecurity strategy. By applying military methods such as red teaming or wargaming to the business world, dangerous real-world situations can be simulated dynamically, so that the interaction of internal teams can be tested without risk. A comprehensive risk management strategy is also critical for large international companies whose global activities mean they must take numerous regulatory and legal IT security requirements into account. The situation is even more difficult if they serve different B2B and B2C customer groups and work with diverse partners and suppliers. The resulting complexity of their IT landscape raises

the potential threat to almost unimaginable levels. Risk management goes a long way toward helping companies maintain an overview in the face of this.

Cooperation with other large corporations is another opportunity available to CEOs and CIOs. Associations such as Cyber Security Sharing and Analytics (CSSA) work closely together so that their members can mutually warn each other of potential attacks ahead of time. And they are extremely successful at it: During the "DDoS for Bitcoins" wave of extortion in 2015, for example, potential damages in the millions were prevented when a company that had been attacked warned its CSSA partners – a week before any notice was published by the BSI, the German Federal Office for Information Security. A week is worth a fortune in the digital age, so the CSSA members were able to protect themselves and ward off subsequent attacks. These and other approaches are models for companies looking for appropriate ways of managing IT security in the future.

12.4 Simple and Secure Is the Motto

The expert essays in this book from the fields of business, politics and society make it clear that there is still much to do, but also that we already have some outstanding strategic approaches and IT solutions that can help users protect themselves against cybercriminals. Users can easily get lost in the multitude of technological options available – from data leakage prevention, through security information and event management, to mobile security and identity and access management. Managed security services delivered in all-inclusive packages such as security-as-a-service or mobile-security-as-a-service can prevent this from happening. This is a central component of IT security strategy. Another component is teamwork, and not only because four eyes see more than two. From in-house security operations centers to expanded, external cyberdefense centers – security will soon come down to extensive analytical expertise combined with forensics, hunter teams and anomaly recognition with the help of sensors and logic, enabling preventative solutions and defensive actions to be triggered.

But we also need much more. For example, the exchange of personal data must be contained so that as little user information as possible is exposed to these risks in the first place. We already have models for this, such as the P3P (Platform for Privacy Preferences) approach, an international standardized platform developed by the WWW Consortium for the exchange of data protection information for websites. The goal of P3P is to return a substantial amount of data sovereignty to Internet users by automatically informing them when third parties want to access their personal data so that they can prevent this. This approach is feasible in other areas as well, such as the Internet of Things. Service providers do not always need all of an individual's personal data; they could often get by with pseudonymized or anonymized information. When dealing with personal data, even apparently minor measures such as these can help ensure that essential information does not fall into the hands of criminals who could abuse it. These tools also show that security does

not always have to be complex; it can actually adapt itself to work and usage processes.

After all, in order to stay safe from future threats as well, it is important to bear one thing in mind: If IT security is going to be broadly used and useful, it has to be even easier to handle, operate and acquire – following the plug-and-play principle of security from a socket. The cloud is the most important foundation for this, because only the cloud offers the necessary resources and flexibility – along with a secure basis for digital transformation via hosting in German data centers, which are comprehensively protected in accordance with national IT security law. The cloud also enables the pioneering of automated solutions in the areas of smart data and machine learning (ML), which will soon make it possible for the security DNA of a company to optimize itself, recognize patterns in real time and evolve through autonomous self-learning.

This long-term strategy for success also depends on factors such as the comprehensive and seamless implementation of security solutions in companies and organizations, proper training of security experts, and measures to make employees aware of the importance of the issue. Finally, users can also benefit from the best practices of other economic sectors, such as the sharing economy, and they can share their own knowledge of how to fight cyberthreats. Together we are stronger. This is particularly true when it comes to IT security – because the attackers are working together, too, and they are often several steps ahead of us. We can not allow this to continue. We have made a start.

