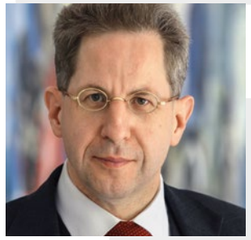
DATA PRIVACY AND DATA SECURITY REPORT 2015

LIFE IS FOR SHARING.

UPDATES
SECURITY POLICY
CYBERWAR
CRYPTOGRAPHY
INDUSTRY 4.0
INTERCONNECTIVITY
BIG DATA
BOTNET
SECRET CODE
REGULATION RULES
CYBERSPACE
INTEGRITY
DATA PROTECTION
CYBER DEFENSE CENTER
FIREWALL
VIRUS PROTECTION
BASIC RIGHTS
ENCRYPTION
DIGITIZATION
CONTROL MECHANISM
DDOS ATTACK
DATA PROTECTION OFFICER
RULES
IT SECURITY ACT
INFORMATIONAL SELF-DETERMINATION
PASSWORD
RULES
IT SECURITY
HACKER
CLOUD SERVICES
EU GENERAL DATA PROTECTION REGULATION
DATA MINIMIZATION
SELF-DETERMINATION
EMERGENCY PLAN

CONTENTS



DATA PRIVACY AND DATA SECURITY REPORT 2015

A KEY STEP TOWARDS FAIR COMPETITION

2015 was overshadowed by terrorism and the refugee crisis. It also ushered in fundamental changes with regard to data protection and security. Although EU members are still a long way from reaching a consensus on the humanitarian crisis, the European institutions have at least made a breakthrough in terms of agreeing on the General Data Protection Regulation. The legislation sets a high standard of protection, and enables new digital business models. Importantly, it now includes clearly defined rules – for example, for pseudonymization – and these apply to all businesses offering their services in Europe. This is a key step towards establishing fair competition between local telecommunications companies and leading Internet players based overseas.

The decision on the part of the Court of Justice of the European Union (CJEU) to invalidate the US-EU Safe Harbor agreement has also impacted transatlantic relations. The court ruled that, currently, European citizens' personal data is not adequately shielded in the US. The nullification of Safe Harbor has little effect on Deutsche Telekom, as we do not process any data that originated in Europe in overseas facilities. In fact, we stand to benefit from the ruling, if major corporations such as Microsoft decide to shift storage to our German data centers.

"DEUTSCHE TELEKOM DOES NOT PROCESS ANY DATA THAT ORIGINATED IN EUROPE IN OVERSEAS FACILITIES."

Additionally, in Germany, the IT Security Act (IT-Sicherheitsgesetz) has come into force. This mandates improved defenses and compulsory reporting of cyber security incidents. Encouragingly, the legislation also extends to hardware and software vendors, and to service providers. And at EU-level, member states are working towards a corresponding directive. We have to ensure the right safeguards are in place across the value chain, throughout Europe – only then can we truly enhance security.

Recently, the German Bundestag controversially decided to reintroduce the compulsory retention of telecommunications data by carriers. Deutsche Telekom cannot really judge how necessary this data is to the work of law enforcement agencies. It is up to these bodies to make their requirements and actions as transparent as possible, to persuade citizens of the value of data retention. Politics is faced with a delicate task: weighing up personal privacy and freedom against the needs of security. In light of terror attacks, people are more willing to favor greater security at the expense of certain liberties. However, we need to maintain the right balance – we are not protecting our freedom if we simply give it up.

Dr. Thomas Kremer

has been a Member of the Board of Management for Data Privacy, Legal Affairs and Compliance at Deutsche Telekom since June 2012. A lawyer by profession, he previously served as General Counsel at ThyssenKrupp; he assumed responsibility of the corporation's legal department in 2003. In 2007, he was appointed Chief Compliance Officer.

BEGINNING THE JOURNEY TO MODERN-DAY DATA POLICIES

2015 SAW A FLURRY OF LEGISLATIVE ACTIVITY IN THE DATA PRIVACY AND DATA SECURITY SPACE – RANGING FROM THE IT SECURITY ACT IN GERMANY, TO THE NIS DIRECTIVE, THE PNR DIRECTIVE AND THE GENERAL DATA PROTECTION REGULATION AT EU LEVEL.

DATA PRIVACY AND DATA SECURITY REPORT 2015

The German IT Security Act (IT-Sicherheitsgesetz) came into force in July 2015, and defines minimum standards for operators of critical networks – in the energy, water, healthcare and telecommunications sectors, for example. At EU level, the European Parliament and the Council of the European Union reached a consensus on the NIS Directive in December 2015. Similar to the German act, it is designed to ensure a high common level of network and information security across the EU.

