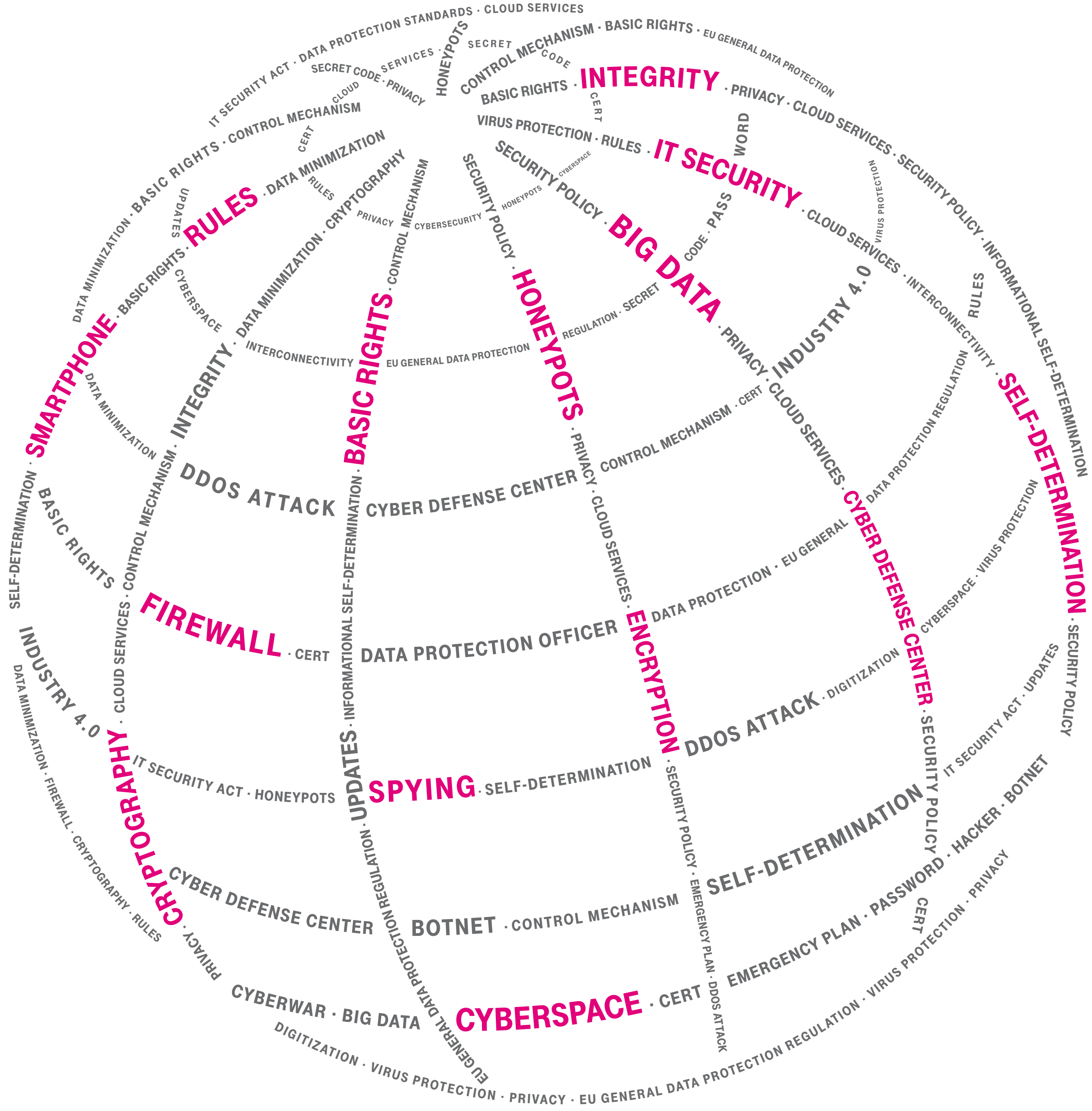


DATA PRIVACY AND DATA SECURITY

REPORT 2014

LIFE IS FOR SHARING.

CONTENTS

4 "As our society becomes increasingly connected, people must have confidence in the digital world and its services," states **Dr. Thomas Kremer**, Member of the Board of Management for Data Privacy, Legal Affairs and Compliance at Deutsche Telekom.

"Germany is a European leader in IT security and data protection": an interview with **Dr. Thomas de Maiziére**, Federal Minister of the Interior. 6

13 "All and any utilization of EU citizens' data should be subject to EU law," says **Axel Voss**, Member of the European Parliament.

14 **Timotheus Höttges**, CEO of Deutsche Telekom: "Differing levels of data protection are distorting competition."

16 "Our informational self-determination is at risk," warns **Dr. Claus-Dieter Ulmer**, Senior Vice President of Group Privacy at Deutsche Telekom.

17 "IT security is becoming increasingly network-centric," says **Thomas Tschersich**, Head of IT Security at Deutsche Telekom.

18 3rd Cyber Security Summit in Bonn: cyber crime and geopolitical crises.

20 Cyber Security Summit for Kids in Bonn / TeachToday / supporting child-friendly content.

24 Deutsche Telekom's Data Protection Advisory Board: mandate extended.

26 **Wolfgang Kopf**, Senior Vice President of Public & Regulatory Affairs at Deutsche Telekom: assuming joint responsibility.

28 **Hans-Lucas Bauer**, Head of the Group Criminal Law unit at Deutsche Telekom: cross-border cooperation in law enforcement.

30 **Dr. Jürgen Kohr**, Senior Vice President of Cyber Security at T-Systems: security is for sharing.

32 Data anonymization process / Certified data protection / Email made in Germany.

34 Data protection and security – facts and figures.

36 Deutsche Telekom's Cyber Defense Center combats online espionage.

38 'Dataslob' / Trade fair appearances 2014 / Privacy Icon / Webportal www.sicher-digital.de/

40 Executive Information System / Digital staff records / Data protection awareness survey / HR software from the cloud.

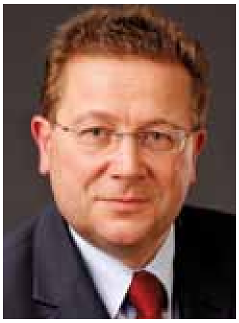
8

"Robust data protection rights that are effectively enforced are the only way to ensure people's trust in the internet, data flows, and new technologies in general," says **Věra Jourová**, EU Commissioner for Justice, Consumers and Gender Equality.

10

Andrea Voßhoff, Federal Commissioner for Data Protection and Freedom of Information, believes "the European General Data Protection Regulation could have an impact far beyond Europe because of the country-of-reception principle, and provisions governing third country data transmission."

Jan Philipp Albrecht, member of the European Parliament, believes that the EU General Data Protection Regulation "will prevent companies from evading data protection legislation to gain an unfair competitive advantage." 22



25 **Lothar Schröder**, Deputy Chairman of the Supervisory Board at Deutsche Telekom, explains that "trust is vital to long-term business success – in the digital age more than ever."

Reinhard Clemens, CEO of T-Systems and member of Deutsche Telekom's Board of Management, is convinced that there will be "no Industry 4.0 without robust data protection." 31

42 Binding Corporate Rules Privacy / Global Privacy Summit / Privacy by design / Road-pricing in Belgium.

44 Cyber Security Report 2014 / Security Report 2014 / A study by market research agency TNS Emnid / Deutsche Telekom's Browser 7.

46 Mobile privacy solution / Mobile Encryption App / Deutsche Telekom fixes mobile network security flaw / Deutsche Telekom acts quickly to neutralize Android virus.

48 "Cybercrime poses a serious threat to the digital industry": an interview with **Axel Petri**, Senior Vice President of Group Security Governance at Deutsche Telekom / Tracking with canvas fingerprinting.

50 The family-owned company Ensinger shields its expertise within a private cloud.

51 Tengelmann: a business must identify its key assets in order to protect itself from cyber attacks.

52 Working with government agencies / Deadlines for security patches / New security requirements / Corporate Security 2030.

54 Built-in protection for mobile devices / Deutsche Telekom and Infineon present security solution for 'Industry 4.0' / Containerizing solution for business apps / Real-time cyber defense with FireEye / The vulnerabilities of FRITZ!Box routers.

56 Training for security experts / A new department dedicated to data protection and security.

58 Digital guide to protecting information / IT security of the highest caliber / Awareness of security issues at peak levels.

“IN TODAY’S **CONNECTED SOCIETY**, CONFLICTS INEVITABLY SPILL OVER INTO THE DIGITAL WORLD.”

Some might be surprised to find that, a year after the Edward Snowden scandal broke, cyber security has not lost its momentum as a hot topic. The headlines in 2014 may have been dominated by the crises in Ukraine and the Middle East, and the new year began with terrorist atrocities. But each of these tragic events had aspects that played out online. They ranged from recruiting new followers and spreading propaganda on social media sites, to cyber attacks on IT systems. In today's connected society, conflicts inevitably spill over into the digital world. As a result, cyber security remains an issue that demands our undivided attention – especially as the torrent of worms, trojans, and other malware shows no sign of relenting. Deutsche Telekom's early warning system alone detects up to one million cyber attacks every day – a trend that is likely to gather pace.

> "Companies need emergency response teams."

Even now, the fallout from the Snowden affair continues to be felt, and questions regarding the scope of his knowledge remain unanswered. Until these points are clarified, Deutsche Telekom lacks important information needed to better protect customers and resolve potential system vulnerabilities. And we are still waiting for corresponding steps and decisions to be taken by politicians: it is difficult for me to grasp, for example, why we cannot agree to forgo spying on one another, at least within the EU.

As our society becomes increasingly connected, people must have confidence in the digital world and its services. This requires more effort on all sides. A major hindrance is a lack of solid knowledge. With this in mind, Deutsche Telekom supports further research in and education on data privacy and cyber security. For example, Deutsche Telekom has established a dedicated department at Leipzig University of Telecommunications (HfTL).

In addition, companies need emergency response teams in order to keep each other abreast of new digital threats. Deutsche Telekom has significantly strengthened its Cyber Defense Center team, and promotes training of security specialists. This resolve is mirrored in the organization's Cyber Security Professional certification program, established in collaboration with the Cologne Chamber of Commerce.

Clearly, security must be taken into consideration throughout the entire value chain. For this reason, Deutsche Telekom will continue to push for end-to-end data transfer encryption. However, the responsibility does not solely rest with the organizations operating infrastructure. Hardware and software vendors must be committed to swiftly resolving potential product vulnerabilities.

We must collaborate more closely to ensure our society is properly equipped for the digital age. There is no denying the facts: our world is becoming increasingly connected. And not just people; a growing number of devices and machines are communicating with each other, and entire value chains are becoming digitized. As a result, we are inevitably more susceptible to virtual attacks. The bottom-line: improving IT security should continue to be a top priority.

ABOUT THE AUTHOR

Dr. Thomas Kremer
has been Board member for Data Privacy, Legal Affairs and Compliance at Deutsche Telekom AG since June 2012. He has been the acting Chief Human Resources Officer since January 2014. As a lawyer by profession, he previously served as Executive Vice President at ThyssenKrupp AG, where he assumed responsibility for legal affairs in 2003. In 2007, the ThyssenKrupp Group appointed him Chief Compliance Officer.

"GERMANY IS A EUROPEAN LEADER IN IT SECURITY AND DATA PROTECTION"

"The digital world is not a world to itself, and cannot be allowed to exist outside the law," says German Federal Minister of the Interior Thomas de Maizière in an interview for this report.

Dr. de Maizière, why do we need to reform data protection legislation?

Dr. Thomas de Maizière: Opportunities to collect and aggregate data have dramatically increased in the past few years. According to a recent study by market research organization Gartner, 30 billion devices will be interconnected by 2020. Data is generated everywhere; by everyday consumer products, household appliances, smart meters, cars, and industrial equipment. This development is often associated with the 'big data' phenomenon – and there is huge potential for new products and business models. Capturing large amounts of information – and using it to create profiles, for example – can create new insights and opportunities. However, it can also jeopardize our privacy. Data protection laws must address these risks. We also need EU-wide legislation, as a national regulatory framework is too limited in the Internet age. A level playing field would also benefit Germany-based service providers.

So, do Internet-specific laws have to be passed?

Dr. Thomas de Maizière: The digital world is not a world to itself, and cannot be allowed to exist outside the law. It must be subject to the same rules as the analog world. But we need tailor-made mechanisms and tools to deal with the specific characteristics of the Internet. It is a phenomenon we have already encountered with other new developments. But it would be wrong to suggest that cyberspace and everything related to it needs its own self-contained regulatory framework.

What would these "tailor-made mechanisms" be?

Dr. Thomas de Maizière: Data privacy principles must continue to apply. More and more information is being created and aggregated – and we must adapt privacy mechanisms accordingly. In the era of big data, we need transparency; we need to be informed on how our data is being used; and we need to have control over our own data. Both private citizens and enterprises stand to benefit from greater control over the

> “ CLEARLY-DEFINED, EFFECTIVELY-IMPLEMENTED DATA PROTECTION SYSTEMS WILL ENCOURAGE CITIZENS TO SHARE INFORMATION. ”

divulgence of personal data. Clearly-defined, effectively-implemented data protection systems will encourage citizens to share information. Europe-wide governance mechanisms will help achieve this vision. In the Internet age, data ignores traditional boundaries and borders. So tailor-made mechanisms entail, above all, a harmonized and enforceable set of commonly accepted rules.

How are the negotiations on the General Data Protection Regulation progressing in Brussels?
Dr. Thomas de Maizière: We're moving forward. The European Council wants to wrap up negotiations by the end of the year. For a number of months, member states have been making all efforts to agree on selected sections of the regulation. Any agreements are subject to reaching a consensus on the regulation as a whole – but they are nevertheless a means of gradually bringing the Council to a comprehensive accord.

What are the major topics of discussion?
Dr. Thomas de Maizière: Four main things: citizen centricity, legal certainty, modernization, and harmonization. A citizen can only be confident of safeguarding their privacy if local institutions offer the highest-possible levels of protection. If major non-EU Internet players do not adhere to European legislation, their European counterparts will struggle to compete. Strict rules on profiling and pseudonymization are essential for the Internet age.

The issues surrounding profiling show how important it is it to draw up clear rules…
Dr. Thomas de Maizière: … correct. And it shows how difficult it is to strike the right balance between the rights of individuals and legitimate commercial interests. After all, profiling often provides valuable insights. So, the German government is striving to implement clearly defined legal provisions.

And don't we need to pay closer attention to the technical aspects of data protection?
That is our stated objective. I am pushing for a greater focus on the concept of pseudonymization in the General Data Protection Regulation. This would make it significantly harder to identify individuals, and would allay fears of personal data misuse through big data applications. By the same token, letting companies do more with pseudonymized information will incentivize them to embrace this technique. For this reason, Germany has made a corresponding proposal at EU level. And we should also mention the concepts of data protection ‘by design' and ‘by default.' These ensure that data protection mechanisms and predefined settings are built into analysis solutions from the outset.

How will the legislation affect non-European organizations, particularly those based in the US, providing services to EU citizens?
Dr. Thomas de Maizière: If they want to offer their services here in Europe, they must adhere to our laws: it's a case of “our market, our rules.” This principle will be a cornerstone of the General Data Protection Regulation. In other words, European data protection provisions will apply to all, including US and Asian organizations, regardless of whether they have a physical presence here or not. We want to prevent the practice of forum shopping, promote fair competition, and establish a consistent level of data protection for all European citizens.

You are responsible for data protection and IT security legislation. On behalf of the German government, you recently presented a draft IT security act. What is its aim?
Dr. Thomas de Maizière: In essence, to safeguard IT systems of critical importance to society against attacks and malfunction. This includes, in particular, energy provision, healthcare, banking, and insurance. We plan to introduce industry-wide security standards and mandatory reporting. This would mean a tangible improvement in IT security in these areas, and would give us a clearer picture of the threats we face from cyberspace – making the Internet a safer place. We will strengthen the role of the Federal Office for Information Security (BSI), and broaden the Federal Criminal Police Office (BKA)'s remit in cybercrime investigation.

The business world initially reacted to the project with a great deal of skepticism. What have you done to allay its fears?
Dr. Thomas de Maizière: It is my impression that the private sector has realized that, due to the ongoing dangers we face, we must urgently safeguard the IT security of our critical infrastructure. In this context, it was important for me to build upon existing forms of cooperation between government and business, and to ensure transparency throughout the entire process. Calm, rational discussion of the draft legislation ensued, providing excellent feedback for further improvements to our proposals. This resulted in a marked increase in acceptance within the business world.

In the context of IT security we always need to be aware of the European dimension. Are you not worried that the network and information security directive currently being negotiated in Brussels could render your own national efforts obsolete – or even undermine them?
Dr. Thomas de Maizière: No. My ministry is responsible for both – for drafting the German IT security act, and for the negotiations in Brussels. It is our aim to achieve the greatest possible degree of alignment in the areas covered by the directive. However, synchronizing two projects of such complexity and consequence is a major challenge, not least because we are just one of a total of 28 member states. I feel our own IT security legislation sends out a signal at national level that has been heard and understood in Brussels, too.

Continues on page 8 >

Any discussion of improved IT security naturally leads to discussion of the entire German IT security industry. How would you describe its role, especially in the aftermath of the Snowden revelations?
Dr. Thomas de Maizière: Within the German economy, the IT security industry is one of the sectors with the brightest futures, and with the greatest proven strengths. It comprises more than 9,000 predominantly small and mid-size enterprises, known for secure, reliable niche solutions that enjoy international success with the made-in-Germany label. For example, just consider these companies' capabilities in encryption or cryptohardware. We intend to leverage this potential to strengthen users' trust in secure digital infrastructure.

ABOUT THE INTERVIEWEE

Dr. Thomas de Maizière
Born in Bonn, de Maizière has been a member of the German Bundestag since 2009. He has served as the Federal Minister of the Interior since December 2013, and also held the post from 2009 to 2011. From March 2011 until December 2013 he worked as the Federal Minister of Defense. From 1999 to 2005, he held a number of positions within the state governments of Mecklenburg-Western Pomerania and Saxony. These included Head of the Chancellery of Saxony, and Minister of the Interior, Minister of Finance and Minister of Justice in the government of Saxony.

STRONGER DATA PROTECTION RULES TO BOOST THE DIGITAL SINGLE MARKET IN EUROPE

"Finalising the reform of the EU data protection rules and restoring trust in transatlantic data flows are among my top priorities for 2015," says Věra Jourová, European Commissioner for Justice, Consumers and Gender Equality.

Since the existing data protection directive was adopted in 1995, technological progress and globalisation have profoundly changed the way our data is processed. We face new challenges to privacy and data protection, mainly on the Internet and in social media. Today, 92 percent of Europeans are concerned about mobile apps collecting their data without their consent. And 89 percent say they want to know when the data on their smartphone is being shared with a third party.
We need updated rules to ensure a consistently high level of protection for citizens and the free flow of data. The European Commission proposed a reform of the EU's data protection rules in January 2012 to strengthen online privacy rights and boost Europe's digital economy. This is necessary as the reform is a key building block both for justice and fundamental rights and the digital single market, two of the ten priority projects of the Commission. We therefore need to swiftly conclude the ongoing negotiations on this reform project and start implementing the new rules. Our aim remains to build on the good progress made in recent months and to successfully conclude the negotiations and to adopt the reform with the co-legislators in 2015.

BUILDING A DIGITAL SINGLE MARKET

Data is a strong currency of our time. But robust data protection rights that are effectively enforced are the only way to ensure people's trust in the Internet, data flows, and new technologies in general. Data protection is not only a right. Data protection and the trust that results from proper enforcement of the rules are a prerequisite for the digital single market. The proposed Data Protection Regulation will do away with 28 differing national laws, and provide a single set of rules on data protection, valid across the EU. We will simplify things by removing unnecessary administrative requirements, such as notification requirements for companies, further cutting red tape and increasing legal certainty for businesses.

The reform will create a level playing field for Europe's digital industry: companies located in third countries such as the US, when offering services to Europeans, will have to play by our rules and adhere to the same levels of data protection as their European competitors. Comprehensive and modern data protection rules would also inspire trust among consumers. People who trust that their personal data is protected will more easily buy goods and services online. Companies that handle personal data responsibly will have a competitive advantage. Clear and enforceable data protection rights will boost the digital single market.

The potential benefits of a digital single market are enormous. But to make it happen, we need to adapt to new technologies coming onto the market – like big data, cloud computing, the Internet of Things. These technologies, these investments will only come to the European market if we have sound data protection rules in place.

> “ WE NEED UPDATED RULES TO ENSURE A CONSISTENTLY HIGH LEVEL OF PROTECTION FOR CITIZENS AND THE FREE FLOW OF DATA. ”

ABOUT THE AUTHOR

Věra Jourová was appointed European Commissioner for Justice, Consumers and Gender Equality in November 2014. She has been a member of the Chamber of Deputies of the Parliament of the Czech Republic since November 2013, and the Minister of Regional Development since January 2014. She is the most popular Czech politician, enjoying widespread public trust.

The European Parliament recognised the significance of data protection reform early on. It showed real leadership and found a broad compromise, backing the Commission's proposals. Member States have taken more time because the positions were further apart. But they have now started to come together and move forward. EU Heads of State and Government affirmed the importance of "a strong EU general data protection framework by 2015". It's not a minute too early. The world will not wait for us. If we want Europe's digital single market to take off, we must get the data protection reform right, and soon. Citizens and businesses in Europe are waiting for it.

RIGHT TO BE FORGOTTEN (GOOGLE RULING)

But restoring trust is not the job of the EU alone. Business also has a role to play. As a reaction to the recent ruling of the European Court of Justice on the right to be forgotten there have been accusations of "censorship". In reality, the "Google ruling" does not give people the green light to have content removed from the web simply because they find it inconvenient. The ruling calls for a balance between the legitimate interests of Internet users and citizens' fundamental rights. A balance that will have to be found in each case. The Court clarified that search engines are controllers of personal data, and search engines, such as Google, can therefore not escape their responsibilities under European law when handling personal data.