References

Bitkom. (2016). *Internet*. Accessed July 5, 2016, from https://www.bitkom.org/Marktdaten/Konsum-Nutzungsverhalten/Factszu-Internet.html

Computerwelt. (2016). *Carbanak: Der Online-Bankraub geht weiter*. Accessed July 4, 2016, from http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/115084-carbanak-der-online-bankraubgeht-weiter/

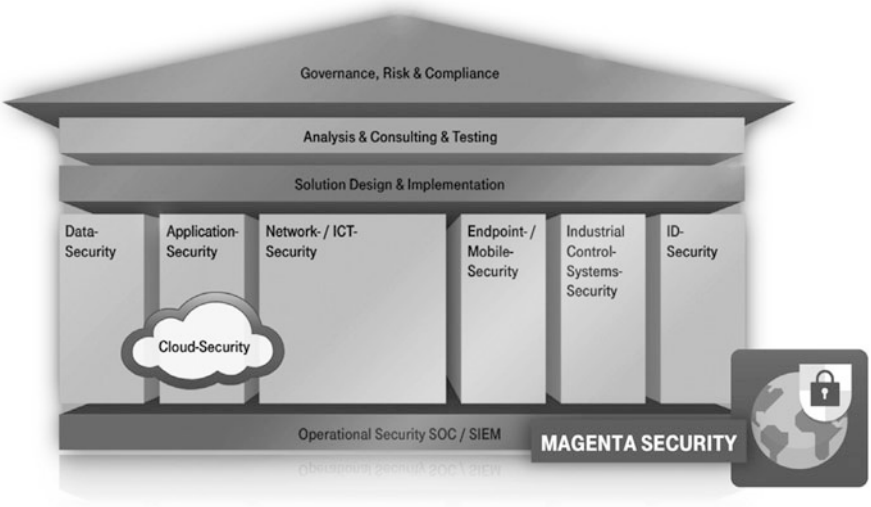
Appendix

Eleven Rules for a Secure Internet of Things (IoT)

1. **Think about security from the start**: Retrofitting is always hard
2. **Know what's connected**: If you are aware of the individual connections between things, you can protect and monitor them better
3. **Don't connect everything just because you can**: Follow the minimization principle – only make connections that are sensible and necessary!
4. **Only allow essential communication**: Networked things will communicate with each other only in predefined cases
5. **Separate critical and non-critical systems**: For example, do not connect industrial controllers directly with office communication networks
6. **Create logical zones**: Make sure to break the whole into parts so that damage is contained in the event of an attack
7. **Conduct pen tests**: When you know where your vulnerabilities are, you can protect yourself in advance
8. **Keep your software up to date**: 95 percent of attacks could be prevented if every system worldwide was patched promptly
9. **Encrypt the connections between things**: Encrypted communication ensures that no information can be picked off along the transmission route
10. **Use certificates to securely identify each thing**: Only authorized individuals can control the devices that are supposed to be controlled
11. **Rely on strong partners**: When in doubt, seek professional help and have a comprehensive protection concept drawn up, like that offered by companies such as Deutsche Telekom

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6

The Magenta Security Portfolio



Technical Literature

Abolhassan, Ferri (Ed.): Security Einfach Machen. IT-Sicherheit als Sprungbrett für die Digitalisierung. Springer Gabler (2016), ISBN 978-3-658-14944-4

Abolhassan, Ferri/Kellermann, Jörn (Eds.): Effizienz durch Automatisierung – Das Zero-Touch-Prinzip im IT-Betrieb, Springer Gabler (2016), ISBN 978-3-658-10643-0, eBook ISBN 978-3-658-10644-7

Abolhassan, Ferri (Ed.): The Drivers of Digital Transformation – Why There's No Way Around the Cloud, Springer Gabler (2016), eBook ISBN 978-3-319-31824-0

Abolhassan, Ferri (Ed.): Was treibt die Digitalisierung? – Warum an der Cloud kein Weg vorbeiführt, Springer Gabler (2015), ISBN 978-3-658-10639-3, eBook ISBN 978-3-658-10640-9

Abolhassan, Ferri (Ed.): Kundenzufriedenheit im IT-Outsourcing – Das Optimum realisieren, Springer Gabler (2014), ISBN 978-3-658-04748-1, eBook ISBN 978-3-658-04749-8

Abolhassan, Ferri (Ed.): The Road to a Modern IT Factory: Industrialization – Automation – Optimization, Springer Gabler (2014), ISBN 978-3-642-40218-0, eBook ISBN 978-3-642-40219-7