Moreover, in December 2015, political agreement was secured on the EU General Data Protection Regulation – set to harmonize legislation in this area across the Union and strengthen the rights of individual citizens. Plus, the Data Protection Directive for the police and criminal justice sector is due to be finalized in the near future.

And, ultimately, the European Parliament and Council arrived at a compromise on the PNR Directive. This specifies the circumstances under which airlines must hand over passenger data to EU member states for criminal investigations. All in all, this represents an impressive amount of activity on the part of legislators, as the speed at which technology is developing creates significant pressure to act.

However, there is no need for politics to react to every digital fad – of which there are many. Internet 2.0 and Internet 3.0 were followed by Internet 4.0; after cloud computing came the Internet of Things and the fourth industrial revolution; big data has led on to big data for good; behavioral tracking and targeting and predictive analytics have been joined by artificial intelligence.

Each of these buzzwords may represent significant challenges for individuals and society as a whole. Yet careful and rational analysis is still required to assess whether policy-makers need to intervene. I have always taken the view that the same values should apply to the digital and analogue worlds. Surely we have long passed the point of drawing sharp distinctions between online and offline, or between digital and analog. The same approach must be taken in both spheres – the same methods, measured against the same values, and based on the same understanding of the role of government and of fundamental rights.

Certainly, different governance mechanisms and instruments are sometimes necessary in the Internet space. However, I fundamentally reject the idea that the online world requires a fully separate and distinct system of regulations and values. If we were to choose a term to encapsulate the challenges we will face, a concept that seems to take precedence above all else, it would surely be the word 'data'.

It appears everywhere, from 'data security' and 'data privacy', to 'big data' and 'open data'. Many hail it as the new fuel that will drive economic development. Digitization is seen as leading to 'datafication' – as various aspects of human life are converted into information that can be measured and analyzed by algorithms.

For some, this marks the dawn of a second Age of Enlightenment. The first era was defined by acquisition of knowledge of the material world. Now, we are gaining control over the material world through data and connectivity. For others, these developments are worrying: they fear that datafication of the individual will lead to the loss of human freedom.

Certainly, data and connectivity have become a central focus across business, R&D, and politics – so it is about time we started giving serious thought to creating coherent data policies. In this context, data security and data privacy are generally seen as two sides of the same coin. But an intelligent approach to policy must widen the lens to include questions beyond these conventional concepts. First and foremost: if data has become a commercial asset, what rights should apply?

Ownership of data per se remains an alien concept in today's legal environment. In copyright law, property rights apply to data collections and databases – but this is because the selection and organization of information constitutes a creative process. Competition and criminal law, moreover, can protect data as an industrial or commercial secret, and can impose limitations on its use. Otherwise, however, there is no legislation governing data ownership. All we have are laws governing freedom of the press, information and expression, and certain constraints on processing through data protection legislation.

But the current rules are not set in stone, and they may not be sufficient to master the challenges of the digital world. The Internet of Things – in the case of autonomous, connected cars, for example – raises complex questions of accountability, and issues of access and attribution, with regard to data from vehicles, machines, sensors, networks and buildings. The same applies to complex online networks with multiple stakeholders, including platform operators, cloud providers, and users of all kinds.

Particularly in debates on privacy, data tends to be treated like a physical thing – as though at any time, individuals could simply recover their information and withdraw consent to its use. But that's just not the technological reality. Suggestions as to how personal data could be commercialized – along the lines of usage rights of use under copyright law – point in the same direction. In contrast, the open data movement takes the opposite approach, striving to liberate information from any form of ownership.

Advocates of open private data go so far as to propose a duty on the part of private citizens to provide information. Even the recently finalized General Data Protection Regulation pursues two juxtaposed goals: the protection of individual citizens and the promotion of free data exchange.

Indeed, the question arises again and again of how far the state should go to protect its citizens – and at what point a resource (in this case, data) should be free from regulation. In its census ruling of 1983, the German Constitutional Court drew a line in the sand, stating that the individual does not have 'absolute' control over 'his' or 'her' data, and arguing that privacy must be seen in context. The right to have personal data safeguarded can be subject to limitations in cases where this benefits the greater public good. I would add that the protection of personal data also ends where the protection of other fundamental rights begins – particularly freedom of information, the press and expression, but also entrepreneurial freedom.