We should also remind ourselves that neither the Commission nor the Court have just invented the right to be forgotten. It already exists, in our rules from 1995. With the data protection reform, we are updating this principle and clarifying it for the digital age. We are doing this by making it clear that EU rules apply to all companies offering products and services to European consumers, no matter whether their servers are based inside or outside the EU.

Like the Court's ruling, the aim of the data protection reform is a fair balance of rights: we want to empower citizens to manage their personal data while explicitly protecting freedom of expression and of the media. We want to strengthen people's rights while creating predictable conditions for businesses in the digital single market.

Among my key priorities is also to uphold the right to data protection in our external relations. I am working to ensure that our "safe harbour" arrangement with the United States is really safe. Moreover, all EU citizens should be able to enforce data protection rules in US courts. When it comes to personal data transferred for commercial purposes, the safe harbour arrangement with the US is the main basis for handling and protecting Europeans' data when it crosses the Atlantic. Europeans are asking questions: how safe is safe harbour after all? Does it protect our personal data? Do we need it at all?

INTERNATIONAL DATA FLOWS

Above all, I want to improve the safe harbour agreement. Doing business with the US is important – both for us and for our American partners. However, business opportunities should not come at the expense of our citizens' fundamental rights. In the European Union, everyone has a fundamental right to the protection of their personal data. This fundamental right applies no matter where the data is collected or processed. We have strong European standards, and we must make sure these standards are respected both in the European Union, and internationally.

We are making progress in this area, but there is further work to be done. My aim is to improve the safe harbour arrangement in the coming months. But the suspension of the arrangement remains an option on the table, should the negotiations not bring the desired results.

Besides this I am continuing the negotiations with the US on an umbrella agreement on data protection rules for exchanges in the law enforcement area. I want us to continue and to intensify our important cooperation on law enforcement across the Atlantic. But we also need to have a robust skeleton of data protection rules agreed between us to sustain it. Progress has also been made there, but we are still waiting for the US Congress to change legislation so that EU citizens can defend their data protection rights before US courts in the same way as US citizens.

A beefed up safe harbour arrangement and an EU-US umbrella agreement would be a huge step forward in transatlantic cooperation on data privacy. This would also be an important signal for other key EU-US projects such as TTIP.

We must get this done.

GREATER LEGAL CLARITY AND CERTAINTY

Andrea Voßhoff, Federal Commissioner for Data Protection and Freedom of Information (BfDI), believes the impact of the European General Data Protection Regulation could reach far beyond Europe's borders – because of the country-of-reception principle, and provisions governing data transmission to third countries.

How is data protection evolving at European level?
Andrea Voßhoff: Current developments are positive. In March 2014, a European Parliament resolution proposed a large number of practical improvements to the European Commission's draft of the General Data Protection Regulation. This was a very important contribution to our efforts at reform. I hope the Council will conclude its discussions and reach a consensus in the next few months. We have already achieved agreement in some areas, such as the country-of-reception principle, and the provisions for data transfer with third countries – and on an issue of key importance to Germany, namely, the degree to which existing data protection provisions in the public sector, including healthcare and social services, can be retained.

What are the key elements for adequate data protection within Europe?
Andrea Voßhoff: I believe a European General Data Protection Regulation is a fundamental precondition for implementing data protection per se. First, in an era of global data traffic and worldwide challenges, it will set a high standard. On account of the country-of-reception principle, and provisions on data transmission to third countries, this could have an impact far beyond Europe. Second, it will give citizens and businesses greater legal clarity and certainty – because as directly applicable legislation, it will harmonize the diverse national approaches of the 28 EU member states. Third, it will modernize our 20-year-old European data protection legislation without abandoning the tried-and-tested principles of the 1995 Data Protection Directive. The key elements of the General Data Protection Regulation are yet to be established – we will

have to wait and see what the European Parliament and the European Council agree at the end of the legislative process. I support the proposal made by the European Commission in 2012, recommending retaining proven principles – while strengthening the rights of individuals, and more precisely defining the responsibilities of companies who process data. Of particular note are the stricter requirements in terms of technological mechanisms for data protection.

I am also in favor of new forms of collaboration between data protection agencies, within the context of providing a one-stop shop and the consistency mechanism. Furthermore, the proposal makes new, improved sanctions available to oversight bodies. Another important issue is profiling. The European Parliament's proposals are a step in the right direction. They call for a clearer definition of profiling, and for clarification of when profiles may be created and how they can be used.

Are German agencies at federal and state level adequately prepared for the new developments?
Andrea Voßhoff: Federal and state oversight bodies need to address the issues at European and international level. New forms of cooperation between data protection authorities – with the aim of providing a one-stop shop, and within the context of the consistency mechanism on the European Data Protection Board – may well lead to a greatly increased case load. Under the new regulations, data protection authorities will have an expanded remit. This will include advance checks of high-risk data processing activities, certifications, and responsibilities associated with the transmission of data to third countries. In general, the challenges faced by data protection authorities will grow – as our society and our private lives become ever more digitized and connected. As a result, we need to strengthen the human and technical resources available to our authorities before the General Data Protection Regulation comes into force.

Andrea Voßhoff was appointed Federal Commissioner for Data Protection and Freedom of Information (BfDI) in January 2014.

> “THE COURT OF JUSTICE HAS STATED THAT EUROPEAN DATA PROTECTION LEGISLATION APPLIES TO COMPANIES OUTSIDE THE EU IF DATA IS PROCESSED WITHIN AN EU MEMBER STATE BY A CORRESPONDING SUBSIDIARY.”

Will the new legislation eliminate the competitive disadvantages encountered by European businesses, and how will the new provisions be enforced?
Andrea Voßhoff: The new regulation will improve the situation for businesses by harmonizing and simplifying the regulatory environment within the EU. Companies that operate in multiple member states will no longer have to contend with diverse national laws. Instead, they must simply comply with the General Data Protection Regulation, which will apply throughout the EU. As the regulation embodies the lex loci solutionis principle, its provisions will apply to companies based in third countries who deliver services to the single European market. As a result, there will be a level playing field in Europe in terms of data protection. By creating a one-stop shop and cutting bureaucratic red tape, the regulation satisfies one of the key demands of the business community. At the same time, I think it would be advisable to verify the effectiveness of these new provisions in practice. For this reason, I am in favor of the proposed evaluation clause.

What is your opinion on the ruling against Google made by the European Court of Justice? Will this have an impact on market participants other than search engines?
Andrea Voßhoff: On the face of it, the ruling guarantees Internet users the right to be forgotten by Google's search engine. Other search engines are equally affected, and must comply with legitimate user requests for data deletion. What is more significant is that the Court has stated that European data protection legislation applies to companies outside the EU if data is processed

Andrea Voßhoff: “At first glance, Big data would appear to be incompatible with the principles of data protection. But is it really?“

within an EU member state by a corresponding subsidiary. It is sufficient for the subsidiary to play a supporting role, for example by advertising data processing services. As a result, the ruling not only applies to Google and other search engines, it also has an impact on other online business activities.

Do you think that the transparency and opt-out provisions are, in contrast to opt-in solutions, enough to entitle companies to process data?
Andrea Voßhoff: Opt-in solutions are an effective means of enforcing Germany’s statutory right to ‘informational self-determination’ as citizens must be asked explicitly for their consent before their data is processed. With the opt-out method, users are often only made aware of their data being processed after the fact, and can only object retrospectively. As a result, opt-out is always less effective than opt-in.

However, opt-in methods are subject to strict conditions under German and European law. Consent must be expressly given, be based on a freely taken decision, and granted while fully aware of all relevant circumstances. And service providers in other countries are bound by these requirements, too, if they claim to be adhering to the opt-in method. Our aim must be to improve the effectiveness of high German and European standards within the context of globalized data processing – and not to allow European standards to be eroded by existing international practices.

Shouldn’t big data models be allowed greater freedom in order to gain information and insights of vital importance to our society as a whole?
Andrea Voßhoff: Big data is a mysterious and ambiguous term. And at first glance it would appear to be incompatible with the principles of data protection. But is it really? Existing big data models crunch huge volumes of data, and there is a danger of data legitimately captured for one purpose being illegitimately exploited for a very different one. And for this very reason, it is important to enforce established principles. For example, the concept of data minimization, i.e. only using as much data as is really needed and only for the original, defined purpose. Moreover, we need to work on the evolution of concepts such as pseudonymization and anonymization. After all, anonymous data is often more than adequate for big data analysis purposes.

What would you most wish to see German businesses do in the context of data protection?
Andrea Voßhoff: My position leaves little scope for wish lists. But I would certainly be happier if all German companies would at least embrace the idea of data protection as a competitive advantage. The concepts of privacy by design and privacy by default should be the bedrock of all projects. If these concepts were applied conscientiously, it would be beneficial on all fronts: for businesses, for customers, and for data protection.

ABOUT THE INTERVIEWEE

Andrea Voßhoff
Was appointed Federal Commissioner for Data Protection and Freedom of Information (BfDI) in 2014. She has a degree in law, and was a member of the German Bundestag from 1998 to 2013, serving on the parliamentary committee for legal affairs. From 2010 to 2013, she was the spokesperson on legal policy within the CDU/CSU parliamentary party.

EUROPE'S GLOBAL ROLE IN DATA PROTECTION AND DATA SECURITY

The European Union's Charter of Fundamental Rights states that "Everyone has the right to the protection of personal data concerning him or her." This puts data protection on a par with other fundamental rights, such as human dignity and freedom of thought, and makes the EU a global pioneer on this issue. Germany's constitution does not explicitly mention the term "data protection" at all.

Digitization has brought about more change than any other technical revolution, transforming our social behaviors and working habits, our communications, competitiveness, relationships between nations, and law enforcement. It affects copyright and intellectual property, the fundamental right of data protection, and ultimately, personal privacy.

In terms of their magnitude and impact, the challenges posed by new technologies, the Internet, and globalization are not yet fully understood. Nor can they be regulated by law. Any attempt to govern the use of data has to resolve issues concerning the protection of

- fundamental rights: data protection, privacy, human dignity, freedom of thought and ownership, press freedom
- global competition and economic growth: value creation, innovation
- data security and other security concerns: law enforcement, intelligence services, cyber warfare and defense.

NATURE OF PRIVACY WILL CHANGE

As traditional structures break down and data scandals undermine consumer confidence, the relevant regulatory bodies – such as antitrust authorities and supreme-court decisions – need to adapt. The perception of the state being the enemy of individual freedom must be reassessed – in light of today's data monopolies, it is no longer tenable – as the greatest threats to personal privacy do not come from the state. At the same time, the degree of privacy that citizens enjoyed a mere ten years ago will soon be unattainable. The nature of privacy will change, and it is our task as legislators to adopt a new and different approach. If data is the currency of the future, then antitrust authorities must respond to data monopolies.

European researchers and innovative enterprises need to constantly revisit the issue of data security. They need to develop ever stronger protections against prying and intrusion. Encryption technology will take on a new and greater role. Legislation to implement fundamental rights is often impeded by the clash between political cultures and value systems. Data protection and data security are a case in point, and occupy a firm place on the political agenda. The European Commission under Jean-Claude Juncker boasts a Commissioner for the Digital Economy and Society (Günther Oettinger), and a Commissioner for the Digital Single Market (Andrus Ansip). This sends a strong message that the EU intends to play a pioneering role in digital issues. While recognizing that the USA is the most powerful player, Europe is no longer content merely to follow its lead.

> "All and any utilization of EU citizens' data should be subject to EU law."

EU-US UMBRELLA AGREEMENT

The EU's task will be to establish a legal environment for its citizens that will generate consumer confidence in digital data utilization through robust rights and protections, while still enabling the innovations that drive growth and competitiveness in the data economy. Our goal must be: all and any utilization of EU citizens' data should be subject to EU law.

In particular, close attention should be paid to the transfer of European citizens' data to non-member states. On this issue, the European Union has become more determined and more demanding of late: since a global agreement on data flows seems unattainable, the EU must at least agree equal competitive conditions with the US. Should it fail, Europe will have to chart its own course. For this reason, the EU-US data protection umbrella agreement should be enacted without delay, and the safe harbor mechanism suspended and placed on a new legal footing.

The EU can set an example by showing how the digitization and global exchange of personal information can be aligned with the fundamental rights and values of the analog era.

ABOUT THE AUTHOR

Axel Voss

A Member of European Parliament since 2009, Axel Voss has been vice chairman of the Committee on Legal Affairs and the legal policy spokesman of the EPP parliamentary group since 2014. A lawyer by profession, Voss was formerly a member of the Committee on Civil Liberties, Justice and Home Affairs, and had a particular interest in migration policy, asylum issues, data protection, and cross-border police and judicial cooperation.

“DIFFERING LEVELS OF DATA PROTECTION ARE DISTORTING COMPETITION”

Deutsche Telekom complies with German data protection legislation, but different rules apply to companies headquartered in the United States. Timotheus Höttges, CEO of Deutsche Telekom, is concerned by this issue. That’s why he’s calling for a level playing field.

Mr. Höttges, a year has passed since the Snowden revelations, and the third Cyber Security Summit took place in Bonn just a few weeks ago. Is cybercrime an evolving threat?
Timotheus Höttges: Yes. Wherever political conflicts spring up around the globe, cybercrime tends to follow. The opponents leverage state-of-the-art ICT for propaganda, and for their own communication purposes. But they also harness this technology to launch digital attacks on their adversaries over the Internet. Against this background, the peril of cybercrime continues to grow.

Is there evidence to suggest terrorists have targeted computer networks and public infrastructure?
Timotheus Höttges: Unfortunately, we are unable to identify the attackers in the majority of cases. However, we should not rule out the possibility of politically motivated cybercrime, even though there have been few confirmed instances to date. There are strong suspicions that a number of years ago, a sophisticated Trojan was used to spy on a number of businesses in the energy, aviation and research industries. And hackers in Syria were responsible for compromising the water supply in Haifa. In the United States, the registered number of attacks on public infrastructure soared by around 60 percent in 2013, compared to 2012. Recently, the NSA confirmed that e-criminals in China had successfully penetrated the IT systems of US power utilities. The NSA believes hackers are capable of crippling this type of infrastructure.

How can we defend ourselves against this new threat?
Timotheus Höttges: First and foremost, any one of us could fall victim to cybercrime, either directly, or indirectly if key infrastructure is taken offline. There is no room for complacency – everybody is vulnerable. It is therefore imperative that everyone – countries, businesses and organizations – works together to combat this threat. Unfortunately, though, I have seen very little progress towards international agreements on this issue.

“We must do everything in our power to safeguard customer data. If customers stopped trusting us, it would destroy a cornerstone of our business model.”

Germany and the United States appear to remain poles apart on the issue of data security – even following the Snowden scandal.
Timotheus Höttges: It is high time that Europe and the US reached a mutual understanding of what data protection entails. The high standards of privacy in Europe are a blessing, but they are distorting competition in the digital economy. American businesses do almost whatever they want – but we permit ourselves very little. With this in mind, the proposed EU General Data Protection Regulation cannot enter into force soon enough. This would mean that all businesses serving EU citizens would have to

ABOUT THE INTERVIEWEE

Timotheus Höttges
has been Management Board Chairman of Deutsche Telekom AG since January 1, 2014. As a business management graduate, he was the board member in charge of finance and controlling from 2009. From December 2006 to 2009 he was responsible for the T-Home division on the Group Management Board. In that capacity he was in charge of fixed-line and broadband business, and of integrated sales and service in Germany. He began his career with Deutsche Telekom in 2000 as Director of Finance and Controlling and later Management Board Chairman of T-Mobile Germany. In 2005, Höttges was assigned responsibility for European business on the Management Board of T-Mobile International.

work within the same parameters – including companies headquartered outside of Europe.

How would this impact European enterprises?
Timotheus Höttges: It would help create a level playing field, and would allow us to reap the benefits of our investments in data protection and data security. However, the US Senate's recent decision to block Barack Obama's surveillance reform bill is far from encouraging – and I feel certain that American businesses share my concerns. Europe is a key market for them, and their customers expect straight answers to data protection questions. We've noticed that more and more of our major customers are specifically requesting 'made in Europe' IT services.

But American companies still store and process enormous quantities of European consumer data.
Timotheus Höttges: That makes it imperative that everyone plays by the same rules, benefitting both the business community and consumers. We need a consistent data protection regulation across Europe – with no loopholes. In short, European consumer data should be treated the same way throughout the globe.

Internet players based overseas would surely disagree.
Data generated in Europe should be subject to the same European data protection legislation. All providers that comply with these legal requirements should be granted access to the data, whether they are headquartered in Europe, the United States or Asia. It is not about splitting up the Internet – it's about creating legal certainty in the digital space.

Why does Deutsche Telekom take data security so seriously?
Timotheus Höttges: That's easy to explain – we process and store vast quantities of data for our customers. Many customers entrust business-critical information to our data centers. As a result, we must do everything in our power to protect and safeguard that data. If customers stopped trusting us, it would destroy a cornerstone of our business model.

How does Deutsche Telekom protect itself?
Timotheus Höttges: Let me give you a couple of examples. We are currently establishing a new Cyber Security unit, where all IT security-related activities will be concentrated. This unit will be responsible for the security of our own organization, but will also market products and services to our customers.

In 2014, prompted by a shortage of corresponding skills on the IT labor market, we became the first company in Germany to create a dedicated training program for cyber-security professionals. We have opened our very own Cyber Defense Center, and we embed IT security into the design of our products from the get-go. And in conjunction with our partners, we are developing a truly end-to-end solution that effectively combats cyber attacks.

In the past, cyber security was primarily the preserve of IT experts, and was rarely discussed at executive management level. Has this changed?
Timotheus Höttges: Yes – as demonstrated by the annual Cyber Security Summit. The number of attendees from the business world has risen year-on-year. And the growing interest in our security solutions and cloud offerings reflects this trend. The whole data protection issue has played its part.

Data protection legislation in Germany is relatively strict. Businesses want to know exactly where their data is stored. They want assurances that highly sensitive customer and corporate data enjoys bulletproof protection. They are concerned about back-door attacks – and as a result, they are increasingly leaning towards European solutions.

How do you, as the CEO of an ICT solutions provider, protect yourself personally against data misuse?
Timotheus Höttges: I store my passwords in a highly secure program, and I send emails using a secure Deutsche Telekom server. I don't post personal photos online, or use services such as WhatsApp. And when it comes to cloud services, I only trust our own products.

“IT IS IMPERATIVE THAT EVERYONE – COUNTRIES, BUSINESSES AND ORGANIZATIONS – WORKS TOGETHER TO COMBAT THE THREAT.”

INFORMATIONAL SELF-DETERMINATION IS AT RISK

Dr. Claus-Dieter Ulmer, Senior Vice President, Group Privacy, at Deutsche Telekom warns that informational self-determination is at risk if governments and businesses can read, save and analyze personal data unchecked.

Dr. Ulmer, the Federal Constitutional Court coined the term informational self-determination over 30 years ago – before Facebook's founder was born, and 15 years ahead of Google's launch. Did the justices have some kind of crystal ball?
Dr. Claus-Dieter Ulmer: By coining the term informational self-determination, the Constitutional Court wanted to make clear that every citizen has a fundamental right – the right to decide what personal data they disclose and, most importantly, how that data is used. The ruling came amidst controversy surrounding the German census in the early 1980's, which many citizens boycotted. The court's decision is all the more important when we consider where and to what extent data is being collected and analyzed today.

In 2008, the Federal Constitutional Court also ruled that the systematic capture of communications data and personal profiling were severe infringements of human rights.
Dr. Claus-Dieter Ulmer: Although both court rulings are related to violations on the part of the government, they also directly impact businesses. Many of the current threats to informational self-determination stem from enterprises. The business models of a number of global Internet players are based on the large-scale collection, analysis and marketing of personal data.

But people who use Google, Facebook or smartphone apps do so by choice. What's the problem?
Dr. Claus-Dieter Ulmer: The problem is the total loss of control over one's own data. Everyone knows that whatever data they enter on social networks is more or less public – and that companies can, to a large extent, leverage the information for their own purposes. But what exactly is done with the data, how data is combined and aggregated, and how it is sold, and to whom and why – users do not know the answers to these questions. However, everyone should know what businesses do with their data, and have the right to decide what is acceptable. When a user simply signs off on a carte blanche agreement to unknown forms of analysis they lose their informational self-determination.

Would you like to ban social media and apps, then?
Dr. Claus-Dieter Ulmer: No, it is not about imposing bans. It is about raising awareness, achieving greater transparency, and striking the right balance between competing interests. There are a number of extremely useful apps, and search engines grant visibility into the infinite depths of the Internet. But we don't know, for example, what algorithms Google deploys to analyze personal data. Above all, commercial interests are pulling the strings. And I'm not just talking about analysis for targeted product advertising. We don't know whether data is sold and to whom – perhaps to banks, to verify credit worthiness. Or to insurance companies looking for signs of 'expensive' diseases. Even users who feel they have 'nothing to hide' may be at risk of losing their digital autonomy without even noticing.

And how can we achieve greater transparency?
Dr. Claus-Dieter Ulmer: Before I relinquish my data I should know exactly what is going to happen to it. Disclaimers should not hand over carte blanche. Instead, they should specifically describe what data is going to be used for. And it's relatively simple to implement on websites, by means of pop-ups or clearly visible links to disclaimers and easily understood consent forms. Deutsche Telekom has already done exactly that for its own products and services. And by taking the initiative in this way, we've won our customers' trust.

Surely personal data can be anonymized for analysis?
Dr. Claus-Dieter Ulmer: There are many insights to be gleaned from anonymized data. And this form of analysis is perfectly legitimate. Even before the digital age, surveys were leveraged to establish how to best advertise a product in a certain environment. Privacy can also be maintained by utilizing pseudonyms. And we should broaden the scope of what is allowed in this regard.

Profiling is performed to tailor products and services to the individual, or at least to their putative profile. This can lead to a situation where the only adverts we get to see are the customized ones. This, too, can lead to a loss of informational self-determination. Moreover, in the long run it could even endanger the plurality of political opinions. And none of us would want that to occur.