Abolhassan, Ferri (Ed.): Der Weg zur modernen IT-Fabrik: Industrialisierung – Automatisierung – Optimierung, Springer Gabler (2013), ISBN 978-3-658-01482-7, eBook ISBN 9783658014834

Abolhassan, Ferri/Scheer, August-Wilhelm/Jost, Wolfram/Kruppke, Helmut (Eds.): Innovation durch Geschäftsprozessmanagement: Jahrbuch Business Process Excellence 2004/2005, Springer (2004), ISBN 978-3540220374; eBook ISBN 9783642171383

Abolhassan, Ferri/Scheer, August-Wilhelm Scheer/Jost, Wolfram/Kirchmer, Mathias (Eds.): Change Management im Unternehmen: Prozessveränderungen erfolgreich managen, Springer (2003), ISBN 978-3-540-03437-7, eBook ISBN 978-3-642-19020-9

Abolhassan, Ferri/Scheer, August-Wilhelm/Bosch, Wolfgang (Eds.): Real-Time Enterprise – Mit beschleunigten Managementprozessen Zeit und Kosten sparen, Springer (2003), ISBN 978-3540023562, eBook ISBN 978-3-642-55458-2

Abolhassan, Ferri/Scheer, August-Wilhelm/Jost, Wolfram/Kirchmer, Mathias (Eds.): Business Process Change Management: ARIS in Practice (english), Springer (2003), ISBN 978-3-540-00243-7

Abolhassan, Ferri/Arend-Fuchs, Christine/Georgi, Hans-Peter/Müller, Peter/Zentes, Joachim: Der Handel im Internet-Zeitalter – Perspektiven für Handel und Konsumgüterindustrie mit mySAP.com, Galileo Press (2001), ISBN 3898421147

Practical Report from the Graduates

Sarah Schuchardt and Alexander Schmitz

> In each beginning dwells a magic, protecting us and helping us to live. . .
> (*Hermann Hesse*)

It was with these words that our fascinating top-up qualification as Cybersecurity Professionals began in September 2014 after a work-study course (Sarah Schuchardt) and training as an IT specialist for systems integration (Alexander Schmitz). At an interesting kick-off event attended by Deutsche Telekom board members and external cybersecurity experts, we gained many insights into the subject that will occupy us well into the future: cybersecurity.

Practical Projects as the Focus of Instruction

The Cyber Security Professional program focuses on practical work. We were therefore given interesting projects right from the start. In the Cyber Defense Center, Sarah worked on the development of a prototype for visualizing firewall log data for small and medium-sized companies (the Cyber Threat Detector), which was subsequently presented at CeBIT 2015. The Cyber Threat Detector is an entry-level solution that works according to the principle of a cyberdefense center – though on a smaller scale and in a more standardized way. The solution collects, aggregates and visualizes all log data generated by a connected firewall. The detector then compares this data with information about current and past cyberattacks and their control structures. If the solution identifies such communication patterns, it sounds the alarm so that action can be taken quickly. The detector also clearly displays traffic streams into and out of the company in real time and visualizes them according to their destination countries, internal network segments and the protocols used. This makes it possible to see in real time whether data is leaving network segments from which no data is usually allowed to flow. The new tool offers various filtering options right in the user interface to easily display relevant data for analysis purposes. Companies using the Threat Detector benefit from the broad networks and analyses of Deutsche Telekom. The solution compares attack indicators from the German Federal Office for Information Security, known attack patterns, data from general attack analyses, as well as data from 180 traps set by the company to provoke and analyze cyberattacks.

From the start, Alexander worked in the Network Services and Data Centers units on projects for protecting cloud storage devices. We were each immediately assigned an employee from our new team as a professional coach. In the early days

in particular, these colleagues supported us with suitable projects and points of contact that were important to our day-to-day work.