To pose a further question: what do we do when data privacy and data security are not two sides of the same coin – where data protection can harm privacy? Take for example, ICT service providers that wish to store communications data in their systems as a precautionary measure to help identify and thwart external attacks.

For reasons of data protection – and, as such, purportedly in their customers' interests – they are very limited in what they are permitted to do. But this is not always necessarily right. If we prevent ICT service providers from accessing customer data, and therefore make it easier for cyber criminals to hack into their systems, that is the very opposite of data protection.

Privacy is subject to the same changes and developments as society itself – and in the digital age, privacy can no longer be protected by legislation alone.

There are many issues we need to address, and not just data privacy and security. What about anti-discrimination rules, controls on big data algorithms, investment in digital skills and mechanisms that enable individuals to control their own data? We need to discuss intelligent rules for platforms and online brokers, the principle of freedom of data exchange, and the once-only principle for the public sector. Plus, we must consider how we govern digital legacies, how we differentiate between personal and non-personal data, and how we respond to open data initiatives. And those are just a few points.

All of these issues are aspects of modern-day data policies. We are still at the start of this journey, and our mission over the coming years will be to shape those policies with intelligence and wisdom. ■

Dr. Thomas de Maizière

has been a Member of the German Bundestag since 2009. Before his appointment as Federal Minister of the Interior in December 2013, de Maizière was Federal Minister of Defense from March 2011 until December 2013, and Federal Minister of the Interior from 2009 to 2011. Born in Bonn, he held various political positions in the state governments of Mecklenburg-Western Pomerania and Saxony between 1999 and 2005 – including the posts of Saxon Minister of State for Finance, Justice and the Interior, and Leader of the State Chancellery of Saxony.

DATA SECURITY AND PRIVACY ARE IMPORTANT ISSUES FOR GERMANY'S DOMESTIC INTELLIGENCE SERVICE (BFV)

THE EXPONENTIAL RISE IN DATA VOLUMES AND THE INCREASINGLY INTERCONNECTED NATURE OF OUR WORLD GO HAND IN HAND WITH A GROWING NEED FOR DIGITAL SECURITY. BUSINESSES, RESEARCH INSTITUTES, GOVERNMENT AGENCIES AND POLITICIANS ARE ALL REGULARLY THE TARGET OF CYBER ATTACKS.

The frequency and intensity of attacks has risen sharply in recent years. A prime recent example was the cyber attack on the network that serves the German Bundestag – which we detected, and we brought to the attention of the Bundestag's Administration in May 2015. In other words, data security is very much part of our remit as Germany's national domestic intelligence agency (Bundesverfassungsschutz, BfV – also known as the Federal Office for the Protection of the Constitution). In cooperation with other government agencies, we actively combat cyber attacks. Naturally, our work in this and other areas brings us into contact with sensitive information. To balance our need for intelligence with data privacy imperatives, a comprehensive legal framework has been established, as well as control and monitoring mechanisms.

PROTECTING INTELLECTUAL PROPERTY AND DATA

The globalized economy is driven by accelerating innovation and ever fiercer competition. Any advantage gained through innovation is quickly eroded. This is especially true of the German economy, which is highly knowledge-dependent. It is therefore vital to protect intellectual assets, for example confidential information related to development, production or sales.

In the digital age, attempts to gain vital business secrets are often launched electronically. Due to the technologies available to conceal and anonymize these attacks, it can be difficult to distinguish between those launched by competing companies and those emanating from government intelligence agencies. Our mission is to protect German businesses against industrial espionage – but not legitimate monitoring by market rivals – and against the competitive disadvantage that ensues from data theft.

The primary role of the German domestic intelligence agency is to precisely evaluate the level of danger. We analyze reported attacks, and attribute them to known sources – not least in order to instigate preventive measures. Where it has not been possible to thwart an attack on IT infrastructure, analysis serves to furnish insights that can be harnessed to alert and protect potential future victims. In cooperation with the intelligence agencies that operate at federal state level, we offer a broad range of information and practical advice to businesses looking to defend their digital estate.

CLEARLY DEFINED LEGAL PARAMETERS

The work of our agency entails data protection issues, and this is an important subject for us internally. We do not collect data en masse, nor without good cause, as is often claimed. Our cyber defense activities in the field of terrorism and extremism take place within clearly defined legal parameters. There are a considerable number of statutes that specifically govern our work, ensuring that sensitive and, above all, personal data may only be captured, stored and transmitted for very specific purposes. The framework includes the Federal Act on the Protection of the Constitution (BVerfSchG), the Security Clearance Check Act (SÜG) and the Article 10 Act (G10-Gesetz), to mention just a few.