ABOUT THE INTERVIEWEE

Dr. Claus-Dieter Ulmer
has been Senior Vice President, Group Privacy, at Deutsche Telekom since 2002. He previously held overall responsibility for data protection at T-Systems International and its forerunner debis Systemhaus. Dr. Ulmer has a doctorate in law, and practiced as an attorney, specializing in commercial law.

NETWORK-CENTRIC SECURITY

How will the market for IT security products and services evolve in years to come? The German Federal Ministry of Economics and Technology most optimistic projections suggest that market volume will more than double between 2013 and 2020 – from 10.6 billion to 26.4 billion euros. Thomas Tschersich, SVP Security Services at Deutsche Telekom, believes the market's characteristics will change, too.

Mr. Tschersich, IT security has always been a major issue for businesses, and not just in the wake of the Edward Snowden revelations. Despite this, the market remains relatively sluggish. Why is that?
Thomas Tschersich: Many businesses still think of IT security only as an expense, not an investment. This perception persists, despite the soaring financial damage caused by cybercrime and online espionage. Many only acknowledge the risks when it's too late – shutting the stable door after the horse has bolted.

Many companies have been using antivirus software and firewalls for years. Could that be a factor?
Thomas Tschersich: The market is almost saturated – at least for business customers. However, many consumers remain remarkably vulnerable. And companies, too, must ask themselves if a software-based IT security solution genuinely meets their needs. Yes, it will intercept widespread, generic viruses and worms – but if professional attackers have you in their sights, standard software will offer very little resistance.

What should businesses do?
Thomas Tschersich: In the future, proactive monitoring of IT security will be absolutely vital. IT professionals cannot afford to wait and see if their defenses will hold – they must survey the landscape around them and eliminate potential threats. This also ties into the development of virtual desktops, and the increasingly mobile nature of our work and everyday lives. Software, data and processing power will continue to be migrated to the cloud. Today, we have thin clients such as tablets that are little more than terminals with a connection to the network.

How should we defend ourselves against cyber attacks and hackers?
Thomas Tschersich: Moving forward, network providers, such as Deutsche Telekom, will assume greater responsibility for this task. Practically all the data that businesses and consumers exchange has to pass across our networks. People and organizations use our networks to access websites, receive emails and watch TV – so keeping transmission paths 'clean' is a must. In other words, IT security is becoming increasingly network-centric. We need to keep our networks 'clean' today and every day – for our own sake. But in the future, we will be rolling out this security service to our customers as well. This will free them of the responsibility for – and challenge of – managing their IT security. Customers will be able to add security features to their basic protection package as easily as they add extra bandwidth today.

Can you name any examples?
Thomas Tschersich: We offer protection against distributed denial of service (DDoS) attacks. DDoS overloads – and ultimately cripples - web servers or entire networks. This paralyzes any business that operates an online shop or offers web-based customer services. In the worst cases, this situation can persist for days – leaving companies susceptible to blackmail. The frequency of DDoS attacks has risen significantly in recent times.

But firewalls intercept these attacks, don't they?
Thomas Tschersich: DDoS assaults are immensely powerful – at their peak, they can inundate targets with up to 400 gigabits of data per second. Firewalls can block some of this traffic at the access points, so the server itself stays online, but the transmission paths are still completely overwhelmed – rendering online services inaccessible to all. So while the firewall has done its job, at least on the face of it, the online shop will still be out of action.

How can Deutsche Telekom thwart the DDoS threat?
Thomas Tschersich: We can intercept DDoS attacks in our backbone: our fiber-optic network. If we discover that a hacker has targeted certain IP addresses belonging to one of our customers, we redirect the incoming deluge of data. In other words, we fend off the onslaught before it reaches the customer's firewall. This type of interception is only possible in the backbone. In the future, we will offer security services of this nature to combat other attack vectors.

A type of security-as-a-service, then?
Thomas Tschersich: Security is part of the package our customers receive. For example, our Magenta Eins package offers both landline and cellphone services – and in the future the basic security level may be included as standard.

Does that mean customers no longer need antivirus software?
Thomas Tschersich: Only if they run their entire business online. If they still use desktop PCs with USB ports and DVD drives, they remain vulnerable to infections that we, as a network provider, cannot prevent. As a result, they still need security software to safeguard their systems. However, the trend is clear – for example, many smartphones and tablet PCs have no local interfaces at all.

ABOUT THE INTERVIEWEE

Thomas Tschersich
is Senior Vice President, Group Security Services, at Deutsche Telekom. As an electrical engineer, he took over as head of IT security and information protection in 2000. Since 2001 he has handled technical security issues at federal and state ministries and public authorities in a wide range of advisory capacities.

CYBERCRIME AND GEOPOLITICAL CRISES

In early November 2014, representatives of the German government, the EU, NATO, the US administration, plus senior executives from leading international businesses, met at Deutsche Telekom's headquarters in Bonn. It was the third time they had convened to discuss digital dangers and defenses in an increasingly interconnected world. The summit was jointly organized by the Munich Security Conference and Deutsche Telekom – to address issues such as critical infrastructure, data protection, privacy, public awareness, and crime prevention.

The some 180 attendees included Brigitte Zypries, Parliamentary State Secretary at the Federal Ministry for Economic Affairs and Energy, and former Federal Minister of Justice, responsible for German government policy in the digital space; Sorin Ducaru, Secretary General of NATO, responsible on behalf of the alliance for new security challenges; Elmar Brok, Chair of the European Parliament's Committee on Foreign Affairs, Christopher Painter, US State Department Coordinator for Cyber Issues; and Ben Wizner, US attorney, data privacy expert, and Edward Snowden's legal representative.

"We have little choice but to acknowledge that warfare as a political tool has made a comeback in Europe. This has far-reaching ramifications for cyber security. Today's Internet communications infrastructure is being exploited to create confusion amongst opponents and to spread propaganda."
Wolfgang Ischinger
Chair of the Munich Security Conference

"Our goal of making Germany a European leader in digitization is impossible without IT security."
Brigitte Zypries
Parliamentary State Secretary at the Federal Ministry for Economic Affairs and Energy

"States and businesses are increasingly dependent on IT, and as a result they are even more vulnerable, and ever more susceptible to manipulation – this includes infrastructure paralysis."
Elmar Brok
Chair of the European Parliament's Committee on Foreign Affairs

"There is remarkable confusion surrounding roles and responsibilities with regard to how our political leadership addresses cyber warfare – at national, European and multinational level."
Karl-Theodor zu Guttenberg
Chairman of Spitzberg Partners LLC

"Faced by the threat of nuclear weapons, countries came together and agreed to forgo certain actions and to sanction others. A similar approach to cyber warfare is feasible."
Christopher Painter
US State Department Coordinator for Cyber Issues

"There is little sense in pursuing a security strategy that focuses exclusively on maximizing the volume of data collected to generate a single hot lead."
Clemens Binninger
Chair of the Parliamentary Control Panel (the body responsible for monitoring the work of German intelligence agencies)

"I am more concerned by the data German citizens willingly disclose in cyber space. They fail to recognize the dangers. This is not the fault of data protection legislation. They themselves consent to their data being processed."
Klaus-Dieter Fritsche
State Secretary at the Federal Chancellery and Federal Government Commissioner for the Federal Intelligence Services

"Unfortunately, it does not get easier to find a needle in a haystack when you build the world's largest haystack," states Snowden's attorney **Ben Wizner** with regard to the efficacy of collecting vast volumes of data.

"I know that you are afraid we may be accessing your communications and stealing your data. If this fear is realized, then the digital economy will collapse like a house of cards."
Ciaran Martin
Director General for Government and Industry Cyber Security at GCHQ

"On both sides of the world the belief exists that we are already engaged in a cyber war, and that economic warfare is a permissible and necessary means to further a nation's wellbeing."
Elmar Theveßen
Deputy Editor-in-Chief of German public TV broadcaster ZDF

SECURITY AND DIGITAL LITERACY

In November 2014, Deutsche Telekom hosted the very first major security gathering aimed specifically at children and young people. The event took place at the company's headquarters in Bonn, and is one of a variety of projects and initiatives designed for improving digital literacy. It highlighted both the opportunities and perils of the Internet age.

On November 3, 180 representatives of the German government, the EU, NATO, the US administration and top executives of leading international corporations met in Bonn to discuss digital dangers and defenses in a hyperconnected world. Just a day later, Deutsche Telekom played host to the Cyber Security Summit for Kids. Attended by 200 children and teenagers, this unique event brought unaccustomed sights and sounds to the corporate HQ. The entire Board of Management was present, fielding a range of intelligent questions from the youthful delegates.

As Timotheus Höttges, Chairman of the Management Board, stated: "The much cited digital native generation needs to acquire self-reliance with regard to the risks inherent to the Internet age; they need to learn how to deal with them responsibly. That is the way to create a future-proof, secure digital society." Deutsche Telekom's most senior executive discovered that many youngsters are already wise to the perils. When he asked a school student to reveal his smartphone password, he encountered an immovable obstacle: "No way. It's my secret, and it's no one else's business."

The very first Cyber Security Summit for Kids also honored the winners of a nationwide competition to foster digital literacy (named Medien, aber sicher!). The award program was organized by Deutsche Telekom in association with leading German daily Die Frankfurter Allgemeine Zeitung (FAZ). The aim is to identify projects that raise young people's awareness of both the perils and opportunities associated with digital media. The judges were particularly impressed by an elementary school in Wurmlingen, in the State of Baden-Württemberg. The nine-year-olds of the fourth grade proved to be highly adept researchers: they gathered relevant information on Internet-related issues, and developed their own assessment form for identifying child-friendly web content.

TEACH TODAY

TeachToday is a Deutsche Telekom initiative designed to promote Internet skills. It provides guidance on how to foster the safe and effective use of new information and communications technologies, and of online content. It includes concrete tips and tailor-made resources. TeachToday helps teaching staff, school administrators, social workers, parents and students to maximize the benefits of digital media, without succumbing to the pitfalls.

teachtoday
Lernen neu denken

What are the educational issues we face in the world of bits and bytes? They include the use of handheld devices in classrooms, privacy, intellectual property rights, and more. How can students and teachers harness digitization for their purposes and goals? The slogan of the TeachToday initiative is 'rethink learning' (Lernen neu denken), and it helps stakeholders to unleash the potential of new media and online content, and to manage the corresponding challenges.

The website, www.teachtoday.de, offers tools for and advice on diverse topics, such as data protection and security. It includes innovative resources in school-friendly formats that make use of today's possibilities to combine education with entertainment. The documents on data protection and security are suitable for classroom use, for parent-teacher events, or for sharing with colleagues in the world of teaching.

VIRTUAL OBSTACLE COURSE

At the Cyber Security Summit for Kids, 200 children, aged nine to twelve, tackled a virtual obstacle course designed to improve their digital media skills in a fun fashion. It comprises five sets of educational and entertaining exercises, providing information on many aspects of digital media usage. The course also addresses issues such as the time children spend playing games, data protection and cyber bullying. Starting in early 2015, Deutsche Telekom will make the resource – reminiscent of a jump-and-run computer game – available to schools free of charge.

SUPPORTING CHILD-FRIENDLY CONTENT

Deutsche Telekom also supports Ein Netz für Kinder, a German government program that funds high-quality online content specifically for children. The aim is to encourage youngsters to learn the safe use of digital media. The initiative supports child-appropriate websites and moderated forums where boys and girls can experiment with social networks in a safe environment.

ein netz für kinder

Within the framework of Ein Netz für Kinder, companies and associations have created **www.fragFINN.de**, a search engine designed for children between six and twelve years of age. It provides them with a child-friendly gateway to the Internet with a whitelist of a wide variety of safe, interesting websites; these are vetted according to a set of criteria defined by experts. “It's difficult to find websites suitable for children using conventional search engines. In addition, inadvertently accessing inappropriate content is all too easy,” explains Fritz-Uwe Hofmann, Deutsche Telekom's representative for the initiative. “Ein Netz für Kinder is part of Deutsche Telekom's wholehearted commitment to every aspect of data protection and security.”

“WE NEED TO LEVEL THE PLAYING FIELD”

Jan Philipp Albrecht, a member of the European Parliament, believes that the EU General Data Protection Regulation will be passed in 2015. This will prevent companies from evading data protection legislation to gain an unfair competitive advantage.

The European Parliament, Commission, and Council of Ministers are hard at work on the EU General Data Protection Regulation. The EU-wide standard for data protection is expected to pass in 2015.

Mr. Albrecht, what is the current status of negotiations on the EU General Data Protection Regulation?

Jan Philipp Albrecht: Despite nearly three years of discussions, and a comprehensive position statement on the part of the European Parliament, there seems to be a need for further clarification within the Council of Ministers. The Council did not present a mandate for negotiations in 2014; there won’t be a complete position on their part before June 2015. Should, by then, the Council not have expressed its willingness to enter into negotiations with the European Parliament, it is highly unlikely that the General Data Protection Regulation will pass in 2015. That would be detrimental for everyone – for consumers and companies in the European market.

With so much discussion, is there a danger of arriving at a compromise that is simply the lowest common denominator?

Jan Philipp Albrecht: The European Parliament has agreed on a compromise that is anything but the lowest common denominator. This compromise holds companies that process personal data to the highest standards in terms of data protection rights and duties of the individuals – in part, higher than German standards. The whole thing includes clearly defined principles, and clearly defined procedures for data protection agencies, ensuring a high degree of legal certainty. These standards can be enforced through robust sanctions, based on the sanctions employed under EU legislation governing anti-competitive practices.

Why do some countries seem so reluctant to support a shared European approach to data protection?

Jan Philipp Albrecht: Resistance is being felt from countries that are under pressure from certain companies operating in their markets – companies that have specifically chosen to locate their headquarters in countries with somewhat lower data privacy principles, and whose data protection agencies lack adequate resources, currently giving them a competitive advantage. The majority of EU member states wish to eliminate this unfair competitive edge. Against this background, the EU General Data Protection Regulation is possibly the most important, largest step towards establishing a platform with worldwide impact – one that could also lead to a change in the mindset of major global players.

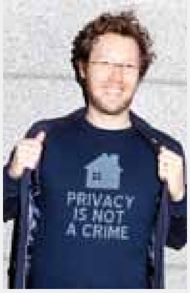
Isn’t there a danger of international companies finding ways to evade European data protection legislation?

Jan Philipp Albrecht: We want to level the playing field in the European market. Each company based in the European market will then have to play by the same rules. This applies equally to businesses not based in the EU. For example, if an enterprise is headquartered in India, and offers products or services, such as cloud services, to customers in Europe, then that company must also comply with European data protection legislation. Otherwise, they will face substantial penalties of the type that already work effectively under current legislation governing anti-competitive practices.

Or companies could simply pull out of the European market.

Jan Philipp Albrecht: The EU is the largest single market in the world. Large Internet and IT providers cannot afford to simply pull out – they will instead consider whether they should adopt the EU standards in their countries. This could raise the bar in other countries, and could ultimately lead to a global standard.

ABOUT THE INTERVIEWEE



Jan Philipp Albrecht,
was born in 1982, grew up in Wolfenbüttel, and studied law. Since 1999, he has been a member of the Greens, and since 2009, the youngest German member of European Parliament. He is Vice-Chair of the Committee on Civil Liberties, Justice and Home Affairs and Substitute Member of the Committee on the Internal Market and Consumer Protection. During his first legislative period, from 2009 to 2014, he was a member of the Committee on Legal Affairs. Jan Philipp Albrecht was also the Coordinator of the Special Committee on Organized Crime, Corruption and Money Laundering from December 2012 to October 2013.

You mentioned that the German government will be actively, constructively participating in negotiations. What did you mean?
Jan Philipp Albrecht: The federal German government took nearly two years to recognize the Data Protection Regulation as proposed by the Commission. Previously, the government had primarily promoted voluntary commitments on the part of the business community. This was diametrically opposed to the Commission's proposal, and to the position and broad will of the European Parliament. The overall impression was that the German government was drawing the issue out; this has sown distrust and had a negative impact on the process as a whole.

You said the EU General Data Protection Regulation is even stricter than German data protection legislation?
Jan Philipp Albrecht: In some instances, the regulation goes a step further than German legislation, in terms of consumer protection, improved transparency and legal certainty. In recent years, particularly when it comes to user consent, the degree of protection has been eroded. Significant exceptions to consumer consent requirements have been made in the interests of direct marketing. This resulted in a lack of transparency with regard to data protection practice, and in effect allowed businesses to evade statutory requirements.

We Germans now have a tendency to condemn the way Americans handle data. Are Europeans totally innocent?
Jan Philipp Albrecht: No, not at all. The collection and utilization of personal information has become far more common in Europe, as well. European companies are just as guilty of forgetting, amid the gold rush, that there are some ground rules and values that they simply shouldn't ignore. And, by the same token, there are many companies in the USA that are highly committed to upholding legislation on data protection and privacy.

How does it benefit us if we reach a consensus in the EU, but the problem persists with countries such as the USA or China?
Jan Philipp Albrecht: We can only establish a transatlantic – or even global – standard if we do our own homework first. Only when we have achieved harmonized, clearly understood legislation in Europe will we be in a position to discuss transatlantic data protection.

In your discussions with representatives of Google and Facebook, do you feel that they are beginning to see your point of view – that data should be handled differently?
Jan Philipp Albrecht: Absolutely. Over the last five years, I have travelled to Washington and Silicon Valley regularly. I held in-depth discussions with companies and with representatives of congress. My impression is that, at the beginning, it was quite challenging to bridge the transatlantic gap with regard to personal information and privacy. However, now, they now have a far better understanding of the European approach to these issues. Major corporations are modifying their attitudes as they come to realize that data protection and security are decisive business success factors.

Quite honestly, will the regulation be in place by the end of 2015?
Jan Philipp Albrecht: I'm an optimist, therefore I am sure we will definitely pass the regulation this year. Two years later, a Europe-wide standard will be in force. For that to happen, the Council of Ministers must reach an agreement early this year – which will only happen if the companies ramp up the pressure on the German and other governments in the Council.

Jan Philipp Albrecht has been campaigning for harmonized EU-wide data protection legislation for a number of years.

Within this context, do you think Deutsche Telekom's Data Protection Advisory Board is a good idea?
Jan Philipp Albrecht: Deutsche Telekom has given firm assurances that the Data Protection Advisory Board is fully independent, and is not simply a PR stunt – it is truly an effective body designed to improve data protection practices. In my opinion, it is a bold, entirely correct and necessary step. It sets an excellent example for all companies of this size and type in Europe. I do hope that many others follow suit. For Deutsche Telekom, the Data Protection Advisory Board is a huge leap forward. It could become the gold standard for online data and consumer protection.

CRITICAL WATCHDOG

Deutsche Telekom's Data Protection Advisory Board provides expert guidance to the Board of Management. It also actively encourages dialogue with external specialists on current data protection and security issues. These exchanges involve thought leaders in politics and business, and at universities and NGOs.

The board's remit is broad. It encompasses business models and processes relating to customer and employee data, IT security, and the effectiveness of implemented solutions. The body also addresses international aspects of data protection, and the implications of new legislation.

Its responsibilities include vetting data protection and security measures at Deutsche Telekom in general, and submitting pertinent proposals to the Board of Management and Supervisory Board. In addition, the Board of Management may proactively request the Advisory Board's opinion on relevant processes. Moreover, the Advisory Board addresses data protection and security issues upon its own initiative, and makes recommendations to the Deutsche Telekom Board of Management.

The Advisory Board convened four times in 2014. Key topics included assessment of data protection and security in mobile payment services, anonymization for big data, the Qivicon Smart Home platform, and collaboration with Mozilla on the introduction of data-protection-friendly smartphones.

CURRENT MEMBERS OF THE DATA PROTECTION ADVISORY BOARD:

Jan Philipp Albrecht
Member of the European Parliament, Vice-Chair of the Committee on Civil Liberties, Justice and Home Affairs, Substitute Member of the Committee on the Internal Market and Consumer Protection, rapporteur of the European Parliament for the General Data Protection Regulation

Wolfgang Bosbach
Member of the CDU, Member of the German Bundestag, Chairman of the Committee on Internal Affairs

Peter Franck
Member of the Chaos Computer Club (CCC)

Prof. Hansjörg Geiger
Guest Professor of Constitutional Law at Goethe University in Frankfurt am Main, State Secretary of the Federal Ministry of Justice and Consumer Protection from 1998 to 2005, President of the Federal Office for the Protection of the Constitution from 1995 to 1996, President of the Federal Intelligence Service from 1996 to 2005

Prof. Peter Gola
Honorary Chairman of the German Association for Data Protection and Data Security (GDD), author and co-author of numerous publications on German data protection legislation

Bernd H. Harder, attorney at law
Member of the Management Board of BITKOM, professor at the Stuttgart University of Media (HdM) and Munich Technical University (TUM)

Gisela Piltz
Member of the Executive Committee of the FDP, Deputy Chair of the FDP in North Rhine-Westphalia

Gerold Reichenbach
Member of the SPD, Member of the German Bundestag, Member of the Committee on Internal Affairs (rapporteur for data protection and privacy, civil protection and disaster management)

Dr. Gerhard Schäfer
Presiding Judge at the Federal Court of Justice (BGH), retired

Lothar Schröder
Chairman of the Data Protection Advisory Board, Member of ver.di's Executive Committee, and Deputy Chairman of the Supervisory Board of Deutsche Telekom

Halina Wawzyniak
Member of Die Linke, Member of the German Bundestag, Spokesperson of the Bundestag Committee on Legal Affairs and Consumer Protection

Prof. Peter Wedde
Professor of Labor Law and Law in the Information Society at Frankfurt University of Applied Sciences, Director of the European Academy of Work in Frankfurt am Main

MANDATE EXTENDED FOR THE DATA PROTECTION ADVISORY BOARD

In late 2014, Deutsche Telekom's Board of Management decided to extend the Data Protection Advisory Board's mandate by a further two years. The board, comprising external experts, has been fulfilling an important role since its inception some six years ago. It has produced tangible results, with 148 concrete recommendations emerging from 28 meetings. Its members examine new business activities, and consider how Deutsche Telekom stores and processes data. "We take a long, hard look at the company's business models, products and processes; this enables us to provide informed advice on data protection," says Lothar Schröder, Chairman of the Advisory Board and Deputy Chairman of Deutsche Telekom's Supervisory Board. Thomas Kremer, Member of the Board of Management for Data Privacy, Legal Affairs and Compliance, explains the thinking behind the renewed mandate: "We live in an age of M2M communications, digitization of manufacturing processes, and big data analysis; this is leading to new business models. Against this background, the insights and advice of external experts are essential." The board, comprising 12 members, has recently made a new appointment – Peter Schaar, former Federal Commissioner for Data Protection. "Deutsche Telekom now enjoys the highest level of customer trust within the industry. We wish to play our part in maintaining and extending this leadership," states Lothar Schröder.