Virtual Detective Work as Final Module Assignment

The last two successful years of continuing education have included a variety of university modules. Topics such as network and application security, programming in an IT security environment and forensics were all covered. The latter was an especially noteworthy highlight. In the module on digital forensic methods, an Internet crime was presented for our final assignment. The case involved a web server that was compromised through a local file inclusion vulnerability. This made it possible for the attacker to read the system's password file. We were given two operating system descriptions for the potential criminal. Using our newly acquired forensic skills, we had to identify the perpetrator – a virtual manhunt, so to speak.

Along with the university modules, we received additional soft-skills training. Sessions such as "Compact IT Security Knowledge" at the start of the program, and workshops such as "Rhetoric" and "Intercultural Communication" were special highlights. We used a "cyberlogbook" to record our progress and the knowledge that was conveyed in the modules and training sessions. This served as evidence of what we had learned and as an exam prerequisite for the Chamber of Commerce and Industry, and it was discussed in personal meetings every two months with our learning process advisors and professional coaches. Reflection workshops were held every six months to foster communication among the CSP participants. In the course of these we discussed the current university modules, contemporary security issues and general suggestions for the program.

There was a lot of interest in our further education program right from the start. Because we were the first candidates for this entirely new job profile, there were internal and external (press) inquiries about our training. We also represented the new program at the Chamber of Commerce and Industry Education Awards 2016 and were on hand to witness the presentation of the third-place prize.

Cyber Security Professional Training for Jobs of the Future

At the end of the program, we have to complete an exciting final project. The only requirement in terms of content is that it has to be practically relevant to our everyday work, so the focus must be on the current issues handled by each security team. At the end of the two and half years there is an oral exam, during which we'll be asked about the final project and what we have learned. After graduating, we will be certified "Cyber Security Professionals" who are highly motivated to start these jobs made for the future. But we know: "...it won't always be easy to feel the magic... never put an end to the beginnings!"

Alexander Schmitz is a Cybersecurity Professional at Deutsche Telekom AG, where he works in the Group Security Services, primarily in the field of cloud security. A specialist in IT system integration by trade, Schmitz focused in particular on using software component integration to model and implement complex IT technology systems during his training as a Cybersecurity Professional. He was also involved in networked IT system installation, configuration and administration, and the presentation of system solutions.

Sarah Schuchardt is a trainee in Deutsche Telekom's Cybersecurity Professional program and works in Group Security Services, the Cyber Defense Center and the CERT. Schuchardt studied Applied Informatics at Baden-Wuerttemberg Cooperative State University and worked for T-Systems International GmbH, with projects including development of the application lifecycle management and version control for complex projects. She also used Metasploit exploits for vulnerability grading work.

Glossary

Advanced Persistent Threat (APT) A targeted attack and stealthy attempt to spy on confidential data and IT infrastructure.

Big Data The rapidly growing volume and complexity of corporate data, which needs to be stored and structured efficiently, and made available for analytical purposes within a very short timeframe – to perform risk appraisals in financial or energy-sector applications, for example.

Bring Your Own Device (BYOD) The trend for employees to use their personal mobile devices such as smartphones and tablets in a corporate environment. BYOD requires a comprehensive concept for the integration of such hardware.

Cloud Computing IT infrastructure and applications (such as software or storage capacity) sourced from a network generally operated by a service provider. Data is no longer hosted on the company's own storage servers, but in the provider's data center. (See also Private Cloud and Public Cloud.)

Cryptolocker An encrypted Trojan that is smuggled into a system where the cryptolocker encrypts files and then demands payment of a fee to decrypt them. (See also Ransomware and Trojan.)

Cyberwarfare The conduct of warfare with information technology as the battleground. Involves attacks targeting computers, data, information and systems.

Distributed Denial of Service (DDoS) A multi-pronged attack against computers, networks or servers. Typically, the attack target will be overloaded by the sheer volume of connection requests, leading to it becoming unavailable and its service therefore "denied."

Firewall A security system placed between local and public IT infrastructures to prevent outside intrusion into local systems.

Hacktivism Exploiting IT infrastructure for ideological, grassroots and/or politically motivated activism.

Honeypot A program or system offering an attractive target to distract intruders from their original objective and render them harmless.

Internet of Things The networking of everyday objects with the Internet, enabling them to communicate independently and carry out various tasks. (See also Wearables.)

Internet Protocol (IP) A network protocol that transports data packets from a sender to a receiver via multiple intermediate networks.