The deployment of informers and surveillance staff, and the monitoring of telecommunications, is only considered when all other means of gathering information have been exhausted, or hold out no prospect of success.

The Article 10 Act includes provisions that, under strict conditions, allow the BfV to override the constitutional right to confidential mail and telecommunications expressed under Article 10 of Germany's Basic Law. Importantly, this must be a targeted interception, directed specifically and precisely at individual persons.

CLOSE MONITORING AND DATA PROTECTION

The work of our agency is not just subject to clearly defined legal parameters. It is also closely monitored. The BfA is directly supervised by the Federal Ministry of the Interior (BMI). Furthermore, we are overseen by the German Bundestag and its various bodies and committees. There is the Parliamentary Control Panel, the Budget Committee, and the G10 Commission. The latter determines the permissibility and necessity of the activities mentioned above that curtail the constitutional rights enshrined in Article 10 of Germany's Basic Law. The Parliamentary Control Panel has extensive powers, including the right to view records, and the right to enter all intelligence agency offices – including not just our own offices but also those of the foreign intelligence service (BND) and the military counter-intelligence service (MAD).

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) is responsible for the very specific task of data protection. She acts in accordance with the Federal Data Protection Act (BDSG) and the Federal Act on the Protection of the Constitution (BverfSchG) to ensure that the BfV always operates in compliance with its data protection obligations. The Commissioner is entitled to full disclosure, and has the right to access records, including stored data and IT programs of relevance to her oversight role. She is further entitled to enter any office at any time. This right has been invoked on occasion.

In addition to external controls, we also have our own internal mechanisms designed to ensure compliance with data protection legislation. This task is performed by the agency's own data protection officer, as mandated by the Data Protection Act. In order to guarantee the officer's autonomy, he is employed as a member of the senior management, and is not required to follow the instructions of any other intelligence service staff member.

Photo credit: BfV

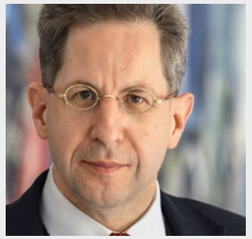
THE FUTURE OF DATA

Clearly, the existing and growing volume of sensitive data is forcing companies, citizens and government agencies to consider how this data is managed. Electronic attacks are of growing sophistication and precision, and it is increasingly hard to keep track of the myriad possibilities of misuse of personal data.

The statutory tasks of the BfV necessitate in a number of instances the capture and use of data, some of it sensitive. But we operate within clearly defined and transparent legal framework.

In the future, too, we will require robust data to safeguard businesses against cyber attacks, and to shield people from terrorism and extremism. To counter these threats, we need to exchange data, not only nationally, but also internationally – which raises further data protection issues. At the same time, the legally compliant and responsible handling of sensitive data is not only a duty, it is also an opportunity for us as an agency to strengthen public trust and confidence in our work.

Dr. Hans-Georg Maaßen



Has been President of the BfV since August 1, 2012. Commencing in 1991, Dr. Maassen worked in a variety of Directorates-General of the Federal Ministry of the Interior. In 2000 he was appointed Private Secretary to the State Secretary for Security. In 2001 he was placed in charge of the Project Group on Immigration, and in 2002 he was additionally named Head of Section for Law on Foreigners. In August 2008 he became Head of the Counter Terrorism unit within the Directorate-General for Public Security in the Federal Ministry of the Interior.

A BIG STEP FORWARD INTO THE DIGITAL REVOLUTION

THE END OF 2015 SIGNALLED A HISTORIC ACHIEVEMENT FOR PERSONAL DATA PROTECTION. IT MARKED THE SUCCESSFUL AGREEMENT BETWEEN THE COMMISSION, COUNCIL AND PARLIAMENT ON THE GENERAL DATA PROTECTION REGULATION, ALONG WITH THE POLICE AND CRIMINAL JUSTICE DATA PROTECTION DIRECTIVE, WITHIN THE 2015 TARGET REQUESTED BY THE EUROPEAN COUNCIL.

Together, we have secured a significant boost for two of President Juncker's top priorities for this Commission: the Digital Single Market and an area of justice and fundamental rights. These two instruments will benefit businesses, public administrations and citizens alike. And not a moment too soon.