TRUST IS KEY TO BUSINESS SUCCESS

Trust is vital to long-term business success – in the digital age more than ever. As **Lothar Schröder**, Deputy Chairman of the Supervisory Board at Deutsche Telekom, explains, the trust of customers and partners is essential; but the trust of employees in their employers is equally important.

Which companies do you trust the most when it comes to handling your personal information? This very question was posed in a representative survey of the German population carried out by the Allensbach Institute in mid-2014. As someone who has been an advocate of robust data protection at Deutsche Telekom for many years, I was not surprised by the findings. When Germany's leading telecommunications and Internet providers are judged on trustworthiness, Deutsche Telekom comes out well ahead of the rest. In fact, our lead over the competitor in second place has extended significantly year-on-year.

Deutsche Telekom's Data Protection Advisory Board and the Group's senior executive management are wholeheartedly committed to the protection of customer and employee data. Edward Snowden's revelations of the extent to which governments monitor all types of communications data – even tapping political allies' cell phones – generated widespread dismay. Against this background, the Data Protection Advisory Board and the Group's top executives have redoubled their efforts to improve data protection and security. This commitment is reflected in the Allensbach Institute's positive findings.

NO RESTING ON LAURELS

As satisfying as these results are, we cannot not rest on our laurels. Almost half of the German population recognizes Deutsche Telekom's trustworthiness – but an equal number expressed no opinion at all. If we are to change this situation, we need to send out a clear message: data protection is one of our absolute top priorities.

German data protection legislation is among the strictest in the world. At the same time, we have, for a number of years, worked hard to improve provisions in two specific areas – but unfortunately in vain. In today's globalized digital world, data protection is a task that transcends national borders.

The urgent need for the much debated EU General Data Protection Regulation has existed for a number of years. The regulation is a recurring topic of discussion. It is a prerequisite for establishing harmonized legal requirements – and obligations – throughout the European Union, and perhaps beyond. Additionally, as digital business models grow more prevalent, we need the regulation in order to level the playing field within the economy as a whole.

EMPLOYEE DATA PROTECTION

Moreover, in Germany, we need a law specifically for employee data protection. Many generic provisions in existing data protection laws are not applicable to employee-related personal information. Such dedicated legislation must guarantee a high degree of protection, but strike the right balance between the legitimate interests of the employer and the privacy rights of the employee. There are still many legal uncertainties for example in the context of video surveillance, liability, biometrics, handling the information of job candidates, and data gleaned from social media.

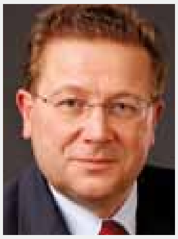
Furthermore, employee representatives need to be given a greater say, as do data protection officers. And a legal basis for class action is required.

Companies need to clearly understand the constraints placed on their activities by data protection. To date, many issues have not been specifically addressed in German legislation, but handled on a case-by-case basis by the courts; a clear legislative framework must be put in place.

INTERNAL POLICY NEEDED

For employees, the ongoing lack of specific employee data protection legislation is a keenly felt grievance. Against this backdrop, it is all the more important that companies, at the very least, agree on an internal policy with their staff. In this context, I regret that Deutsche Telekom's senior management was unable to submit a proposal that found the approval of employee representatives in 2014. A balanced policy, agreed upon in a spirit of fairness by employer and employees, would underscore the company's commitment to data protection – with no ifs or buts. I am convinced that this would further increase the trust partners, employees and the general public place in Deutsche Telekom.

ABOUT THE AUTHOR



Lothar Schröder
is the Deputy Chairman of the Supervisory Board at Deutsche Telekom. In April 2006, he was appointed to the Executive Committee of ver.di, a major labor union, where his responsibilities include telecommunications and IT.

ASSUMING JOINT RESPONSIBILITY

Responsibility, self-determination and independence are integral to freedom – in both the analog and the digital worlds. If Germany and Europe wish to exert their sovereignty in cyberspace, their data protection and security objectives need to be reflected in their legislative framework.

Trust is the bedrock of our business. When it comes to data protection and security, customers put more stock in Deutsche Telekom than in any other Internet service provider – and yet we have to earn this trust anew every day.

Digital services will not be used if users feel their personal data is not adequately protected. And in the past year, fundamental faith in a secure cyber space was repeatedly put to the test. Misgivings lead to reduced revenue and stymied growth – especially for new offerings, such as cloud services.

PULLING IN THE SAME DIRECTION

To build trust, the ICT industry must assume joint responsibility for greater security. To this end, all market participants must pull in the same direction, and comply with minimum standards. This applies to us as a network provider, and to all other organizations offering services and products within the online landscape. Unfortunately, this imperative has not received due attention during discussions on the proposed IT security act in Germany and the EU network and information security directive.

To date, obligations have only been placed on network providers. However, achieving robust protection requires all players to be obligated to play their role. This applies to hardware and software vendors, and to Internet service providers, in particular. These actors have – without persuasive justification – not been addressed by the scope of the proposed legislation with the necessary clarity.

DEFINING A EUROPEAN FRAMEWORK

The status quo leaves a large portion of Internet traffic unshielded. The providers of services, including email, cloud offerings and social networks, process the lion's share of Internet data. It is therefore only logical to impose direct obligations on them, too, to comply with minimum standards.

The same applies to hardware and software vendors – whose products, when manipulated, are often the gateway for attacks. It makes sense to mandate these vendors to provide security updates, and to therefore play their part in overcoming vulnerabilities. Only when the ICT industry as a whole assumes collective responsibility can we achieve our goal of greater digital security. It

> “WE MUST EMPOWER PEOPLE’S DIGITAL SELF-DETERMINATION”

makes no sense to make exceptions for service providers, and hardware and software vendors.

Although the Internet is a global phenomenon, it is subject to diverse national and regional legal systems. This was particularly evident in transatlantic relations in recent months: conflicting attitudes toward data protection, and toward the right balance between personal liberty and public security, have become very apparent.

Europe has to forge its own path – because a global consensus on all relevant legal issues is wishful thinking. Even where there are established multilateral agreements, for example on mutual legal assistance, these have been ignored. For Europe, with its shared values (with regard to both society and the business community), it is more practical to first lay down the ground rules for its own legal sphere – rules to which all actors, regardless of their origin, must comply.

INCREASED INDEPENDENCE IN EUROPE

This has nothing to do with isolationism, marginalization or protectionism. It is an expression of sovereignty, of autonomy, of the desire to define a framework for the digital world that reflects European values, that embodies what we believe in and rejects what we do not. At the same time, we are eliminating country-specific provisions. The proposed European General Data Protection Regulation is an essential step. It establishes overarching legislation for all digital services in the EU – even when these services are provided for European citizens by a player based overseas.

Europe must reassert its sovereignty, its autonomy, in cyber space. This requires both standardized EU legislation and the ability to develop and, when necessary, locally produce our own software and hardware. This includes establishing secure and innovative IT systems, and secure data transmission paths, as the foundations for the future digital development of our society. And it entails promoting research and development, for example to create leading-edge, trusted high-tech solutions in key areas, such as network components.

RECOGNIZING POTENTIAL THREATS

We must identify those areas that are of importance to our security, and to our industrial viability. In this context, it is not just purely technical skills and resources that are important – each individual citizen must acquire the digital literacy needed to apply them. We must empower people’s digital self-determination. This means more than just the ability to use digital media; citizens need to be able to critically evaluate security issues and recognize potential threats.

Europe’s digital autonomy requires huge effort and considerable investment in the research and development of IT solutions, and in education and training. European enterprises are already doing a great deal in this regard. However, governments need to become more actively involved. The experience of other successful economic regions in the world has shown: we need government-funded lighthouse projects.

ABOUT THE AUTHOR

Wolfgang Kopf, LL.M.
Senior Vice President, Public & Regulatory Affairs, since November 2006. His role includes the representation of national and international political interests, and association, media and spectrum policy in addition to general regulatory issues. He studied law and humanities at the University of Mainz, the German University of Administrative Sciences in Speyer and the University of London.

BREAKING DOWN BARRIERS TO COOPERATION

Cybercrime rates are skyrocketing, rising faster than for any other felony. Yet the percentage of cases solved remains low. To successfully track down and prosecute cyber criminals, law enforcement authorities need to establish and extend dedicated units, and facilitate close cooperation between these teams and the corporate sector.

If law enforcement officers are to prevail, they will have to overcome operational, organizational, technological and legal challenges.

A few years ago, cybercrime – broadly understood as all offences committed by means of modern information and communications technology, or targeting ICT systems – was simply a footnote in police statistics. But this has changed. No other type of crime has seen incidents rise as rapidly in recent times, with the latest figures revealing double-digit growth rates for certain felonies. Moreover, there is almost certainly a huge degree of underreporting.

IT has become increasingly central to our private and professional day-to-day activities, and our lives are becoming ever more connected. As a result, there are unprecedented possibilities for manipulating data and attacking IT systems. It seems the only way for cybercrime rates to go is up – with severe consequences for the wider economy. A 2013 study published by Internet security provider McAfee and the Center for Strategic and International Studies (CSIS) estimates that black hats cost the global economy half a billion US dollars each year. Others have put this figure even higher.

A CHALLENGE FOR LAW ENFORCEMENT

As cybercrime has mushroomed, it has rapidly moved up the list of priorities for law enforcement agencies. Yet success rates in prosecuting perpetrators are below par when compared with more traditional felonies. Jörg Ziercke, former head of the German Federal Criminal Police Office (BKA), voiced concern in a recent interview in light of around 70 percent of cases remaining unsolved. And Thomas Kutschaty, Minister for Justice in the State of North Rhine-Westphalia (NRW), recognized the increasingly complex and multifaceted nature of cybercrime when he labeled it the “greatest challenge facing law enforcement”. These highly professional criminals often band together in organized gangs. They are innovative, adaptable, and deploy the very latest technologies in their ceaseless pursuit of new targets. Plus, they work globally. National borders pose no obstacle, and there is often no relationship between where the criminals are based and where the victims are located.

This means that if law enforcement officers are to prevail, they will have to overcome operational, organizational, technological and legal challenges. The tried-and-trusted working methods, processes and organizational structures deployed by police and judicial authorities can be inflexible and overly bureaucratic; in the fast-paced Internet era, they struggle to keep pace. This is a problem, because when it comes to combating cybercrime, time is of the essence – it is vital to act before evidence disappears into the ether. The authorities only stand a chance if they can engage with cyber criminals ‘on their level’: in terms of expertise, innovation, agility and technical resources. And it appears that law enforcement bodies are starting to appreciate that the nature of their world has changed.

DEDICATED CYBERCRIME FIGHTING UNITS

The European Cybercrime Center (EC3) opened its doors in early 2013, with the aim of strengthening cooperation between the agencies of EU member states.

Moreover, with Europol launching a Joint Cybercrime Action Taskforce (J-CAT) in September 2014, the continent has benefited from a new, cross-border unit in the fight against online criminals. J-CAT is tasked with coordinating the international investigations of participating countries, with the Europeans joined by Canadian and US representatives.

In Germany, too, dedicated units have sprung up in police organizations and public prosecutors' offices in recent years. At national level, a special-purpose cybercrime investigation group has been put in place. While at state level, a central competence center has been up and running at the Criminal Police Office of NRW since 2011, providing a central point of contact for all issues related to cybercrime. The Criminal Police Office of Saxony has followed suit, as its own specialist statewide unit set to work in June of last year.

Judicial authorities at state level have also taken action to ramp up the fight against cyber crime and taken targeted steps, particularly with the aim of streamlining cooperation between police and public prosecutors. Frankfurt's public prosecutor's office led the way back in 2013 with the establishment in Giessen of the Hessian Central Agency for Combating Internet Criminality (ZIT).

CLOSE COLLABORATION

In Cologne, the public prosecutor's office set up a Central Cybercrime Agency and Contact Point (ZAC) in January of last year, to complement and support the work of the competence center at NRW's Criminal Police Office. At present, these specialist units at state level are still in the pilot project phase. But as it is clear that crime-fighting in cyber space requires dedicated teams of experts, the hope is that other federal states will soon follow the example of NRW, Hesse and Saxony.

The above points address the working methods and processes of police and judicial authorities. But the same insights apply to interaction and communication between law enforcement agencies and the enterprises that fall victim to attacks. Here, too, an overhaul is overdue. Today, an employee phoning to report a crime may well have to display exceptional patience as he is transferred from department to department, before getting through to a contact with the necessary expertise and authority. Or a company representative might have to physically go to the nearest police station or prosecutor's office to file a formal complaint in writing. In either case, it is unlikely that the authorities will be able to collect evidence in time to identify and pursue the perpetrators.

OVERCOMING RESERVATIONS

For legal and other reasons, the chances of convicting cyber criminals have been small to date. To maximize the likelihood of success, companies need to take the initiative. First of all, it is essential that they overcome any reservations they may have with regard to collaborating with the police and judicial authorities. Secondly, they can benefit from establishing good and close relations with the dedicated cybercrime fighting units already in existence, particularly at local level. They should, even before a crime has been committed, explore with the authorities the options and methods available for tracking and prosecuting offenders, and how best the two sides can cooperate to achieve successful convictions.

Deutsche Telekom's Group Security Service unit regularly exchanges information with federal agencies responsible for information security – the Federal Criminal Police Office, the Federal Office for Information Security (BSI), the German Domestic Intelligence Service (BfV), and the Federal Office of Civil Protection and Disaster Assistance (BKK).

And the ICT provider's Group Criminal Law unit, responsible for matters of criminal law and prosecution, has been holding cybercrime workshops since 2013. These have been attended by employees from the competence center of NRW's Criminal Police Office, the ZAC of Cologne's public prosecutor's office, and the public prosecutor's office of the city of Bonn. Feedback has been positive, and law enforcement agents in particular have shown great interest – which is good reason to further intensify the exchange of information and experience with these stakeholders, and to continue promoting the establishment and expansion of dedicated units by police and judicial authorities.

ABOUT THE AUTHOR

Hans-Lucas Bauer has been Head of the Group Criminal Law unit at Deutsche Telekom since November 2004. Previously, the legal expert worked for the Ministry of Justice of the State of Baden-Württemberg, as a judge at civil law courts, and later as an attorney specializing in economic crime.

SECURITY IS FOR SHARING – STRONGER TOGETHER

In cyber warfare, skilled, well-equipped attackers often appear to have the edge. To stay one step ahead of their foes, enterprises must cooperate.

229 days – more than seven months: that is the average time it takes for a company to realize their IT systems have been compromised by a cyber attack. During this time frame, the attacker has the upper hand. He leverages the head start to his advantage, stealing critical information assets and manipulating business processes undetected.

Why does it take so long to identify cyber attacks? Established defense models have their limitations, since the criminals who pose the greatest threat remain under the radar while infiltrating networks. Firewalls and antivirus software are still valuable defenses, and will continue to provide base-line protection in the future, since they intercept generic mass-targeted attacks. However, they are only effective against threats and malware that display known patterns.

OBSERVATION AND ANALYSIS

Antivirus software engineers work 24/7, observing and analyzing the structure and behavior of new threats. They develop filters as soon as possible, and add them to their existing solutions. When everything runs smoothly, antivirus software users are shielded from new risks in a matter of hours.

However, these tactics alone are not effective against all potential risks. Increasingly sophisticated cyber attacks can only be countered by more advanced safeguards. Against this background, major businesses employ entire teams of security specialists who are on constant lookout for signs of intruders, and quickly address and resolve any issues. But any valuable insights gained by these teams are not generally shared with other enterprises. That's the nature of business, and of IT security – companies like to keep their cards close to their chest. This means that critical information is often only exchanged at conferences and similar forums, and not in the daily battle against cybercrime.

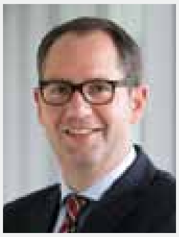
INFORMATION EXCHANGE IN REAL TIME

This situation needs to change. In November 2014, Deutsche Telekom launched an initiative to connect security experts from major corporations: CSSA (Cyber Security Sharing and Analytics). The platform is intended to be a point of contact for multiple enterprises and industries, allowing them to share information on cyber attacks in real time. Additionally, CIOs and corporate security experts alert their counterparts to current attack patterns and discuss potential defense strategies.

Until now, many enterprises have been reluctant to reveal that they have succumbed to a successful attack. The breach is only made public when, for example, the website or customer-facing business processes are paralyzed. Decision makers are afraid of negative publicity and the potential damage to reputations. To overcome this issue, CSSA members can share data on the platform anonymously.

The cyber security exchange platform offers tangible benefits: armed with privileged and timely information, participating organizations are better able to defend themselves. And they are living up to the values that the Federal Minister of the Interior hopes to promote through the proposed IT security act: greater transparency and increased cooperation for more robust security in the digital world.

ABOUT THE AUTHOR



Dr. Jürgen Kohr
is Senior Vice President of Cyber Security at T-Systems. He was previously Senior Vice President of Corporate Strategy at T-Systems, and managed the support team for Reinhard Clemens, a member of Deutsche Telekom's Board of Management. Committed to the development of new security products, Dr. Kohr is also a member of the investment committee for the infrastructure fund at T-Venture, Deutsche Telekom's venture capital subsidiary.

NO INDUSTRY 4.0 WITHOUT ROBUST DATA PROTECTION

The digitization of industry is transforming markets. And Germany is well placed to become a key player in this new era: an established leader in engineering, Europe's economic powerhouse also ticks the boxes when it comes to privacy and data security.

Reinhard Clemens, member of Deutsche Telekom's Board of Management: For manufacturing heavyweight Germany, the prospect of transforming production lines by means of machine-to-machine (M2M) technology offers a unique opportunity.

It's criminally simple: the software can be easily accessed online – and once a mobile connection is established, the industrial robot can be controlled remotely from a smartphone. Attendees at the 2014 Cyber Security Summit were taken aback to discover just how simple it is to manipulate numerically controlled manufacturing plant and equipment. This live demonstration by an expert from the German Federal Office for Information Security (BSI) left spectators in no doubt: there is much work to be done before we can herald the brave new era of connected manufacturing, known widely in Germany as the 'fourth industrial revolution' or 'Industry 4.0'.

For manufacturing heavyweight Germany, the prospect of transforming production lines by means of machine-to-machine (M2M) technology offers a unique opportunity. Thanks to the engineering prowess of its big-name corporations and the innovative agility of its midsize Mittelstand, few nations enjoy such a formidable reputation in the manufacturing sphere. Yet the Internet whirlwind that has swept the global economy in recent years has, with a few notable exceptions, bypassed the German business world almost entirely.

SECURITY MADE IN GERMANY

The digitization of production processes could be a game changer. The manufacturing sector is on the brink of a massive upheaval, with all the major players struggling to implement digital business models while upholding the hard-earned Made-in-Germany seal of quality. So who will emerge as the driving force of the Industry 4.0 era – the Internet juggernauts or the manufacturing titans? We shall soon know.

As digitization enters its second act, there are signs that Europe is set to move center stage. Already, two thirds of the embedded systems used to control industrial plant and equipment are produced in the EU – with Germany a clear leader in control systems, for example. But the big question is: how can manufacturers protect these automation technologies from the perils lurking in the wider Internet?

With the rise in cyber attacks on industrial facilities and critical infrastructures such as power plants and telecommunication networks, it has become clear how vital IT security is to making Industry 4.0 a reality. Vulnerabilities and hidden threats in control systems can have disastrous consequences for manufacturers. And a successful violation of critical infrastructure would have ramifications for the entire economy, not just for individual companies. The BSI's 2014 report on IT security in Germany describes an attack that deliberately targeted a German steelworks. Hackers manipulated networks at the facility, leading to the failure of control components and entire systems – causing severe disruption to mission-critical operations, including a key furnace.

EUROPE TAKES POLE POSITION

But fear is not a good companion for progress and innovation. Industry 4.0 offers great opportunities for Germany and Europe. The US and the former leading lights of the digital economy have lost the public's trust, in the wake of revelations of unbridled collection of personal information, and business models built on gathering, analyzing and selling customer data. As a result, security is now paramount to success. Long neglected by companies and consumers, privacy and data protection have become the cornerstones of fair business practice.

It will be a few years yet before Industry 4.0 is comprehensively established in the manufacturing sphere, and before products are digitized from end to end, across the entire lifecycle. This is where our opportunity lies. Cloud computing and M2M systems have laid the technical foundations. And with Europe's expertise in engineering, we are in pole position. But as we are all aware, being first on the grid does not make you a winner – there will always be others hot on your heels. We must move fast. To secure our competitive edge, Germany must rapidly make Industry 4.0 a reality while ensuring robust security.

ABOUT THE AUTHOR

Reinhard Clemens
has been the member of Deutsche Telekom's Board of Management responsible for T-Systems since December 1, 2007, and also holds the position of CEO of T-Systems. On January 1, 2012, he assumed responsibility of all Group IT.

MOTIONLOGIC'S BIG DATA ANONYMIZATION PROCESS

Berlin-based startup Motionlogic – a wholly-owned subsidiary of Deutsche Telekom – develops and markets self-learning analysis systems. Interpreting large volumes of data, these recognize patterns and correlations, streamlining and enhancing business processes.

Big data solutions process and analyze large volumes of information in real-time to gain valuable insights. However, this can raise privacy issues. To address these concerns, Deutsche Telekom has defined certain principles and rules for managing personal data within its own business intelligence projects. For example, only anonymized data may be processed – individuals cannot be identified.