F. Abolhassan (ed.), *Cyber Security. Simply. Make it Happen.*, Management for Professionals, DOI 10.1007/978-3-319-46529-6

Intrusion Prevention Monitoring of data traffic within the network with the aim of detecting and blocking attacks by analyzing network usage patterns.

Load Balancing Distribution of loads within server environments or data centers to increase the speed of the overall system.

Machine Learning (ML) Generic term for the artificial generation of knowledge from experience. An artificial system learns from examples and can generalize this experience once the learning phase is over. The system therefore not only memorizes the examples but also identifies laws and patterns in the data.

Major Incident (MI) A severe fault – such as the failure of an entire IT system – that results in a serious interruption of business activities and must be resolved with great urgency in order to avoid significant loss or damage (such as damage to the company's reputation or financial losses).

Malware Undesirable and damaging pieces of software. (See also Trojan, Virus and Worm.)

Managed Services Provisioning of information and communications services by a specialized provider in accordance with a framework contract.

Mobile Application Management (MAM) Software and solutions that provision internally developed and publicly available mobile applications for use in a business environment. Alongside apps on work devices, this also covers apps on personal devices within the framework of a BYOD policy. (See also Bring Your Own Device.)

Mobile Content Management (MCM) Provisioning, administration and backup of company-internal documents and content on mobile devices.

Mobile Device Management (MDM) Software-based and centralized administration of mobile devices in terms of inventory, software, data distribution and security.

Network Time Protocol (NTP) Standard for clock synchronization between computer systems.

Outsourcing Moving of services or units to external providers.

Patch Piece of code correcting software vulnerabilities in software or systems.

Phishing Luring users to enter personal data with fake websites or messages for the purposes of identity theft. If successful, bank accounts or email accounts from affected users can be viewed and used without restriction.

Predictive Maintenance (PdM) Monitoring a system to forecast potential defects or failures with the aid of data collected on a continuous or cyclical basis.

Private Cloud A non-public implementation of cloud computing. The cloud infrastructure here is operated for a single company or a specific group of people – either by the company itself or by a provider. (See also Cloud Computing and Public Cloud.)

Public Cloud A public implementation of cloud computing. The cloud is made available to a broad group of users and is freely accessible over the Internet. (See also Cloud Computing and Private Cloud.)

Ransomware Malware that not only seeks to restrict or prevent data usage or access but which actively demands payment of a fee to decrypt or release this data. (See also Cryptolocker.)

Red Teaming Testing method for plans, strategies and hypotheses in a simulation scenario. While the term originated in a military context, the method is now also deployed by companies. (See also Wargaming.)

Reverse Engineering Creation of a blueprint or source code from a finished system for the purposes of reconstructing its design and/or further developing the system.

Sandbox An isolated software environment that can be used to test program code. Deployed in a security context to safely activate malware and study its mechanisms.

Smart Data Generating added value from Big Data by the intelligent use of very large volumes of data. (See also Big Data.)

Social Engineering Manipulation of interpersonal relationships to cause people to perform a certain action (e.g., to disclose personal data, purchase specific products or services, pay sums of money, etc.).

Trojan A piece of computer malware that disguises itself as a useful application but executes other actions in the background. (See also Malware.)

Underground Economy Economic activities that proceed in parallel to and undetected by the Government taxation system.

Vendor Lock-In Dependency on a specific manufacturer.

Virus A piece of computer malware that self-propagates by infecting other programs. (See also Malware.)

Wargaming Simulation of dangerous real-world situations to test strategies without risk under realistic conditions. While the method originated in a military context, it is now also used by companies as a means of testing their security strategies. (See also Red Teaming.)

Wearables Computer technology that is worn by the user. Generally used to help the user in the collection, processing and sharing of information and data. (See also Internet of Things.)

Web Proxy Communications interface within a network which accepts queries and establishes a connection to the recipient using its own address.

Worm A piece of computer malware that self-propagates without infecting other files or boot sectors. (See also Malware.)

Zero-Day Exploit Possibility of exploiting a vulnerability in a system or program before a patch is available as a countermeasure. (See also Patch.)