The General Data Protection Regulation in particular actively responds to necessities in an era of rapid technological change, while building on and updating the sound principles of the original 1995 Directive. Since then, the Digital Revolution has brought important economic and innovative opportunities. But its fast-paced developments have left too much room for inconsistencies, uncertainties and administrative burdens, as companies struggle to understand and adhere to a patchwork of rules and conventions. This calls for a streamlined modernization of both business dealings and fundamental rights. We need data protection that is future-proof to pave the way for both innovation and the fundamental right to privacy, whichever technologies we choose to use. The new rules enable us to do this, by truly grasping the economic potential of the Digital Revolution, whilst providing citizens with the security they need to invest in business growth.

DATA PROTECTION: AN ECONOMIC ENABLER BASED ON TRUST

Data is the currency of today's digital economy, and citizens' confidence is the key to shared economic prosperity for all. Personal data contain and represent the life of an individual human being. Personal data cannot just be traded like a commodity, but they need protection. When it travels abroad, this protection has to travel with it. That is what our Charter of Fundamental Rights requires.

Fears of increased data protection damaging the economy are unfounded. In fact, it is citizens' insecurity regarding the handling of personal data that prevents businesses from growing. Six out of ten Europeans do not trust phone companies or internet service providers, and seven out of ten are concerned about their data being used for a different purpose than the one it was collected for. The Regulation provides a solution to these fears by creating a virtuous circle between robust privacy principles and safeguards and economic prosperity. With these principles and safeguards, citizens will be encouraged to unleash the economic potential of their personal data, whose value is predicted to grow to 1 trillion euros annually by 2020.

The Regulation also emphasises that data's cross-border economic potential depends on 'one law for one continent'. That is why the new rules replace 28 widely different laws with a single set of rules across Europe. This common framework is a key achievement, which brings legal certainty and protection for businesses and citizens across the EU. The Regulation's one-stop shop system also creates significant improvements in business efficiency. Companies will deal only with the national Data Protection Supervisory Authority of the country where their headquarters are based, regardless of how many countries they operate in. This will cut red tape and administrative burdens, giving companies the opportunity they need to expand. The new rules also encourage maximum protection for companies by advocating data protection by design and default. By making use of suggested cautionary measures like anonymization and pseudonymization, we aim to limit the risks companies face when processing large amounts of personal data, so as to avoid the fines foreseen for misuse of that data.

These robust rules will apply to all businesses offering goods or services to European citizens, whether these companies are European or not. This creates a level playing field for all businesses and secures sound protection for citizens, whoever is managing their data. At the same time, the Regulation avoids a one-size-fits-all policy, and instead allows for a rational risk-based approach, tailored to the nature of the activity of the business in question and the risks incurred for rights and freedoms of individuals. For example, only those businesses whose core activity is risky data processing operations are obliged to appoint a Data Protection Officer.

These measures should reassure citizens that their data is being handled on a secure and fair basis. Citizens must regain control of their personal data before they can be comfortable with businesses using it. Their right to protection of personal data is enshrined in Article 8 of the Charter on Fundamental Rights and it is our shared responsibility to protect this right. This includes the right to be forgotten, as well as the right to be informed of any data breaches. In fact, the new rules take the right to clear and accessible information on one's personal data as their starting point: citizens must be clearly aware of how their personal data is processed, including cases of data transfer. With free and informed consent, data portability between service providers will be facilitated, making both citizens' and businesses' lives easier. One thing is clear: the data subject must not become the data object. Citizens' right to personal data protection is crucial if businesses want to prosper.

A SAFER SAFE HARBOR

Of course, this right to personal data protection doesn't just apply to Europe. It goes for all data transfers both within and outside of the EU, including with the U.S. Establishing a safer Safe Harbour is a top priority for me. I have been working closely with our American counterparts to reach an agreement that benefits businesses and citizens on both sides of the Atlantic. EU citizens' fundamental right to data protection is our guiding priority, especially in light of the Schrems ruling.

Let me be absolutely clear: we also need the continuation of transatlantic data flows. They are important for our economy. I have already met with business representatives and fully understand their concerns after the suspension of the Safe Harbour. Companies need guidance, clarity and the assurance that the personal data flows so many of them rely on will be back on track as soon as possible. Alternative transfer arrangements are a temporary solution, and companies must always bear in mind necessary derogations in cases of public interest. But it is in all our interests to reach an arrangement that stays true to the standards of the Schrems ruling. This means robust safeguards for citizens' personal data. In a globalized economy, people must be assured that their personal data will be protected wherever it is sent, processed or stored. Only with these safeguards, trust in transatlantic transfers will be restored, and businesses will thrive.