The Group Privacy unit helps Motionlogic develop marketable offerings based on anonymized telecommunications data. Deutsche Telekom intends to combine this information with anonymous attributes, taken from customer databases. The results are then provided to Motionlogic. Multiple mechanisms have been deployed to ensure robust data protection across the entire process, ensuring the people behind the bits and bytes remain hidden. The startup leverages the data in a variety of ways, for example for traffic flow analysis – generating actionable information for businesses and urban planners.

In February 2014, Deutsche Telekom presented its anonymization method to the Federal Commissioner for Data Protection and Freedom of Information (BfDI). The initial response was positive, but formal approval had not been issued at the time of this report's publication, in early 2015. If the process is deemed lawful, Deutsche Telekom will implement it in other big data solutions. Furthermore, Motionlogic will be free to market its analysis offerings.

CERTIFIED COMPLIANCE

Customer and employee data is safe with Deutsche Telekom. Its highly-effective data protection compliance management system was the first in the world to be certified to IDW PS 980.

In summer 2014, auditors Deloitte scrutinized Deutsche Telekom's data protection governance model and mechanisms for around three months. The entire system – including procedures, acceptance protocols and audits – was judged on design and implementation. Each and every process, and every step within each process, was examined in detail. The Deloitte experts also considered how tasks and workflows were modelled in IT systems. Furthermore, they conducted in-depth interviews with relevant employees.

Deloitte applied standard 980, developed by the Institute of Public Auditors in Germany (IDW), widely known by its abbreviation as IDW PS 980. It defines due-diligence principles for the verification of compliance management systems. Moreover, it is the basis for verifying that data protection systems comply with legislation, voluntary undertakings, and internal policies.

A brief description (in German) of certification can be found at www.telekom.com/verantwortung/datenschutz/datenschutz-im-unternehmen/22790.

A JOINT INITIATIVE FOR SECURE EMAILING

Email made in Germany (EmiG) was launched on April 29, 2014, and is a joint initiative on the part of Deutsche Telekom, freenet, GMX, and WEB.DE. The email service provided by the partners, used by around 50 million Germans, ensures the encrypted transfer of all emails sent and received via participating providers.

Furthermore, data is only stored and processed in data centers in compliance with Germany's strict data protection legislation. An icon in the shape of a green tick on the user interface of the webmail service indicates that the provider can deliver emails in accordance with the initiative's standards. This is under the premise that the recipient is also registered with an EmiG participant. Around two thirds of non-business email users in Germany leverage services provided by Deutsche Telekom, United Internet – GMX, WEB.DE – and Freenet. As a result, they automatically benefit from EmiG's advantages. It is still possible to send emails to users registered with other providers, such as Google, Yahoo and Microsoft. However, in these cases, data is neither guaranteed to be processed in Germany, nor to be safely delivered.

SECURE EMAIL ALSO AVAILABLE FOR BUSINESSES

The two leading email hosting companies in Germany – 1&1 and Strato – have three million business customers without their own dedicated email servers. These users, too, can sign up to the initiative – they can activate their domain with point-and-click simplicity. Furthermore, TÜV Rheinland offers EmiG certification to all commercial and non-commercial organizations with their own email infrastructures. This allows them to harness EmiG for encrypted communications with customers and business partners. "It's a big step forward in terms of secure communication," stated Björn Haan, COO at TÜV Rheinland i-sec, a subsidiary dedicated to cyber security, at the launch of EmiG. "If you send or receive a message with EmiG, you can be sure that your data will be transmitted and processed to the highest security standards – unlike conventional emails hosted outside Germany."

GERMAN ENCRYPTION CERTIFICATES ONLY

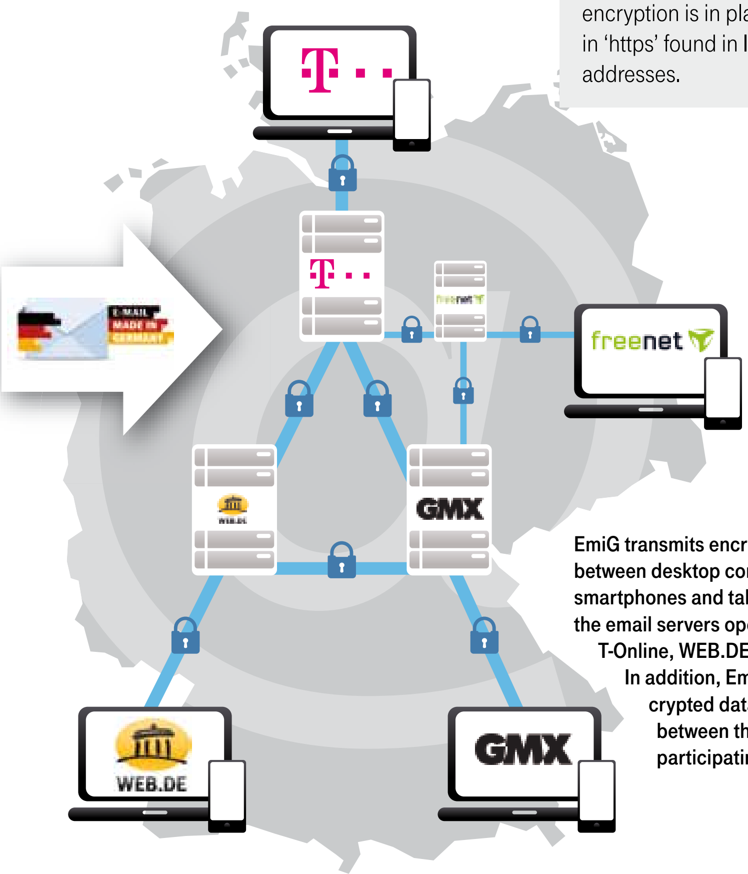
The robust encryption employed by EmiG is a cornerstone of Deutsche Telekom's security strategy. And the initiative has been warmly welcomed by the general public. This has been highlighted by a survey conducted by market research organization YouGov. 58 percent of respondents stated that EmiG is very helpful; they did not wish their emails to be read by unauthorized third parties.

EmiG employs the Transport Layer Security (TLS) protocol for end-to-end encryption. Additionally, the initiative has gone a step further – by only using German TLS certificates. And all partners have implemented the Perfect Forward Secrecy protocol, which creates an additional layer of protection against decryption.

Moreover, the participating email providers have introduced a new method of certificate validation and identity verification. Whenever data is transmitted, the provider's certificate and identity is checked to prevent third parties from eavesdropping. Communications are also protected with a key based on the AES 256 bit protocol – one of the strongest encryption standards in existence.

FOR YOUR INFORMATION

TLS: Transport Layer Security
TLS is the successor to Secure Sockets Layer (SSL). It is an encryption protocol that protects data when being transmitted over the Internet – for example when accessing emails and surfing the web. It only transmits encrypted content and only interacts with servers whose identity has been confirmed. It checks that data reaches the recipient completely intact and unchanged. Users can recognize when TLS encryption is in place by the 's' in 'https' found in Internet web addresses.



EmiG transmits encrypted data between desktop computers, laptops, smartphones and tablet devices and the email servers operated by GMX, T-Online, WEB.DE and freenet. In addition, EmiG allows encrypted data to be transferred between the data centers of participating email services.

THE DANGERS AND DEFENSES IN NUMBERS

The number of cyber attacks continues to rise. Attack vectors constantly evolve. It takes huge expense and effort to analyze and thwart these threats.

70 employees in the Group Privacy team test Deutsche Telekom's IT systems, processes, and new products

1.16 million customer credit cards were compromised between July and September 2014 by hackers who infiltrated the systems of Staples, a US office supply chain

10,000 data protection inquiries addressed to datenschutz@telekom.de

170 national data protection coordinators assist the Group with data protection tasks

400,000 new viruses flood the Internet daily

40 percent of Internet-connected computers in Germany were targeted by and infected with malware in 2013

5 attacks on the German government's secure network registered daily

575 billion dollars of damage to the economy caused by cybercrime in 2013

2,500 development projects vetted by the Privacy and Security Assessment (PSA) process annually

1,000,000

attacks on the Deutsche Telekom networks logged each day

72

audits of Deutsche Telekom, in both Germany and other countries, performed by internal and external experts

580

organizations have joined the German Cyber Security Alliance (Allianz für Cybersicherheit)

9

out of 10 companies in Germany have been the victims of cyber attacks

2

million reports of infected customer systems processed by the Deutsche Telekom Abuse Team in October 2014 alone

35,000

customers informed by the Abuse Team of malware-infected computers monthly

180

honeypots in use by Deutsche Telekom to analyze attack vectors

54

data protection officers employed at Deutsche Telekom locations outside of Germany

1,444

security warnings and advisories, and 43 incidents, reported by the Deutsche Telekom CERT

HUNTER TEAMS COMBAT INDUSTRIAL ESPIONAGE

Deutsche Telekom's new Cyber Defense Center (CDC) was established in April 2014 to safeguard the corporation against cybercrime. A team of highly skilled analysts leverages a security information and event management (SIEM) system, risk modelling, cyber-attack simulations and correlated log data to fend off potential threats.

Today's digital spies do not collect data arbitrarily. They specifically target a company's critical assets, including patents, high-tech designs and other valuable intellectual property. Furthermore, hackers often have access to extensive resources, and have ample time to carry out the attacks. The same applies to government intelligence agencies.

"If an intelligence agency or a highly-motivated, professional industrial spy decides to infiltrate a corporate network, it's only a question of time before he succeeds," states Bernd Eßer, Vice President of Cyber Defense & CERT at Deutsche Telekom. To this end, the criminal either breaks into the network directly, or employs some other method – such as seeding a company parking lot with malware-infected USB sticks or planting an accomplice who can infiltrate and infect the network from within.

DETECTING AN INVADER

A desktop PC infected with malware acts as a springboard for the criminal, who then works his way through the system to steal critical information assets. "This takes some time, however, since he first has to get his bearings in the network and then slowly navigate the system," explains Eßer. It could take weeks or months to map out the network of a major company and pinpoint the targets.

The real damage is done when a hacker makes the data available over the Internet. Consequently, the Cyber Defense Center's mission is to swiftly detect the intruder and resolve the security breach before intellectual property is compromised.

Bernd Eßer and his team protect Deutsche Telekom and its customers from threats originating within the Internet. They quickly intervene in the case of an attack to restore reliable IT operations, and deactivate malware. The forensicists at the CDC need to pinpoint hazards within a huge volume of data. To this end, they aggregate complex data from multiple sources, and analyze it to detect anomalies missed by conventional security systems. These sources include firewalls, intrusion prevention systems, proxy servers, Microsoft Exchange servers, Deutsche Telekom's antivirus software, and the Active Directory servers.

AVERTING ATTACKS

Extensive experience gives the security specialists an edge when it comes to dissecting the cyber criminals' strategies in use cases, or when scanning through log data for clues. They are supported by a security information and event management (SIEM) system. The SIEM collects and analyzes various log data based on criteria defined by the specialists. If it detects a suspicious correlation of events, as described in the use cases, the system alerts the hunter team. This is a group of computer emergency response professionals ready to spring into action at any moment. In the case of a genuine threat, they quickly resolve the issue and restore security.

Deutsche Telekom employs a unique, highly efficient method for the identification of malware. It aggregates data from a narrow range of sources, and then looks for predefined correlations and patterns (described internally as use cases). This approach ensures the CDC's hunter teams work with a manageable quantity of notifications with high hit ratios. A standard SIEM system typically generates a high number of false positives and subsequent alerts. This is resource and time intensive. Deutsche Telekom intelligently analyses a comparatively small number of events – and attains high-quality results, with very little "bycatch". When a use case does not have the required hit rate, it is deleted from the system. This minimizes the amount of data needlessly captured, collated and analyzed.

MODELLING NEW SCENARIOS

The insights gained from hands-on experience are harnessed to refine the use cases, to respond to emerging attack trends, and to model entirely new scenarios. At the moment, the CDC specialists are focused on safeguarding internal security at Deutsche Telekom. However, T-Systems will soon offer security as a managed service to its customers.

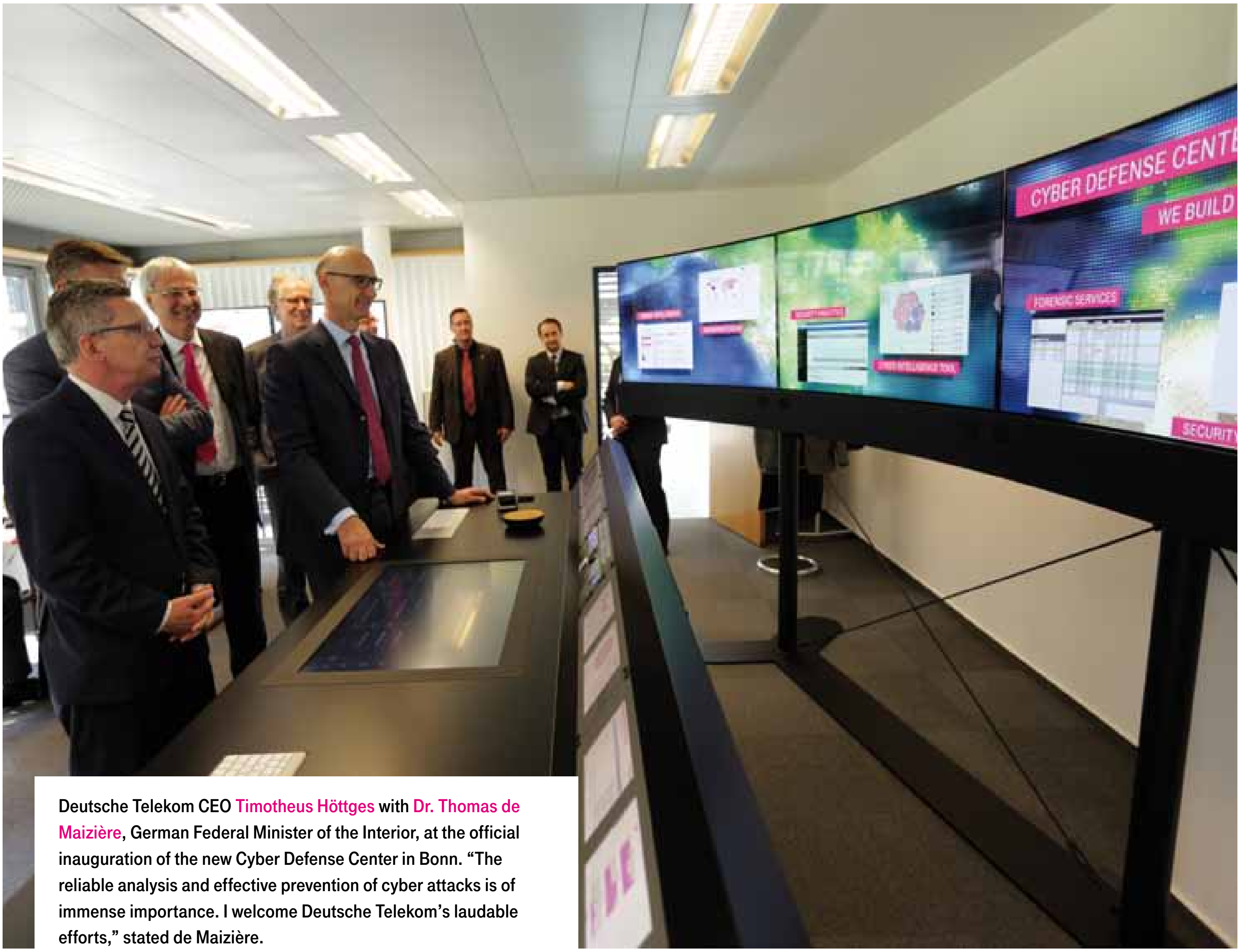
FOR YOUR INFORMATION

SIEM

SIEM stands for security information and event management. SIEM systems are capable of identifying and evaluating significant events in real time, and alerting the hunter team. They capture and correlate millions of data points.

Early warning systems, such as honeypots, help to recognize and combat the activities of cyber criminals. They pretend to be vulnerable in order to attract attacks and analyze them.

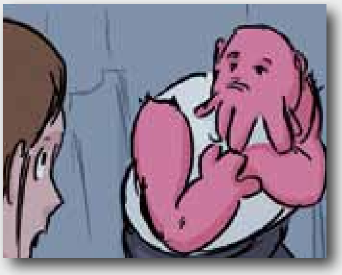
The Cyber Defense Center leverages behavioral analysis methods. Special sensors are employed to identify patterns that indicate criminal activities.



Deutsche Telekom CEO Timotheus Höttges with Dr. Thomas de Maizière, German Federal Minister of the Interior, at the official inauguration of the new Cyber Defense Center in Bonn. “The reliable analysis and effective prevention of cyber attacks is of immense importance. I welcome Deutsche Telekom’s laudable efforts,” stated de Maizière.

BE MORE VIGILANT, DATASLOB!

Hollywood has come to Deutsche Telekom's intranet: in December, the Group Privacy team launched a global awareness campaign with a teaser trailer.



Everyone's been there – your desk is covered in documents, including one or two that shouldn't really be shared with others. Then work is over, and the lockable filing cabinet or the paper shredder is just too far away. So you shuffle all your papers together, maybe quickly drop them in an unlocked drawer, and head out the door.

Day-to-day scenarios like this – the kind of thing everyone's done in a hurry – happen without malicious intent, but from a data protection perspective, they're problematic. They can result in personal, and often confidential, information falling into the wrong hands. In January 2015 Deutsche Telekom introduced a series of films featuring Dataslob, a made-up nickname denoting someone who handles data carelessly, as does the protagonist. The aim of this campaign is to raise employee awareness of data protection challenges, and encourage better practice. The films will be supported by a competition: employees across the globe can submit their ideas for day-to-day data protection challenges and how to (and how not to) tackle them.

SECURITY A RECURRING THEME AT THIS YEAR'S TRADE FAIRS

Data protection and security were among the hottest topics on the 2014 trade-fair agenda – helping Deutsche Telekom to raise its profile among visitors to exhibitions such as CeBIT, IFA and it-sa.

Trade fairs for industry experts and the general public are an important way for Deutsche Telekom to raise awareness of data protection and security issues. The organization focuses on top technology exhibition CeBIT, IFA – the world's leading consumer electronics show – and it-sa, the largest event for information security in German-speaking countries. In 2014, information was provided on many topics, including the protection of personal data, the secure operation of mobile devices, and security solutions for the cloud.

THE ISSUE OF DATA PRIVACY TURNS HEADS

The Security Report 2014, a representative survey carried out by the Allensbach Institute (IfD) on behalf of Deutsche Telekom, underlines the importance of raising awareness of cyber threats. 74 percent of respondents believe that the risk of data fraud will increase.

Market research at this year's trade fairs confirms that data security was one of the hottest topics for visitors to Deutsche Telekom's booths. Moreover, the majority of visitors view security as integral to the Deutsche Telekom brand.

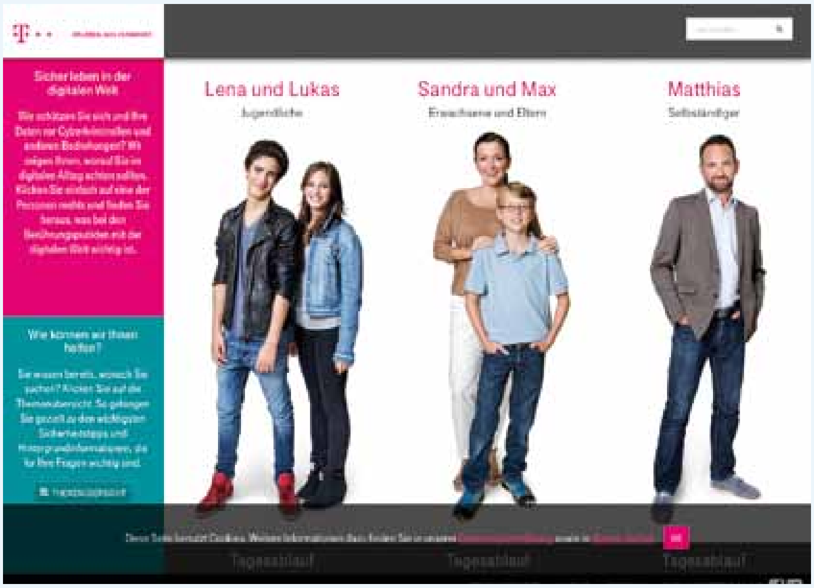
At IFA, booth team members were joined by representatives from Bürger-CERT, an initiative of the Federal Office for Information Security (BSI) aimed at consumers and small businesses. A key focus at IFA was empowering users to make their own decisions on data protection and security. To this end, Deutsche Telekom published a multimedia online guide (in German): sicherdigital.de. Launched at the start of the event, this resource includes useful self-assessments and practical advice on improving security, for example by changing Internet and website settings. It is aimed at children, young people, parents, consumers and small businesses.

THE CYBER DEFENSE CENTER

Deutsche Telekom's new Cyber Defense Center was a central focus at CeBIT, with visitors gaining insights into the facility's tools and resources. The key element is an analytics environment that identifies and visualizes suspicious activities. Visitors were able to observe attacks in real time and discuss possible solutions with security experts. As a result, Deutsche Telekom succeeded in drawing people's attention to potential threats and in establishing a basis for delivering targeted, personal advice.

STAYING SAFE IN THE DIGITAL WORLD

Cybercrime, malware, phishing – [sicherdigital], Deutsche Telekom's online guide, offers helpful advice on security and data protection in today's digital world.



www.sicherdigital.de provides guidance on security and data protection, aimed at youngsters, adults and businesses. The information is tailored to the needs of specific types of user, helping them identify where they are at risk and how they can protect themselves. An intuitive interface allows visitors to browse through security topics related to their real-world situation, geared to three target groups: youngsters, represented by characters Lena and Lukas; adults and parents, represented by Sandra and her son Max; and entrepreneurs, represented by Matthias.
A fictitious day with various activities has been created for each group, depicting common scenarios pertaining to security and data protection. Lena and Lukas's day, for example, includes texting friends using smartphones, social networking, browsing the net before doing their homework, and downloading an app before going to bed.