In order for us to succeed in this, we need clear commitments from our U.S. colleagues. We are working very closely with them to achieve the right solutions as soon as possible. Negotiations are ongoing at the time of writing.

In the meantime, I welcome the General Data Protection Regulation as a victory for businesses and citizens alike. With this new streamlined system, we are set for a Digital Revolution where a thriving economy and fundamental rights go hand in hand.

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.

Photo credit: Chara Kaminara-Pipitsouli

“THE GENERAL DATA PROTECTION REGULATION STRENGTHENS THE STRENGTHS OF THE EUROPEAN IT INDUSTRY.”

IN MID-DECEMBER 2015, THE COUNCIL OF THE EUROPEAN UNION, THE EUROPEAN PARLIAMENT AND THE EUROPEAN COMMISSION REACHED AGREEMENT ON THE FINAL TEXT OF THE EU GENERAL DATA PROTECTION REGULATION (GDPR) – AFTER ALMOST FIVE YEARS OF NEGOTIATIONS. PARLIAMENT IS EXPECTED TO GRANT FINAL APPROVAL IN EARLY 2016. FOLLOWING A TRANSITIONAL PERIOD, THE REGULATION WILL COME INTO FORCE AT THE START OF 2018. DATA PROTECTION EXPERT JAN PHILIPP ALBRECHT, MEMBER OF THE EUROPEAN PARLIAMENT FOR THE GERMAN GREEN PARTY AND VICE-CHAIR OF THE COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, WAS THE PARLIAMENT RAPPORTEUR RESPONSIBLE FOR THE GDPR.

Mr. Albrecht, after five years of tough negotiations – are you happy with the final EU General Data Protection Regulation?
Jan Philipp Albrecht: We can all live with and work with the outcome. We have created a unified regulation from 28 distinct sets of national laws, laying the foundation for the digital single market in Europe. And this single level playing field – where everyone operates within the same competitive environment, under the same conditions – will benefit European enterprises in particular.

What level of approval does the current draft enjoy?
Jan Philipp Albrecht: Among the members of the lead committee in the European Parliament – the Committee on Civil Liberties, Justice and Home Affairs – and the permanent representatives of the Council of Ministers, over 90 percent voted in favor of the text agreed at the trilogue negotiations. Only Austria abstained from the Council vote, as they did not believe the proposal went far enough. In Parliament, three MEPs voted against the draft legislation as they thought the protections too strict. The next step is for the text to be formally approved by the plenary sitting of the European Parliament and by the Council of Ministers. In theory, it could still be rejected, but only if an absolute majority were against. Realistically, however, I don’t think there is any danger of this – ultimately, all political groups voted for the proposal at the committee stage.

What milestones does the regulation set, in your view?
Jan Philipp Albrecht: One major achievement is the inclusion of the point-of-consumption principle. This means that in the future, all companies delivering services to the EU market must comply with European data protection legislation, regardless of where they are domiciled. Failure to do so will incur severe penalties – as high as four percent of a company’s global annual revenues. This is a sharp sword in the armory of European justice. Moreover, the regulation strengthens consumers’ personal rights, particularly regarding transparency and the duty of data processors to provide information on their use of customer data. And it will be easier for citizens to understand these rights, allowing them to make informed decisions. For example, there is now a right to data portability: if a consumer wishes to switch providers, the current provider must make available all data stored on that customer. This translates into improved competition, as consumers can more easily move to a company that offers better information protection. In addition, the regulation has more clearly defined the right to be forgotten, and provided greater clarity on how it can be enforced.

But can the penalties really be applied? Might countries not differ in how strictly they enforce fines? That would mean certain players would be disadvantaged.
Jan Philipp Albrecht: We recognized this concern from the outset, and incorporated a mechanism to address it. Parliament and the Council have decided that, ultimately, a majority decision on the part of the European Data Protection Board can override an individual national authority. This board comprises representatives from the data protection authority of each member state. So if a national body imposes a penalty that is clearly too low or too high, the European body can correct it. And anyone can take invoke this mechanism.

Criticism has been levelled by parts of the business community that the regulation will hinder economic growth.
Jan Philipp Albrecht: No matter what agreement is reached, criticism from one corner or another is inevitable. But a clear majority has decided that the regulation represents a very good compromise. Particularly for mid-sized companies in the European Union, and especially in Germany, it marks a big step forward in comparison to the current state of play. Some might say we should have taken our lead from existing legal frameworks, such as that in Silicon Valley. But we would not have been able to secure a majority. In fact, I get the impression that the agreement will encourage major corporations from Silicon Valley to work to the standards we have defined. The US government, too, seems to be inclined to change its attitude. Here in the EU, we are taking the initiative in a positive sense – setting in motion a trend that will advance technologies that provide robust data protection. This will strengthen the strengths of the European IT industry.