EDUCATIONAL AND ENTERTAINING

The tool's easy-to-use interface invites visitors to browse these scenarios and their attendant risks. Deutsche Telekom provides detailed explanations of the potential hazards, and how to avoid and overcome pitfalls – for example, by properly configuring a smartphone's operating system, and with special accounts for youngsters and children. Alongside purely informative articles, the tool includes checklists, summarizing the key points. In addition, users can fill out interactive questionnaires to evaluate their own security level, and watch a series of video clips showing how the featured characters handle their scenarios. The tool also has an alternate screen view, listing content by topic. This allows users to find information on a specific issue rapidly and easily – such as security for PCs and laptops, e-mail, and online banking. The website's mobile-optimized version also supports this view, giving a clear overview of key topics.

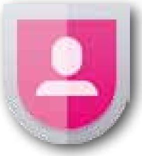
SHARING INFORMATION WITH OTHERS

[sicherdigital] is designed to be a one-stop source of tips on Internet security. Users find all the facts and advice needed to protect themselves and their data. The database also provides links to further content available around the Internet.
The tool's database is regularly updated and expanded; its format allows content to be easily edited to keep pace with the digital world. Social media functionality allows users to share articles and video clips. After all, life is for sharing – and so is security.

A SYMBOL OF DATA PROTECTION

Deutsche Telekom's privacy icon shows customers where they can find information on data protection, and access privacy settings. It is an increasingly recognized symbol.

Deutsche Telekom's privacy icon is synonymous with data protection. Since summer 2014, it has been displayed on Speedport routers' firmware user interface, and in Deutsche Telekom's DSL Help app for cell phones. By clicking on the icon, users gain access to settings that allow them to change their IP address for online anonymity.



The Group Privacy team developed this icon to make customers aware of the availability of data privacy guidance when buying a product or concluding a contract.

It is a symbol of data protection, and has high recognition value. It is found wherever Deutsche Telekom offers privacy information, for example when confirming consumers' online purchases. It is also found on the organization's Business Marketplace. This software rental portal also features further icons. These provide details of where cloud applications are hosted, and of who has access to customer data.

Deutsche Telekom Browser 7 also includes the icon, indicating a special mode of operation that ensures anonymity while surfing. With Deutsche Telekom's connected car solutions, the icon allows non-business travel in company cars to be logged without capturing highly personal data. In the future, the symbol may be introduced on temporary replacement devices issued to consumers by Deutsche Telekom's stores. The software will remind users to delete their personal data before returning their devices.

DIGITAL SIGNATURES FOR 40 MILLION DOCUMENTS

Deutsche Telekom introduced digital staff records 11 years ago. In 2011, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) instructed the company to attach digital signatures to records for Beamte – a type of civil servant unique to Germany, with specific privileges and duties. When Deutsche Telekom was privatized, these staff members retained this special status. The HR department decided to roll out the digital technology for all employees – encompassing more than 40 million documents.

In 2004, Deutsche Telekom announced it would no longer maintain hard copies of staff records. This has resulted in the generation of approximately 115,000 digital records for its civil servants and 130,000 for other employees. These electronic documents are centrally available to HR professionals, and to the individual employees themselves, who can access their personal information over the corporate intranet. Access rights are governed by a special agreement signed by Deutsche Telekom and employee representatives.

AN EVOLVING RISK LANDSCAPE

Until 2013, Deutsche Telekom safeguarded the integrity of its electronic documents with the MD5 checksum method. Experts believed this encryption technology, which was originally employed widely around the globe, to be a sound defense mechanism. However, potential attackers have increasingly powerful computers at their disposal – and systems relying on the MD5 algorithm are now vulnerable. Against this background, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) called on Deutsche Telekom to beef up security for civil servants records: each document must now have an electronic signature in accordance with the rigorous mandates of the German Digital Signature Act (SigG).

Digital signatures need to be attached to all documents – both those already on file and new ones, as and when they are generated. This posed an immense challenge. According to participants, the scale of the project was without precedent in Germany. Moreover, Deutsche Telekom had decided to apply the robust security technology to the records for all salaried employees, and not just for civil servants. In total, the project impacted over 40 million documents in approximately 245,000 staff records. In fact, the company has twice as many records as there are current employees. This is a result of Germany's statutory retention periods for these documents, and to the high number of retired civil servants receiving pensions.

EMPLOYEE REPRESENTATIVES PLAY AN ACTIVE ROLE IN PROCESS DESIGN

To reduce costs, Deutsche Telekom developed a process to generate digital signatures in batches. This semi-automated method minimizes manual input. Deutsche Telekom developed the process in cooperation with the BfDI and the North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information (LDI NRW). Employee representatives and Deutsche Telekom's Group Privacy team were also actively involved. In early 2015, Deutsche Telekom will destroy any remaining hard-copy records – taking a further step along the path to complete digitization.

HIGH AWARENESS OF DATA PROTECTION CONFIRMED

The annual Deutsche Telekom data protection awareness survey gauges employee knowledge of security and privacy issues – and how they apply this expertise on a daily basis. Results remained high in 2014, and improved at international subsidiaries.

Do you know how to encrypt emails containing personal data? Or how to report data protection incidents? These are the types of questions – based on real-world scenarios – posed by the data protection awareness survey.

The goal of the survey is to determine the extent data protection imperatives have been understood and put into practice by staff at Deutsche Telekom. To assess long-term trends, the Group Privacy unit performs the survey every year. In 2014, a representative sample of 30 percent of employees from Germany and 34 international subsidiaries was invited to participate.

In Germany, the results matched the previous year's very positive scores. And at Deutsche Telekom's international subsidiaries, there was a further improvement. This is most apparent in the aggregate score – which combines all individual metrics to create a single figure. While the aggregate for German employees remained stable at a very high 9.6 points, the international results continued to rise – from 7.6 points in 2013 to an all-time high of 7.9 in 2014. Moreover, the participation rate for the survey again increased.

EXECUTIVE INFORMATION SYSTEM

In 2013, Deutsche Telekom suspended use of its Executive Information System (EIS), based on SAP Business Warehouse. This was prompted by a suspicion that EIS could be processing personal employee information without appropriate authorization. An independent external auditing company investigated the matter, but found no evidence confirming the suspicion.

While auditing the software, the Group Privacy team found that it contained personal data on Deutsche Telekom employees. This is only permitted when in compliance with data privacy legislation, and where the data concerned is used solely for legitimate purposes. Based on the information held by the system, there was no indication that data had been misused or that privacy regulations had been breached.

CLEARLY DEFINED ROLES AND RESPONSIBILITIES

However, there was still scope for improvement regarding the IT systems employed by Human Resources. Against this background, all involved parties committed to address and implement five action items recommended by the external auditors. In consultation with the Group Privacy team, the HR and IT departments have now agreed on clearly defined roles and responsibilities for all HR systems. These will be set down in the form of binding group policy. In line with the segregation of duties principle, the HR and IT departments will each provide two representatives who will supervise all activities relating to the IT systems concerned, and take responsibility for their further development.

A further important step is the tight integration of IT security, financial, and data privacy audits. In the future, auditors will be obliged to inform the Group Privacy team of any anomalies they have detected – during financial audits, for example. This will ensure that a data privacy and security audit is then carried out. Other action items relating to HR software include the full, accurate documentation of all relevant rules, policies and agreements, and a comparison of corporate data privacy rules with agreements between Deutsche Telekom and employee representatives. Moreover, the Group Privacy team will set up a special training and awareness program for managers and HR software users.

HR SOFTWARE FROM THE CLOUD

Deutsche Telekom has been a long-time user of SAP's HR management software. Now, as part of a major international project, the existing range of modules is to be extended to include a cloud-based SAP solution. This requires customizing the software to remain compliant with data protection requirements.

The advantages of software-as-a-service (SaaS) are well-known: low upfront investment, scalability, and consumption-based pricing. Nonetheless, many companies shy away from cloud services. This hesitance is especially marked for tasks related to the processing of personal data – even more so when it is employee information.

HOSTING AT A GERMAN DATA CENTER

Against this background, the Group Privacy team has supported Deutsche Telekom's HR department from the onset of the SaaS implementation project. Two key issues had to be considered: in which country can personal data be stored and processed? And can a standard cloud solution fulfill the specific data protection needs of Deutsche Telekom's various international subsidiaries?

Deutsche Telekom's data center in Germany meets all of the data privacy requirements for hosting the HR cloud. Moreover, country-specific legislation governing personal data originating outside of Germany permits this arrangement. The Group Privacy team carried out an in-depth review of the contracts concluded between Deutsche Telekom and its international subsidiaries for internal data processing services, and modified their provisions where necessary.

The most difficult part was customization of the software. One of the greatest strengths of cloud solutions is the high degree of standardization. There is naturally only limited scope for customization. For this project, modifications were agreed upon with the Group Privacy team and carried out by T-Systems. For example, functionality needed to reflect the variations in statutory and highly strict retention periods for employee records. SAP will implement additional country-specific requirements based on a detailed data protection model.

IN LINE WITH DATA PROTECTION LAW

The goal is to ensure all aspects of the solution are in line with applicable data protection legislation. Deutsche Telekom began rolling out SuccessFactors Business Execution Suite (BizX) across all international subsidiaries in mid-2014 – the first countries included Germany and Poland.

PRIVACY BY DESIGN

Deutsche Telekom has added more checks and controls to its privacy and security assessment (PSA) process. The goal is to take data protection imperatives into account sooner, in the early phases of a product's development.

In any development project, if an error is discovered late in the game it will be time-intensive and costly to resolve. This applies equally to data protection. To nip potential issues in the bud, Deutsche Telekom decided to enlist the support of its internal security and privacy specialists at an even earlier phase. These changes were implemented in 2014. Jan Lichtenberg, who played a key part in the concept's development, explains, "We take a proactive approach. And customers are glad to receive our advice. Within just a year, we had provided expert assistance to a large number of projects, and have helped project leaders save on costs."

A STANDARDIZED CHECKLIST

To deliver effective advice, the Group Privacy team developed a checklist that ensures all key issues are addressed, and in a coherent way. The next step is to identify project-specific challenges that go beyond the scope of these standard requirements. During subsequent focus audits, Group Privacy professionals and project leaders concentrate their efforts on the most critical aspects of the development project. As Lichtenberg notes: "This enabled us to reduce the scope of data to be processed at an early stage, and to effectively implement anonymization mechanisms for a variety of projects." The experts no longer need to dedicate as much time to checking documentation; instead, they can run a system check on-site or via a web conference. Lichtenberg adds, "We are getting away from paper and are checking the real-life situation. After launch or go-live, additional focus audits monitor data protection in practice."

BELGIUM'S NEW ROAD-PRICING SYSTEM

In July 2014, Satellic NV won the contract to build and run a satellite-based road-pricing system in Belgium. Viapass, their client, is a government agency founded specifically for this project.

Data privacy is a key issue with road-pricing solutions, as they process huge volumes of data. A prime example is the tolling system implemented in Germany for trucks. Critics were concerned that data captured could be leveraged to track drivers' precise movements.

These doubts were addressed in part by including specifications on data privacy and security during the bidding process. Moreover, the German Federal Commissioner for Data Protection (BfDi) evaluated the system, developed by Toll Collect, in which Deutsche Telekom holds a stake. Following a thorough review, the project was approved. Permission to process the data was granted based on compliance with two specific acts of German legislation – one governing all major highways (BFStrMG), and the other the road-charging system itself (Lkw-MautV). The operator is obligated to process all

DEUTSCHE TELEKOM IMPLEMENTS BINDING CORPORATE RULES ON PRIVACY ACROSS THE GLOBE

21 EU member states have approved Deutsche Telekom's new Binding Corporate Rules on Privacy (BCRP). Global rollout of the Group policy commenced in July 2014. Deutsche Telekom's customers and staff will benefit from a consistently high level of protection worldwide, fully in accordance with European legislation.

The German Federal Commissioner for Data Protection and Freedom of Information (BfDI) approved the BCRP in May 2014. During the process, the BfDI consulted 21 European oversight agencies before reaching her decision. Deutsche Telekom is the first telecommunications company that completed the Europe-wide approval procedure.

The BCRP supersede the Privacy Code of Conduct of 2004, and include provisions on how the Deutsche Telekom Group captures, stores and processes personal data. They are a prerequisite for the legally compliant cross-border exchange of data within the Deutsche Telekom Group. The BCRP complies with all applicable EU legal requirements regarding the protection of personal data, and exceeds the minimum standards in some aspects.

A LEGALLY SOUND BASIS

Against this background, the BCRP provide a legally sound basis for data transfer with non-EU countries and demonstrate the Deutsche Telekom Group's full compliance with applicable data

data confidentially, in accordance with the applicable legal requirements, and only for the approved road-pricing purpose.

In Belgium, Satellic will play a different role. The company will be solely responsible for implementation and operation. Data processing will be entrusted to a Belgian government agency. The Satellic telematics platform includes modules for the automatic collection of data on road usage and for the calculation of the appropriate toll. The onboard units (OBU) on the trucks only transfer information relevant to the road-pricing tasks. All information on the precise movements of each truck remains on the OBU. The new system is expected to begin live operation in 2016.

protection legislation. This benefits both customers and the Deutsche Telekom Group itself – by adhering to the requirements of the BCRP, European subsidiaries will be able to transfer personal data to sister companies in third countries without requiring case-by-case approval of national oversight agencies. Deutsche Telekom is therefore able to develop international business models more rapidly.

The first company-wide Global Privacy Summit has been held in Berlin with Dr. Thomas Kremer, Board member for Data Privacy, Legal Affairs and Compliance at Deutsche Telekom.

THE DEUTSCHE TELEKOM GLOBAL PRIVACY SUMMIT

In late August, employees from across five continents gathered in Berlin for the first company-wide Global Privacy Summit. The goal of the two-day meeting was to establish a common understanding of data protection requirements throughout the worldwide organization.

Ninety data protection officers from the Deutsche Telekom Group traveled from South Africa, the United States, Singapore, and 20 other countries to participate in the summit. Host Dr. Claus-Dieter Ulmer described the motivation for this gathering during his opening address. The Senior Vice President of Group Privacy advocated leveraging the growing significance of data protection to strengthen cross-country collaboration.

During workshops and panel discussions, attendees came to the consensus that the key to successful collaboration lies in a common and mutual understanding of data privacy requirements. This applies to all countries where Deutsche Telekom is active. Fortunately, the organization has already established a solid foundation – for example, with its clear and standardized definitions of roles and responsibilities for data protection officers, and the Binding Corporate Rules on Privacy – whose international roll-out commenced in July 2014.

A number of projects have already been initiated that clearly illustrate how close, international collaboration can be successful in the real world. At its core, the success of such endeavors lies in actively supporting colleagues in product development, sales, system integration, and operations, from the onset. This ensures that data protection is an integral component of the Deutsche Telekom brand.

ALTERNATIVES TO GOOGLE, FACEBOOK AND CO.

The NSA debacle has influenced the opinions of key players in business and politics worldwide. In Europe, a recent survey shows that approximately two-thirds of executives believe it advisable to establish local alternatives to the leading US Internet and IT organizations.

Two years ago, the majority of senior managers felt that there was no need for European equivalents of US IT behemoths. Now, in the wake of the NSA scandal, the general consensus has completely reversed. This is clearly visible in the results of the Cyber Security Report 2014, a representative survey of members of the Bundestag and top executives at German medium- and large-sized enterprises. In the survey, administered in summer 2014 by the Allensbach Institute (IfD) on behalf of Deutsche Telekom, approximately two thirds of the 621 decision-makers polled recognize the appeal of an intra-European Internet, but believe it is not truly feasible.

Almost two thirds of top decision makers want an intra-European Internet.

The Cyber Security Report 2014 also reveals that the number of digital attacks on German businesses is on the rise. In 2014, nine out of ten organizations registered external attacks – with 14 percent reporting daily incidents, and 18 percent at least one per week. Despite this increase, only 39 percent of top management at major corporations felt hacking attempts posed a serious or very serious threat. This is a significant drop from the 53 percent of respondents in the previous year.

AS ATTACKS INCREASE, CONCERN DECREASES

60 percent of survey participants believe their company is well protected against IT threats. This is perhaps surprising, especially as four out of five managers are of the opinion that cyber attacks inflict significant damage on the economy. 69 percent of the surveyed decision-makers from medium- and large-sized companies view IT security as pivotal to their business – following directly on the tail of stalwarts customer service and cost efficiency. This train of thought has encouraged approximately 75 percent of organizations operating in global value chains to regularly exchange information on IT security with suppliers and partners. Cyber security is a particularly high priority when inter-enterprise data transfer is automated – something that is becoming increasingly common in light of trends such as big data and M2M.

90 percent of Internet users feel uneasy entering credit card details online.

FEAR OF CYBER ATTACKS GROWS AMONG INTERNET USERS

Online fraud, abuse of personal data by businesses and social network users, computer viruses – according to Security Report 2014 by the Allensbach Institute (IfD), these and other dangers are growing.

In spring 2014, the Allensbach Institute (IfD) – commissioned by Deutsche Telekom – carried out a representative survey of Germans aged 16 and over. Back in 2013, 44 percent of the population as a whole, and 47 percent of Internet users in particular, held major concerns over web security. A year later, the figures have increased to 47 and 54 percent respectively. Furthermore, 74 percent expect risk to rise in the future.

59 percent are apprehensive when prompted to enter personal data – for example when shopping online, logging into social networks, or signing into email accounts. Only 26 percent have no concerns whatsoever. The numbers vary greatly with age – younger people tend to be more wary than older ones.

AN UNEASY FEELING

For web users, not all data is equally sensitive. Credit card numbers and bank details are regarded as especially critical. More than 90 percent of Internet users are anxious about submitting this kind of information online. In excess of two thirds are leery of divulging their telephone numbers or addresses. People are generally less reluctant to key in their email address.

Despite these suspicions, only 17 percent of Internet users regularly read privacy statements on online shops or other websites – 26 percent read them occasionally. Why? They are too lengthy – reading them is an arduous task. And 55 percent of respondents said that they were too complicated to be understood. One in three thinks they are often hidden away and difficult to find.

THE OLDER, THE LESS CAUTIOUS

A survey, carried out by the market research agency TNS Emid on behalf of Deutsche Telekom, has brought to light an interesting correlation between user age and vulnerability to online crime. It shows that older users of computers, laptops, tablets and smartphones are more likely to be victims of digital attacks.

Survey responses indicate that most users do heed warnings regarding phishing, spyware, viruses, and hackers. The majority of the 1,000 Germans polled confirmed they implement, at a minimum, the most basic IT security measures. This includes practices such as using and keeping antivirus software up-to-date, encrypting data and regularly changing passwords.

But not all IT users follow this example; 12 percent do not make use of any security mechanisms for data and devices. Among those in their 50s this percentage increases to 22 and to one in three above 60. Of the 36 percent of the participants who rated their IT expertise as poor or very poor, 30 percent neglect to implement any security measures at all.

SUPPORT FROM FRIENDS AND FAMILY

There is a strong link between these numbers and the respondents' self-assessment of their IT skills. The older the users, the weaker they believe their knowledge to be – with 39 percent of those 50 to 59 and two thirds of those over 60 believing their IT proficiency is poor or very poor. Conversely, among participants between the ages of 14 and 29 this figure is only 14 percent.

Should technical problems arise, two thirds of respondents state that they turn first to friends and family if they feel they do not possess the knowledge to resolve the issue themselves. 23 percent, on the other hand, pay for assistance from IT professionals. The reasoning behind this decision varies. For the majority, the prime motivation is to gain access to expertise per se, whereas for others the driving force is the belief that an expert can solve the issue more rapidly than they could independently.

One in three over-60s do not have any form of protection in place for their data and devices.

DEUTSCHE TELEKOM BROWSER WITH BUILT-IN PROTECTION

Deutsche Telekom's Browser 7 has been downloaded over one million times to date. Since November 2014, it has been equipped with built-in security functionality designed to make hacking more difficult. This feature is the first of its kind in Germany.

While security configurations in many browsers are hidden in complex and difficult-to-understand Internet setting submenus, Deutsche Telekom Browser 7 users can easily access theirs directly from the toolbar. A simple click of the "security" button opens a dropdown list. The user is able to easily delete Internet history and cookies, and check the security status of the Internet connection. The system also automatically notifies users if their Internet access has been compromised, and suggests countermeasures – for example, changing passwords or installing a security packet or patch. This reduces the likelihood of a virus or Trojan going unnoticed, and damaging the system.

BLACKLIST FOR UNDESIRABLE WEBSITES

The browser automatically opens a private session for selected websites to avoid the user leaving "digital tracks". It also has a blacklist option to block access to undesirable websites. Users can also enable wildcards to block websites with predefined kinds of content – without needing the precise website address or name.

A key role is played by honeypots. Worldwide, more than 180 of these traps gather data on the origins and types of cyber attacks. This is displayed on a digital map at www.sicherheitstacho.eu, a Deutsche Telekom website. Detailed information and statistics on cyber attacks can be viewed via this online tool. Deutsche Telekom Browser 7 is based on Mozilla Firefox, and is available for download free of charge at: **www.t-online.de/browser** (website in German only)

DATA PRIVACY MADE SIMPLE FOR SMARTPHONES

Protecting personal data on cell phones has become a fine art. Often effective privacy settings are rare, or hard to find without substantial research. Mozilla and Deutsche Telekom are striving to change this. Starting in 2015, Firefox cell phones will be equipped with privacy mechanisms that are easy to use, even for non-IT professionals.

Most leading operating system providers offer only limited mechanisms for safeguarding personal data on mobile devices. Privacy settings are often difficult to recognize and, in light of increasing threats, frequently inadequate. Currently, Firefox OS is the only exception. It was created by the open source community Mozilla. It provides users with a range of features to manage external access to their device's services and data.

MORE CONTROL OVER DATA

Going forward, Mozilla will be significantly expanding this functionality, in close collaboration with Deutsche Telekom. At the 2014 Mobile World Congress in Barcelona, the development partners unveiled a prototype, and granted visitors an opportunity to experience pioneering features. These include variable location accuracy. In other words, the user can specify how precisely an app can report their smartphone's position. For example, the user might restrict GPS data transfer to navigation apps. A weather app, on the other hand, would only be notified of the city, but not the device's exact coordinates.

A new remote privacy protection feature similarly offers a higher level of user control. Unlike other operating systems, Firefox does not transmit location data to a central point of administration for use in the case of device theft of loss. Instead, a localization password is stored on the phone. When this password is sent to the misappropriated or mislaid hardware via text, the operating system responds with a message giving the device's current position.

Mozilla will phase in the data privacy functionality, developed in collaboration with Deutsche Telekom, in 2015. This will include a permission history, making clear which apps have access to which device services and data. This helps users to recognize and restrict access permissions for data-hungry apps.

INDUSTRY-WIDE INFORMATION EXCHANGE

Deutsche Telekom is committed to promoting industry-wide exchange of information, with the goal of improving data privacy for all smartphones. Against this background, the company organized an international workshop in association with the World Wide Web Consortium (W3C). Top-level data privacy experts from practically all operating system providers, and representatives of universities and non-governmental organizations, gathered in Berlin in late November. One of the key goals of the event was to share Deutsche Telekom's insights from the development partnership. The discussion is being continued within W3C's Privacy Interest Group.

DEUTSCHE TELEKOM RAPIDLY FIXES MOBILE NETWORK SECURITY FLAW

In December 2014, a team of security research experts from Berlin uncovered vulnerabilities in SS7 – a cellular network protocol used worldwide. The weaknesses enabled third parties to spy on UMTS and GSM communications. All mobile carriers are susceptible to the flaw. Deutsche Telekom responded by immediately plugging the gap in its own network.

In the months before the news broke, Deutsche Telekom had already started to improve its SS7 systems. Once the severity of the problems became apparent, the enterprise immediately took further steps. Moreover, Deutsche Telekom works closely with external specialists – such as members of the Chaos Computer Club (CCC); a non-profit, 'white-hat' hacker organization.

At the CCC's annual conference, one of the club's mobile telephony experts demonstrated how it was possible to hijack functions in SS7 to reroute communications. They would first redirect calls to themselves, before forwarding them to the intended recipient. This sidesteps network encryption, allowing access to private telephone conversations and text messages. All information needed for decryption is communicated over SS7. However, only professional criminals possess the ability and expertise needed to put theory into action – the process requires dedication and sophisticated planning. Furthermore, it is impossible without specialized devices unobtainable on the consumer retail market.

Individual network operators can only provide temporary solutions. The entire industry has to work as one to develop a long-term answer to these issues. Network operators and infrastructure providers, end-device manufacturers, IT industry associations, and standardization bodies – such as the European Telecommunications Standards Institute (ETSI) and the Groupe Speciale Mobile Association (GSMA) – must all take responsibility.

A SMARTPHONE APP FOR SECURE COMMUNICATION

Deutsche Telekom's Mobile Encryption App encrypts voice-over-IP phone calls, and text messages on smartphones that leverage Android or iOS platforms. The software can be deployed anywhere in the world, independent of device and network.

Deutsche Telekom's encryption app enables secure telephony on popular smartphones with Android or iOS operating systems. This solution, developed in partnership with the mobile security company GSMK, has a variety of powerful features. It supports all telecommunications networks, and can be used without a SIM card via a satellite or WiFi connection. The app even operates in countries where Internet telephony is disabled.

Data is transmitted at 4.8 kilobits per second – requiring only limited bandwidth. As a result, the app is well suited for regions with poor network coverage. The software also works in GSM networks in developing countries. And while each individual participant in a conversation must have the app installed on their device, they do not need to be registered with the same mobile carrier. Additional software is not required.

SHIELDING PRIVATE INFORMATION

The app is ideal for a variety of situations: when negotiating contracts, discussing mergers, or exchanging confidential research and development information, for example. It would also be useful in witness protection programs.

For each conversation, a robust encryption key is generated on the smartphone itself, and deleted after the data is received. This ensures that communications are only available to intended recipients, and protect against spying by third parties via man-in-the-middle attacks. Contact data, written messages and documents are encrypted and saved in a dedicated, secure container on the smartphone. Confidential information can only be read after entering a password.

Deutsche Telekom deliberately developed a product that is versatile and geared towards international customers. The app will initially be marketed to major corporations. In the medium term, it will also be marketed to consumers and small businesses.

BOTNETS: DEUTSCHE TELEKOM ACTS QUICKLY TO NEUTRALIZE ANDROID VIRUS

In early 2014, Spanish authorities discovered that 60 Deutsche Telekom cellphone customers had been connected to a botnet. Deutsche Telekom immediately contacted each victim, providing clear instructions on how to stop the misuse of their smartphones.

A botnet is an illegal network that takes control of Internet-enabled devices without the user's knowledge. It works by installing malicious code onto the targeted device. Cyber criminals are increasingly taking aim at high-performance smartphones – with Android mobile devices by far the most popular targets. Once a smartphone is connected to the botnet, it can be operated remotely via a command-and-control server. The server can then spy on the user's login data, to name just one potential peril.

In January 2014, the German Federal Network Agency notified Deutsche Telekom of an ongoing cyber attack.

While investigating an Android botnet, Spanish authorities had discovered data from a number of cellphone users – including 60 of the company's customers. Deutsche Telekom's Group Privacy service team immediately provided support to the affected customers. First, the service staff contacted each customer by telephone. If the team failed to get through, they sent a text message asking for a return call. During the calls, the service team provided step-by-step instructions on how to completely remove the malware from the device. In addition, customers were advised to install antivirus software, with the goal of preventing potential reinfections.

DON'T FINGERPRINT OUR USERS!

In summer 2014, researchers described a new, exceptionally powerful and persistent web user tracking method, known as canvas fingerprinting.

They studied some 100,000 websites to see the technique in use. T-Online was also briefly affected. Canvas fingerprinting enables companies to track what sites a user visits – without them being able to disable the function directly. This is a clear contravention of Deutsche Telekom's data protection policies. Moreover, the method flies in the face of German and European legislation. One particular partner had employed the backdoor technology on the T-Online website, without the knowledge of Deutsche Telekom. The offending service provider insisted that it had not collected any personal information. Nevertheless, the action was considered a betrayal of trust. T-Online immediately suspended the partnership. One workaround to prevent this form of tracking is to disable JavaScript. But most online content would then be incorrectly displayed. Deutsche Telekom is currently working on a solution that will enable it to detect the unauthorized deployment of canvas fingerprinting on its portals – and to enforce its data protection policies.

Tracking website visits without the user's consent contravenes applicable legislation.

THE TELECOMMUNICATIONS

In the summer of 2013, Edward Snowden's revelations sent shockwaves through the digital industry. Their effects are still being felt. But we should not forget the growing problem of cybercrime. Both of these issues pose a serious threat.

Mr. Petri, what is your take on the current state of global security?
Axel Petri: Unfortunately, the general geopolitical situation continues to worsen, and this is having a substantial impact on the digital world. Until the end of last year, the debate surrounding striking the right balance between collective security and personal freedom was relatively unaffected by outside socio-political influences. However, recent developments in Ukraine, the rise of ISIS in Iraq and Syria, and the tragedies in Paris, have cast a shadow on the discussion.

So, where do you stand in the Internet security debate?
Axel Petri: I think we're facing a paradox. All governments, including democratic ones, engage in a certain amount of surveillance. The hope that this will cease, particularly in light of the current world crises and geopolitical situation, is little more than a fantasy. The notion of total digital security is also an illusion. This is something that we simply have to come to terms with. Nevertheless, Deutsche Telekom makes all efforts to improve the security of its networks and services. We know that there's no silver bullet – no magic solution to all the challenges we face. So we're going to continue working step by step to resolve them.

Why does Deutsche Telekom have to continually work on the security of networks and services?
Axel Petri: Cyber space is becoming an increasingly dangerous place. On the one hand, there are hackers out there who want to steal business and customer data for profit. On the other hand, there are the politically-motivated cyber terrorists and hacktivists intent on sabotaging systems, and causing financial and material damage. And there are also intelligence agencies that wish to intercept our customers' sensitive data.

How can Deutsche Telekom combat these dangers?
Axel Petri: As an international provider of telecommunication network services, it is our job to safeguard against these threats, and to protect our customers' communications and data. Consumers trust us to achieve this, and this means they put a lot of faith in us. The findings of the Security Report 2014, a representative survey of the German population carried out by the Allensbach Institute (IfD), are illuminating. The study demonstrates that Deutsche Telekom is by far the most trustworthy company when it comes to handling personal data. We do everything we can to justify our customers' trust in us.

What do you do to improve security for your customers?
Axel Petri: In terms of security, the migration of our network infrastructure to all-IP is an important step forward for us. A private data network across Europe is more reliable, and offers better protection against attacks. It also allows the end-to-end encryption of landline and cellphone VoIP communications. By contrast, analog technology is outdated and unreliable.

Furthermore, we work closely with government organizations, such as the Federal Network Agency and the Federal Office for Information Security (BSI), to protect our customers. However, as we offer telecommunications services throughout Europe, we have to consider the regulations and legislation of many countries. For example, we must deal with diverse national data retention laws and rules on the duty of disclosure to government authorities. Another issue is that the

INDUSTRY FACES GLOBAL CHALLENGES

A dedicated European network would allow end-to-end encryption of data, e.g. for voice over IP.

security mechanisms in place for telecommunications services, IT and other critical infrastructure vary from country to country in terms of quality. Germany stands out among EU member states as a leader in terms of network infrastructure security. Deutsche Telekom is actively working to significantly increase security levels across Europe.

What action do you want European states to take?

Axel Petri: Governments must prepare for changes that will be wrought by emerging technologies such as all-IP. Their agencies must also allow greater visibility into the working relationship between themselves and telecommunications organizations. They have to support internationalization efforts, and establish a common legal framework to enable the public to take full advantage of pan-European networks. We need a solution that allows businesses in particular, but also government agencies, to enjoy the benefits of secure, encrypted cross-border communications. This will not be possible with country-specific solutions and segregated national networks.

What steps need to be taken?

Axel Petri: To successfully implement pan-European networks, government agencies must recognize the need for network infrastructures that transcend national borders. This is likely to have a significant impact on national government agencies. We have to make agencies aware of the social and economic advantages of international networks over national ones – for both governments and their citizens.

But this doesn't mean that legitimate national security interests should be neglected. The business community and governments will have to work together to find solutions. We are more than willing to make our contribution, at any time.

FOR YOUR INFORMATION

Critical infrastructure comprises assets and systems that are vital to the functioning of the state and society as a whole. Their failure or degradation would disrupt the provision and distribution of essential resources, would severely endanger public safety, and possibly have other catastrophic consequences.

ABOUT THE INTERVIEWEE

Axel Petri

is Senior Vice President of Group Security Governance at Deutsche Telekom. In this role, he is responsible for all aspects of security throughout the organization. This includes strategy, policies, monitoring and enforcement. He also coordinates security units throughout Deutsche Telekom. Furthermore, he is responsible for protecting information and other valuable business assets, and for investigation and prevention. Moreover, he ensures that Deutsche Telekom complies with its statutory duties within Germany in terms of public safety, including strategy and management of lawful interception and data provision. Petri holds a degree in law, and has co-authored a guide to the legal issues surrounding e-commerce (Rechts-Handbuch zum E-Commerce), and has written many other publications on Internet and media law, and on security issues. He lectures at Darmstadt University.

ENSINGER SHIELDS ITS EXPERTISE WITHIN A PRIVATE CLOUD

Ensinger, a mid-sized family-owned company, is a leading global player in the thermoplastics industry. It opted to deploy a private cloud solution for its 28 production and distribution centers – creating an environment shielded from the pitfalls of the public cloud.

“New materials play a critical role in industrial progress” – this insight transformed Ensinger from a garage start-up into one of the world’s leading high-performance plastics suppliers in just five decades. Customers from many industries turn to Ensinger for semi-finished goods, precision-engineered components, and construction profiles that test the limits of the technically feasible. To meet these high expectations, Ensinger has made innovation management a central element of their business model.

PROTECTING KNOWLEDGE

“Our products and manufacturing methods are what differentiate us from other market players. Protecting this knowledge is one of my core duties,” explains CIO Erwin Schuster, responsible for Ensinger’s ICT systems all over the world – a responsibility that grows with every year, as Ensinger continues to expand its international operations. The company is now present in over 20 countries, adding to the complexity of the corporate IT environment. What’s more, globalization is only one of the challenges faced by the IT department. It also has to address 21st-century work methods and models – including ever-greater mobility, virtual collaboration, and global management of production plants.

Changing requirements open up new vulnerabilities within ICT systems. To counter this increasing complexity, Ensinger implemented a private cloud solution. This is built around three data centers operated by Ensinger at its German production sites in Cham, Nufringen und Rottenburg-Ergenzingen. In cooperation with Deutsche Telekom, the plastics manufacturer has created a wide area network (WAN), connecting all three facilities.

TWO ACCESS POINTS

As Schuster explains, “The key is that our business data is exclusively transmitted via dedicated Deutsche Telekom lines, and is segregated from the public Internet. There are just two access points for web communications that transcend the private environment, and these are guarded by Deutsche Telekom experts around the clock.”

Base-line operations started in late 2014. Step by step, Ensinger is integrating all its sites and international subsidiaries into the private cloud environment.

ICT professionals must build solid defenses, but without placing excessive constraints on the free flow of communications. Erwin Schuster believes that striking the right balance will become increasingly important. A key driver is machine-to-machine communications – the emergence of manufacturing and logistics systems that exchange data over networks. “A prime example is our own production equipment. The next generation will have something like five to six network ports. This poses entirely new challenges in terms of connectivity – and security. Moreover, there is a clear trend towards ever greater vertical integration of all operational applications.”

ROBUST GOVERNANCE

To steer an acceptable path between the needs of security managers and wants of users, Ensinger has produced a comprehensive policy document. This clearly defines who is permitted to perform firewall administration tasks, for what period, under what circumstances, and to what purpose – and Deutsche Telekom retains overall operational responsibility for both technology and processes. CIO Schuster advises other companies looking to develop a similar document to put aside ample time for the task: “In our instance, it took us more than nine months just to finalize the structure and key points. It entails a huge amount of effort, but it is the basis for a coherent, robust solution that supports both business needs and security imperatives.”

SEPARATING THE WHEAT FROM THE CHAFF

The proposed German IT security act will help protect key infrastructure, such as power grids, telecommunications networks, and critical sectors of the economy, such as the food industry.

Hackers attack websites 24 x 7. However, only the most dramatic cases get widely reported. Over Christmas 2014, digital assaults on the PlayStation Network and Xbox Live made the headlines. In January 2015, there was media uproar when the websites of Angela Merkel and the German Bundestag were infiltrated. However, the only outcome was negative publicity. If hackers were to target the IT systems that control the nation's electricity, by contrast, the impact could be catastrophic – without power, Germany would quickly grind to a halt. Consequently, the Federal Ministry of the Interior plans to include definitions of critical infrastructure in the proposed IT security act – and to specify corresponding security imperatives, including mandatory reporting of IT security events. The scope of critical infrastructure is to include essential sectors of the economy, such as the food industry. Riccardo Sperrle, CIO of Tengelmann Group and of retail chain Kaiser's Tengelmann, can understand the rationale. However, the risk of a cyber attack precipitating a serious crisis is lower than with critical infrastructure per se. He states: “We are attacked by hackers every day. But if they ever succeeded in taking our IT systems down, we would be quickly back up and running. The food supply would not be impacted for any length of time.”

The Tengelmann Group safeguards its IT systems with a cutting-edge information security management system

His thoughts chime with the findings of EHI Retail Institute, which studied the food retail industry's security standards and the threats it faced in 2013. It concluded that retailers were well prepared. According to the report: “Security standards are very high. Due to the wide variety of IT systems implemented across the industry, and the number of organizational units involved, there is only modest risk. The probability of a cyber attack causing large-scale food shortages is very low.” The report also found that IT security roles and responsibilities were generally clearly defined, and that all enterprises had implemented an information security management system – or were in the process of doing so. Retailers had also carried out risk assessments, and developed corresponding security mechanisms and plans. Sperrle has experienced this first-hand. “Deutsche Telekom's IT security specialists helped us test our systems and, where needed, modify them in line with the latest methods of attack,” he recalls. He also encourages his counterparts to take stock of vulnerabilities before moving on to actual testing: “Every company has to be aware of where their most valuable assets reside. It would be illusory to believe you can fully safeguard your IT systems at all times against targeted, large-scale attacks. So, it's important to clearly define the degree of protection each system needs, and to concentrate your defenses on business-critical processes and data.”

Against this background, a retailer who generates a significant portion of revenue through online sales must make all efforts to bulletproof their web presence – for example, against attempts to access and misuse customer data, and DDoS (distributed denial of service) attacks (of the kind that caused Angela Merkel's website to go offline). Sperrle highlights the problem: “If an online store is down for several days, it can cause huge financial losses, and permanently damage a brand's image.” Online channels account for a relatively low proportion of Kaiser's Tengelmann's total sales. But for other Tengelmann Group subsidiaries, they are a significant source of revenue.

Industrial espionage is also not a major issue in the food industry, as Sperrle explains: “We sell products developed and made by others – so we don't have as much patented knowledge as the suppliers themselves.” The CIO may seem sanguine about the perils he faces. But he did not divulge what Tengelmann's key assets are, and where they reside.

GREATER SECURITY FOR EVERYONE

Deutsche Telekom has revised its 1,800 security requirements for IT/NT systems and has made them available to the public free of charge.

Deutsche Telekom's security specialists have been working on security requirements for IT/NT systems for over a decade. These requirements describe the issues that in-house developers and third-party service providers must pay attention to when creating new products and systems, such as websites. Security requirements form the backbone of the Privacy and Security Assessment (PSA) procedure implemented by Deutsche Telekom to guarantee that all new and updated products and services used in-house or offered to customers meet the same high security and data protection standards. Since 2011, the procedure is applicable to all group companies worldwide.

AVAILABLE TO ALL AS A FREE DOWNLOAD

Over the years, 55 in-depth papers have been produced, detailing security requirements relating to general functionality, system-specific functionality, and implementation of products and services such as Apache servers. In the summer of 2014, experts of the Group Security Service (SEC) reviewed and revised all of these papers, which contain a total of 1,800 individual requirements. Deutsche Telekom has made them available to the public for the first time since they came into force on July 1. 2014. They can be downloaded free of charge from http://www.telekom.com/security.

"These requirements are relevant to anyone interested in improving the security of their products," asserts Dr. Markus Schmall, Vice President for Application Security and Testing at Deutsche Telekom. "And of course for any company wanting to define security requirements for itself and its service providers," he adds. Schmall explains the motivation for publishing the requirements: "If every developer complied with our requirements, the security of IT/NT products would be much tighter than it is at present," he says. Greater security for everyone.

CORPORATE SECURITY 2030 STUDY HIGHLIGHTS IMPORTANCE OF HUMAN ELEMENT

Supported by the North Rhine-Westphalian Association for Security in Business (VSW NW), senior executives at Bayer, Daimler, Deutsche Post DHL, Deutsche Telekom and RWE have considered the likely development of security issues between now and 2030. They focused, in particular, on protecting information and data assets.

Corporate Security 2030: Challenges & Opportunities is a cross-industry study. It was initiated and performed by the EBS Business School's Strascheg Institute for Innovation & Entrepreneurship (SIIE) and Z_punkt The Foresight Company, a consulting firm. They brought together security specialists, data protection officers and senior executives from Bayer, Daimler, Deutsche Post DHL, Deutsche Telekom and RWE. These experts were joined by representatives from the VSW NW.

DEVELOPING THE RIGHT STRATEGY

The study's main goal was to ascertain and assess future security challenges faced by business organizations. Moreover, the participants developed corresponding strategies for these companies and for security management as a whole. There was broad agreement that the protection of knowledge, information and data remains a key entrepreneurial challenge.

It was recommended that strategies should not place excessive emphasis on technology. It is at least equally important to consider the human factor. Against this background, it is critical to strengthen the loyalty of staff with special skills and access to sensitive information. Employees must also be given the skills needed to deal responsibly with critical data – effectively turning them into human firewalls. Furthermore, it is crucial to strictly define and govern external service providers' physical and logical access to valuable assets. In light of the growing importance of security, raising employee awareness is a major priority.

WORKING WITH GOVERNMENT AGENCIES

Telecommunications companies are legally required to cooperate with government agencies under certain circumstances. In 2014, Deutsche Telekom began disclosing the number of lawful interceptions carried out in Germany, and the type and frequency of information obtained.

In 2014, a total of 47,958 access lines were monitored. The majority of requests from judges and state prosecutors were made pursuant to Section 100a of the German Code of Criminal Procedure (Strafprozessordnung). A minority of interceptions were made in accordance with the provisions of legislation placing constraints on the constitutional right to confidential telecommunications (known as the Article 10 Act (G10)). A small number were authorized under state-specific legislation governing the rights, duties and organizational structures of police forces (Landespolizeigesetze). In all, 49,796 connections were monitored in 2013 – in other words, year on year, there has been little change.

GROWING DEMAND FOR TRAFFIC DATA RECORDS

By contrast, the German state's interest in traffic data records has grown significantly. In 2014, Deutsche Telekom accessed its database 502,847 times to fulfill its legal obligations. The equivalent figure in 2013 was 436,331. The number of identifiers in these records is substantially higher; however, the exact figure is not reported. This is primarily attributable to mobile telecommunications. The relevant data records include all customer identifiers active in a cell during a given period of time. As a result, the number of recorded identifiers often runs into the tens and hundreds of thousands, particularly in major cities.

A total of 27,957 requests for subscriber data were made in 2014. The majority of requests were for the following customer details: name, date of birth, telephone number, network termination point, billing address and bank account details. Moreover, Deutsche Telekom supplied data for a total of 733,377 IP address owners.