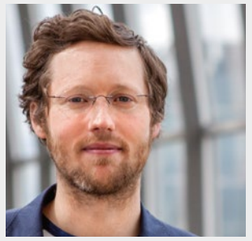
But national exceptions will still apply?
Jan Philipp Albrecht: Yes, that is true. In the public sector, in particular, we can only define basic principles. National legislation will continue to govern this sphere. Exceptions also apply in certain circumstances in the private sector: for example, to enterprises processing highly sensitive data such as genetic or biometric information. In these cases, the member states have reserved the right to define further standards. The same is true of employee data protection. We would have liked to have made progress in this area, too – but it was too early for that.

It has been claimed that the obligation to report data breaches has also been watered down.
Jan Philipp Albrecht: Parliament made it clear that this obligation may only be waived if a data processor can satisfactorily prove that there is no risk to the individuals affected. Otherwise, breaches must be reported. This represents a high burden of proof – so processors will presumably prefer to report an incident if there is any doubt.

Critics have suggested that the mandatory appointment of a data protection officer has been undermined.
Jan Philipp Albrecht: We need to look at this through a European lens. There are now standardized EU-wide rules on the appointment of data protection officers at business organizations. This marks significant progress for German enterprises, which have long been subject to provisions of this nature – while few other EU member states applied similar requirements. Moreover, the regulation changes the criteria defining which companies must appoint a data protection officer: it is less the size of the organization that matters, but how sensitive the data being processed. For me, that’s the more important factor. And if a member state believes these rules do not go far enough, it can pass additional legislation. So in Germany, the existing laws in this area will in all probability remain in place – insofar as legislators agree to this.

After five years of negotiations, you have finally arrived at your goal. What’s next?
Jan Philipp Albrecht: Data protection must continue to evolve in step with digitization, so the debate is far from over. Moreover, there are plenty of other directives linked to this issue in the pipeline – such as the revision of the E-Privacy Directive governing electronic communications, or the never-ending discussions on telecommunications data retention. ■

Jan Philipp Albrecht



Born in 1982 in the German town of Wolfenbüttel, Albrecht has a degree in law and joined the Green party in 1999. In 2009 he became the youngest German Member of the European Parliament. He is the Parliament’s rapporteur for the General Data Protection Regulation, and is Vice-Chair of the Committee on Civil Liberties, Justice and Home Affairs, and a Substitute Member of the Committee on the Internal Market and Consumer Protection. During his first term (2009 – 2014), he was a member of the Committee on Civil Liberties, Justice and Home Affairs, and a Substitute Member of the Committee on Legal Affairs. Moreover, between December 2012 and October 2013, Albrecht was a coordinator on the Special Committee on Organized Crime, Corruption and Money Laundering.

Photo credit: Fritz Schumann

THE GROUND-BREAKING RULING

SHAKING UP THE DIGITAL ECONOMY

THE COURT OF JUSTICE OF THE EUROPEAN UNION (CJEU) HAS RULED THE SAFE HARBOR AGREEMENT BETWEEN THE EU AND THE US INVALID – MEANING A NEW BASIS MUST NOW BE FOUND FOR TRANSATLANTIC DATA TRANSFERS. IF STRINGENT EUROPEAN PRIVACY STANDARDS ARE TO BE UPHELD, IT IS ESSENTIAL THAT US SECURITY AGENCIES DO NOT HAVE UNRESTRICTED ACCESS TO EUROPEAN CITIZENS' DATA. THIS IS NECESSITATED BY THE CJEU'S LANDMARK RULING IN THE CASE OF SCHREMS VERSUS FACEBOOK.

The media response made it clear that the Luxembourg court's ruling was a bolt from the blue. Few expected such a decisive ruling, on the heels of the legal opinion issued by Advocate General Yves Bot. The CJEU ruled the European Commission's Safe Harbor decision from July 2000 invalid, effective immediately, without a grace period. The court stated unambiguously that the level of personal data protection in the US is not adequate, as European customers' data is not sufficiently safeguarded against access by American security agencies.

The original European Commission decision declared the US a 'safe harbor': US companies could self-certify that they met European data protection requirements, under the oversight of the Federal Trade Commission (FTC).