PROCESS IS STRICTLY MONITORED

Deutsche Telekom must comply with the right to confidential telecommunications, enshrined in the German constitution (Basic Law), and with data protection legislation. As a result, Deutsche Telekom can only carry out interceptions where all legal preconditions have been met. If there is any doubt, any official request will be challenged, and communications will not be intercepted. All monitoring is subject to dual control – in other words, it requires the participation of two employees, with each scrutinizing the actions of the other. Every step is fully documented, and regular checks are made by Deutsche Telekom's government-approved security representative and by the Federal Network Agency. In addition, the data protection officer and Deutsche Telekom's internal auditors may perform unannounced inspections at any time.

CLEARLY DEFINED DEADLINES FOR SECURITY PATCHES

Deutsche Telekom is tightening up requirements for suppliers in regard to resolving security weak points. In 2014, the organization began defining set time frames for the release of patches.

One of the top priorities within ICT security management is to swiftly address critical vulnerabilities. Software vendors have recognized this need, and in response, taken measures to significantly accelerate their development processes. Patch management on the part of network equipment manufacturers, by contrast, is often far slower. Against this background, Deutsche Telekom has revised supplier contracts to reduce time-to-resolution. Depending on the weak point's severity, manufacturers may be obligated to release a suitable patch within just a matter of days. However, where it is not feasible to meet the deadline due to the problem's complexity, suppliers must provide a temporary solution, generally known as a work-around.

The Common Vulnerability Scoring System (CVSS) is a standard ICT industry method of assessing the severity of weaknesses. It rates the potential threat of a vulnerability on a scale from 1 to 10. Deutsche Telekom has defined a score of seven as the threshold for a highly rapid response by suppliers. By comparison, problems rated between one and six can be resolved by means of standard updates.

SHIELDING MOBILE DEVICES FROM MALWARE

A new security service prevents malware infections and lets business professionals communicate safely using their smartphones, tablets and other mobile devices.

Malware is mushrooming: in 2013 alone, there were 2.5 million new malicious programs targeting mobile devices. And yet only one in five German enterprises takes the precautions needed to ensure robust Internet security on smartphones, tablets and laptops. A new offering from Deutsche Telekom allows organizations to set their own security levels. The cloud service proactively shields devices from malicious code on the Internet, preventing rather than curing infections. As a result, antivirus software and firewalls do not have to be deployed on each hardware asset.

Data that has been cleaned in the cloud will not cause damage when transmitted to mobile devices.

Users of this service can allow or block traffic to and from individual source and target addresses. They also determine which ports are open or restricted in order to fend off known botnets. Moreover, data is encrypted and then transmitted via a secure SSL VPN tunnel. If an employee accesses the Intenet by means of an insecure hotspot this will safeguard against session hijacking, i.e. the infiltration and eavesdropping of communications.

Devices can be registered and configured on a web portal. An overview of all attacks for each asset can be displayed at the touch of a button. The number of users can be defined and modified in line with changing needs. Security standards are always up to date and all traffic is processed and managed at Deutsche Telekom's data centers in Germany – where data is monitored in real time, and any potential threats removed before they can inflict harm.

SECURITY IN TERMS OF INDUSTRY 4.0

In October 2014, German business and political leaders gathered in Hamburg to discuss the digital economy at a summit organized by the Federal Ministry of Economic Affairs and Energy. Infineon and Deutsche Telekom unveiled a security solution that protects M2M and other manufacturing-industry communications.

They demonstrated how it is possible to build end-to-end defenses for the transmission of sensitive manufacturing data between two sites located within Germany. The solution is particularly suited to the needs of small and mid-size businesses, for example in plant and general engineering, and component suppliers in the automotive industry. And it is a timely response to the challenges associated with the growing volume of data exchanged by laboratories, factories, and warehouses operated by manufacturers, suppliers and customers.

The made-in-Germany solution presented in Hamburg was developed with the input of Fraunhofer SIT, TRUMPF, Wibu-Systems and Hirschmann. Infineon supplies the chips that authenticate the identities of computers, routers and machines, ensuring only authorized individuals and non-manipulated devices are granted access to IT networks. Once authentication checks have been successfully completed, the data is encrypted and transmitted via secure telecommunications networks. Deutsche Telekom provides the secure, high-availability network infrastructure required for real-time connectivity. The company's contributions include secure cloud services, mobile end-points, and their seamless integration into processes and applications. A key role in delivering robust end-to-end protection is played by Deutsche Telekom's Cyber Defense Center.

Chip-based authentication of devices ensures that only authorized users gain access.

PROTECTING FRITZ!BOX ROUTERS FROM CYBER CRIMINALS

Deutsche Telekom first informed its customers of a weak spot in AVM's Fritz!Box routers in mid-February 2014. By mid-December, only 40 of the original 4,000 customers had WLAN routers that were still vulnerable.

In October 2014, Deutsche Telekom and AVM, a manufacturer of hardware products for broadband Internet and smart home networking, identified Fritz!Box routers where an essential patch had still not been installed. The users were contacted by Deutsche Telekom's customer service team, and a dedicated hotline was established. 99 percent had either downloaded the software update or exchanged the hardware by December 12, 2014.

The insecure WLAN router allowed cyber criminals to gain remote access. The hackers could then exploit the weak spot to use expensive foreign phone services at the cost of the victim. When Deutsche Telekom learns of potential vulnerabilities, such as those encountered with Fritz!Box routers, the company promptly notifies customers, and provides viable solutions. This also applies to email accounts that have been identified as the source of spam. Customers are prompted to change their passwords to prevent these unwanted messages from being sent.

PARTNERSHIP PROMOTES REAL-TIME CYBER DEFENSE

Since November 2014, Deutsche Telekom has been working with cyber security specialist FireEye to safeguard against cyber attacks.

Cyber security enterprise FireEye specializes in protecting networks from complex digital threats. Its security solutions detect and defend against targeted attacks, which may evade firewalls, antivirus software and other conventional defense systems. On average, cyber attacks in corporate networks go undetected for 229 days. During this time frame, the malware can potentially wreak havoc. FireEye, however, identifies threats within minutes and takes immediate action to resolve any issues.

Together, FireEye and T-Systems offer a fully-managed service to respond quickly to threats, and effectively protect organizations from IT espionage and cyber attacks. In 2013, the experts at FireEye discovered 11 previously unknown zero-day exploits. Most of these vulnerabilities were found in extremely popular programs, for example Internet Explorer and Adobe.

FireEye's solutions augment Deutsche Telekom's Advanced Cyber Defense (ACD) portfolio. This offering, developed by T-Systems, is tailored to the imperatives of major international corporations. It is particularly effective in safeguarding against under-the-radar attacks. These breaches often stem from malware propagated by sham email attachments or by malicious websites (drive-by downloads). To avoid infection, suspicious attachments are placed in a controlled environment. Once sandboxed, the files can be opened and the behavior of the suspicious data analyzed.

CONTAINERIZING SOLUTION FOR BUSINESS APPS

Business professionals often use their own smartphones for work purposes. This gives hackers a backdoor into corporate IT environments. Safe Mobile Business Apps can ring-fence applications, blunting this risk.

Bring your own device (BYOD) describes the use of personal endpoints in the workplace. According to a survey by Bitkom, Germany's leading IT industry association, seven out of ten workers in the country take advantage of BYOD. However, it can increase the risk of intruders exploiting commercial apps to break into an enterprise's systems. Deutsche Telekom's Safe Mobile Business Apps securely containerizes corporate apps. As a result, the IT team only has to manage a single container, not multiple apps. This allows employees to work securely with corporate data on their own tablets and smartphones. The container lets all apps on the device seamlessly communicate with each other. New security policies for individual apps, updates and entirely new programs can be loaded within minutes – fully automated, over the mobile network. Mislaid or stolen devices can be remotely disabled, and the data wiped. There is a dedicated solution for the central management of apps and content. Administrators can assign user rights on the basis of pre-defined roles. As a result, each employee is only granted access to the data and apps that they require for their work tasks.

HACKERS, MADE BY DEUTSCHE TELEKOM

Instead of scouring the job market for highly skilled, highly scarce IT security specialists, Deutsche Telekom works with the Cologne Chamber of Commerce to nurture their own experts. In 2014, the first ten participants began their Cyber Security Professional program.

Sandra Rutkowska is no greenhorn. She has just completed a formal three-year course in systems integration. But the 22-year-old's education is not over yet – she is one of ten Deutsche Telekom employees taking part in the Cyber Security Professional certification program. Over two and a half years, attendees with a variety of previous qualifications, including university degrees, will learn the ins and outs of IT security. This extends to learning the fine art of hacking. For Rutkowska, this is an exciting challenge: "I was familiar with the topic of IT security generally, but the complexity and depth of the subject are new."

MODULAR STRUCTURE

For Deutsche Telekom, developing their own IT security experts is an important arrow in their quiver – especially as external threats are growing in number and sophistication. "Despite rising cyber security expectations and needs, Germany still lacks adequate education programs and university degrees," explains Inge Rader, Vice President and HR Business Partner for the Data Privacy, Legal and Compliance Department at Deutsche Telekom. "Through in-house training, we provide our employees with opportunities for career development geared to real-world needs. We invest in their future, and at the same time protect our customers and their interests."

The program is a blend of theory and on-the-job experience. Participants are salaried employees, but also take time out to attend workshops and online seminars. These sessions focus on topics such as digital forensics, IT security theory, testing, and programming. Attendees also work on their soft skills, such as intercultural project management, presentation techniques, and structured discussion under pressure.

Module timing and sequence are flexible; the program can be structured according to individual needs, and offers opportunities to put newly-learned skills into practice. Participants are also given the chance to try their hand at hacking, exposing vulnerabilities in Deutsche Telekom systems, and developing appropriate solutions. Specially-trained mentors assist future IT security experts throughout the program.

EMPHASIZING SOFT SKILLS

New challenges call for new forms of education. At the end of their training in early 2017, attendees must pass examinations set by the Cologne Chamber of Commerce. Ulf C. Reichardt, the institution's director, explains how IT security impacts digitization strategies. "Digitization affects not only business processes, but the corporate culture as a whole," says Reichardt. "For companies, good communication is essential when it comes to security. In our Cyber Security Professional program, we place emphasis not only on technical knowledge, but also on soft skills such as the creation and presentation of security proposals and plans, and the management of complex projects."

In order to graduate, a final project must be submitted at the conclusion of the course. Participants are encouraged to describe and resolve a real-life case from their own immediate working environment. They present their results to the examining board. They are expected to demonstrate both their knowledge of technical solutions and their ability to put them into practice. The course also addresses how to handle sensitive information. "The human factor is just as important in IT security as the technology, and the Cyber Security Professional course teaches this as well. The program is a good example of how the Cologne Chamber of Commerce can offer its member companies practical support during the digital transformation. New challenges must be met through new forms of education."

"It does no good to simply lay all the blame on a lack of security experts. We must take action to tackle the issue," explains Inge Rader. "Our new IT security and data protection training programs provide the knowledge and skills necessary to transition from qualified IT expert to experienced hands-on security specialist. This is beneficial for both sides – our business gains highly sought after and highly qualified specialists. Our employees gain new skills and exciting career opportunities."

Deutsche Telekom is collaborating with the Cologne Chamber of Commerce to train employees to be experts in cyber security.

NEW DEPARTMENT AT LEIPZIG UNIVERSITY

In addition to the Cyber Security Professional program, Deutsche Telekom has created a new department and professorial chair for data protection and IT security at Leipzig University of Telecommunications (HfTL), funded by the company. For an initial period of five years, teaching staff and students will address the following questions: How can we raise awareness of data protection and security, both in the working environment and people's private lives? How can we minimize the risks associated with processing large quantities of sensitive data? How can software be made more secure, without negatively impacting user-friendliness and barrier-free design? The new department also aims to create new modular course elements to continuously improve IT security and data protection education. In the 2015/16 winter semester, the university will launch a new bachelor's degree, including a focus on data protection awareness, IT law and digital forensics.

Hochschule für Telekommunikation Leipzig
University of Applied Sciences

A BIG STEP UP

Alexander Schmitz is one of the first members of Deutsche Telekom staff to successfully complete the cyber security professional certification program.

Mr. Schmitz, you are amongst the first ten employees to graduate from the cyber security training course. What previous IT knowledge did you have?
I had already completed a three-year training program as a systems integration specialist, combining paid work at Deutsche Telekom with part-time studies. I then spotted the new training opportunity on an internal job portal.

Why did you apply?
I was attracted by the prospect of playing a key role in making the Deutsche Telekom world a little bit safer and in helping to effectively protect our customers' data. And I simply enjoy working in IT security.

Have you always been interested in IT security?
Not really. But the description of the training program and the first couple of assignments I was given in the department really fired my enthusiasm.

What do you expect to gain from the program?
I am looking forward to discovering a wide variety of things about IT security – and to applying that knowledge. I'm especially interested in cloud computing, virtualization and storage. And I'm really keen to play the role of a hacker, and experience the whole thing from the other side.

What will you be doing once you graduate?
Certification is definitely a milestone in my career. I can now envisage going on to university and gaining further security certificates.

DIGITAL GUIDE TO PROTECTING INFORMATION

The InfoSecWheel app shows Deutsche Telekom employees how to classify and process sensitive information.

Imagine this scenario: an employee from product development has a dilemma. A presentation describing the functionality of a future prototype is ready to be sent to his supervisor – who needs the slides for a meeting with top management. However, the information is sensitive and should not be made available to the general public. Should he simply send the file as an email attachment or does the data need to be encrypted?

CLASSIFICATION OF BUSINESS INFORMATION

Just to be on the safe side, he launches the InfoSecWheel app on his smartphone to reference company policy. The app, developed by the Group Security Governance department (GSG) for Deutsche Telekom employees, features two information wheels. It displays typical examples of business information, such as an audit report, management report, and a draft contract. The employee chooses the option that corresponds best to his file with a simple swipe across the screen. Based on his selection, the app indicates that the presentation is classified, and instructs him to label it accordingly.

LIST OF APPROVED DEVICES, SERVICES AND APPLICATIONS

The employee can then switch to the “handling of information” view where he learns that the presentation can be emailed if encrypted. The program also warns that an unencrypted email or scan-to-email is not permitted. Should there be uncertainty regarding how to properly encrypt the file, he need only tap the “approved products” option. This pulls up a list of approved devices, services, and applications for storage, editing and exchange. Filters can be applied so that only products authorized for use with classified information are displayed.

AVAILABLE AS A FREE DOWNLOAD

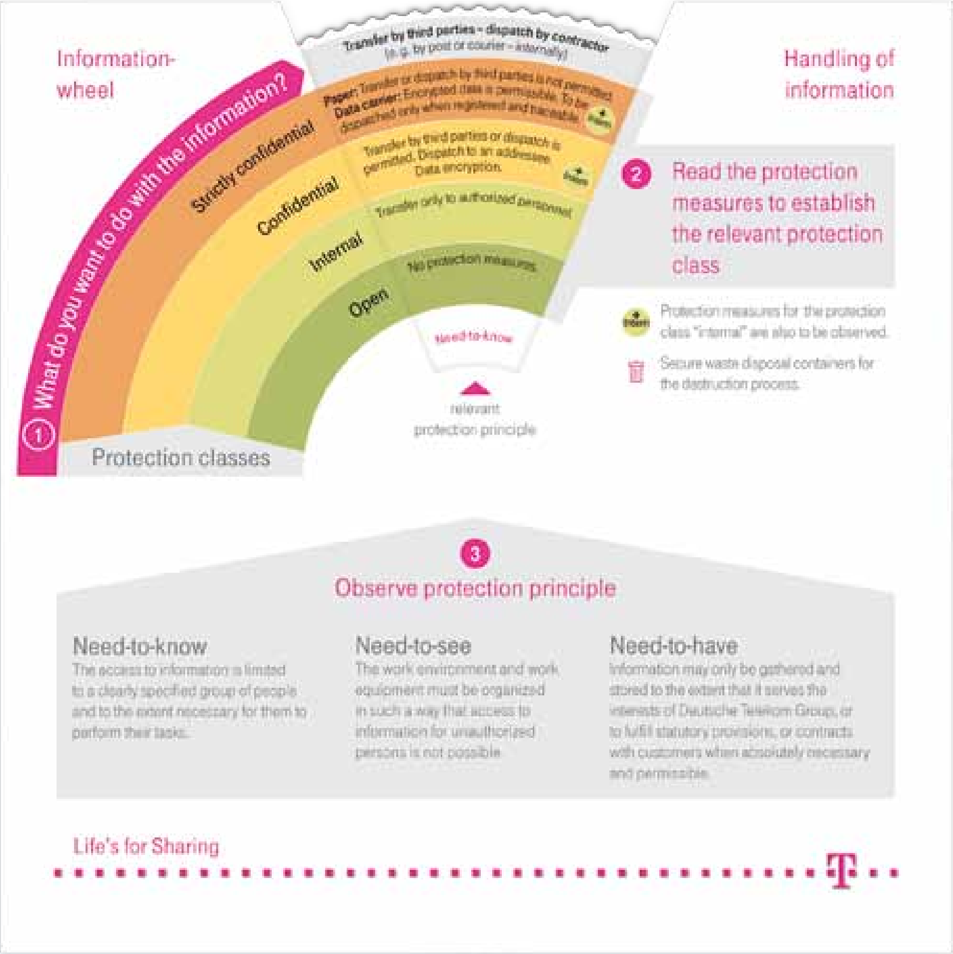
Under “additional information” the user can access a guide explaining the use of the product. In other words, with InfoSecWheel, Deutsche Telekom employees can now easily and quickly discover whether encryption is needed – without wading through hardcopy policy documents.

IT SECURITY OF THE HIGHEST CALIBER

Specialized auditors DQS took a long hard look at Deutsche Telekom’s information security management system (ISMS). Their findings confirmed that the organization effectively manages risks in accordance with ISO 27001.

DQS certification is proof positive that Deutsche Telekom has implemented robust processes to ensure consistently high enterprise-wide security. Within the ISMS, Deutsche Telekom’s security specialists have defined what information assets are subject to what risks. It also models the corresponding security management processes. In fact, Deutsche Telekom has created a comprehensive framework governing all areas and activities of relevance. This includes IT and network security, physical access control, and continuity and situation management. As ISMS supports all processes from end to end, it is an effective basis for security-related decision-making on the part of executive management.

DQS auditors also scrutinized the continuous improvement process integral to ISMS. This lets Deutsche Telekom’s security team systematically minimize residual risk. According to DQS’s internally defined benchmark, ISMS is a solution of exceptionally high caliber. Deutsche Telekom has implemented consistently high security standards worldwide – which are appropriate for the risks the company faces. The quality of ISMS reflects Deutsche Telekom’s commitment to effectively protecting the information assets entrusted to it.



Information-wheel

1 What do you want to do with the information?

Strictly confidential

Confidential

Internal

Open

Protection classes

Transfer by third parties – dispatch by contractor (e.g. by post or courier – internally)

Paper: Transfer or dispatch by third parties is not permitted. Data carrier: Encrypted data is permissible. To be dispatched only when registered and traceable.

Transfer by third parties or dispatch is permitted. Dispatch to an addressee. Data encryption.

Transfer only to authorized personnel

No protection measures

Need-to-know

relevant protection principle

Handling of information

2 Read the protection measures to establish the relevant protection class

Protection measures for the protection class "internal" are also to be observed.

Secure waste disposal containers for the destruction process.

3 Observe protection principle

Need-to-know
The access to information is limited to a clearly specified group of people and to the extent necessary for them to perform their tasks.

Need-to-see
The work environment and work equipment must be organized in such a way that access to information for unauthorized persons is not possible.

Need-to-have
Information may only be gathered and stored to the extent that it serves the interests of Deutsche Telekom Group, or to fulfill statutory provisions, or contracts with customers when absolutely necessary and permissible.

Life's for Sharing

InfoSecWheel is based on a paper information wheel, developed by GSG in 2012, already used by approximately 20,000 Deutsche Telekom employees. In the fall of 2014, the company decided to transfer this information to an app – enabling quick-and-easy content updates, and allowing the inclusion of additional information on approved security products. Deutsche Telekom employees can download the app from the in-house appstore. It is also available free to external businesses via the Google and Apple appstores. For a fee, InfoSecWheel can be customized, e.g. to feature the user organization's corporate design or a tailored list of security products.

AWARENESS OF SECURITY ISSUES AT PEAK LEVELS

Every year, Deutsche Telekom measures employee awareness of information security. The adopted benchmark is the Security Awareness Index developed by the Steinbeis Consulting Center. In 2014, Deutsche Telekom achieved the highest marks of all organizations studied by Steinbeis.

The index compares awareness levels of staff at companies in automotive engineering, banking, and IT. More than 30 national and international studies have already been conducted. Data is collected by means of an online questionnaire. In the past year, Deutsche Telekom randomly selected and invited 40,500 employees from a total of 57 organizational units to participate in the survey. The response rate has been the highest to date, at 45 percent.

Moreover, the findings of the 2014 study indicate that security awareness at Deutsche Telekom is at peak levels. On the SAI scale, which ranges from one to 100, the professionals at Deutsche Telekom in Germany scored 77.6 points. As a result, Deutsche Telekom in Germany not only outperformed all other companies in the cross-industry comparison – it also came out on top within the international Deutsche Telekom Group as a whole.

In addition to comparing performance across multiple industries, the SAI also provides insight into security awareness within each company. Furthermore, the questionnaire provides executives with feedback on aspects of security that require additional attention.

Deutsche Telekom has tasked security experts throughout the enterprise with addressing these weak points and with raising awareness of security management requirements. Particular weight is placed on executive training. Topics covered in the training sessions include information security and data protection, IT and network technology, physical access management, social engineering and social networks.

Publication details

Published by

Deutsche Telekom AG
Data Privacy, Legal Affairs and Compliance
53262 Bonn
Phone: +49 (0)228 181 4949
Fax: +49 (0)228 181 94004
Email: datenschutz@telekom.de
cert@telekom.de
www.telekom.com/dataprotection
www.telekom.com/security

Photo credits

Deutsche Telekom, BPA/Jesco Denzel (page 8), Bundesregierung/Kugler, Henning Schacht (page 6), Fritz Schumann, Valentina Vos, Fotolia, iStockphoto

Date of publication:
February 2015

www.telekom.com/dataprotection

www.telekom.com/security