INEFFECTIVE IMPLEMENTATION OF BASIC PRINCIPLES

On the basis of the Safe Harbor decision, over 4,400 enterprises had made a declaration to the FTC of their commitment to seven essential European data protection principles. However, these principles were not fully implemented at the companies themselves – and US legal protection for EU citizens affected by these practices is limited and not very effective. Moreover, following Edward Snowden's revelations, it became public knowledge that US security agencies are accessing personal information transferred to the country – to a far greater extent than was previously thought.

Photo credit: The Court of Justice of the European Union

This situation was inacceptable. Here in Europe, protection of personal data is one of our shared fundamental values – and it must be vigilantly safeguarded. For this reason, we at Deutsche Telekom began calling at an early stage for the existing Safe Harbor rule to be overturned, and replaced by a new system featuring more robust mechanisms. Following the CJEU ruling, the onus is on the German federal government, the European Commission and the US to take action. They must lay suitable foundations for data exchange between Europe and the United States. In our increasingly digital world, the secure transatlantic transfer of information is absolutely essential.

Following successful conclusion of the trilogue negotiations, the EU General Data Protection Regulation is set to be approved by the European Parliament in early 2016. It includes the 'country-of-reception principle', meaning that EU rules are applicable to all those who offer products and services in Europe – regardless of where the providers are based; whether in the EU, the US or Asia. Moreover, this union-wide legislation will offer a range of legal mechanisms for scenarios where data is stored outside of Europe. For example, companies will be able to apply for certification in line with the Data Protection Regulation. This ensures that providers from non-EU countries will also uphold European standards when they are processing information on European citizens.

TIME TO DISCLOSE DETAILS OF THE EU-US PRIVACY SHIELD

Any new transatlantic agreement on data transfers must not undermine these principles. We have to avoid a situation where US security agencies can access European citizens' information indiscriminately, and without oversight. This was made very clear in the CJEU's Schrems versus Facebook ruling. Under the status quo, Europeans' data is not sufficiently protected in the US. For this reason, the European Commission should disclose the details of the new EU-US Privacy Shield as soon as possible. Only then all stakeholders can judge whether the new agreement delivers on its promises.

Deutsche Telekom had already taken appropriate action before the CJEU ruling. First, we never process data generated in Europe overseas. Moreover, our major US partners store all information on German customers in our data centers in Germany. And in the rare cases where data is not processed in Europe, we make this clear to our customers. Plus, we have included data protection provisions in standard contractual terms with partners. In addition, German law defines specific requirements for commissioned (outsourced) data processing, and these are also incorporated into our contracts. Moreover, our Binding Corporate Rules or equivalent agreements apply to any and all data transfers within the Group.

If bits and bytes sent via the Internet no longer take a detour through legal jurisdictions such as the US, the transfer process as a whole will become more secure. For this reason, we at Deutsche Telekom have long advocated an approach whereby data takes a direct route from sender to recipient, and is not diverted through third countries. We have already implemented this in our networks. Our aim is to make it significantly more difficult for unauthorized parties outside the EU to access data transmitted within Europe, and we are taking steps to encourage as many Internet providers as possible to get on board.

Moreover, to ensure robust protection of personal data, it is important to address the issue of secure encryption. Effective end-to-end encryption – that is easy for consumers to use – strengthens safeguards, including against inappropriate access by security agencies.

For Deutsche Telekom, the CJEU ruling means we must proactively take responsibility. From speaking with our corporate customers, it is already clear that they take a critical stance toward their data being stored in countries outside the EU – and demand for cloud services 'made in Europe' is growing fast. Our encryption technologies provide an answer to the need for secure information transfer. And Deutsche Telekom guarantees the same high security standards in all its data centers, not just those located in Germany – standards that are subject to annual auditing and review.

When we partner with businesses from outside the EU, we require that their solutions reside on, and all data is processed on, our servers. If that is not possible, we insist that they abide by the EU's model contract clauses. If the company does not agree to include these clauses, we either do not use the service at all, or we explain the situation to our customers, so that they are free to choose for themselves.

Commentary by Board Member for Data Privacy, Legal Affairs and Compliance, Deutsche Telekom

EUROPE AND ITS "PRIVACY SHIELD"

IN 2016 IT HAS BECOME AXIOMATIC TO DESCRIBE DATA AS THE RAW MATERIAL OF THE 21st CENTURY. AND DATA IS, WITHOUT DOUBT, OF HUGE STRATEGIC IMPORTANCE TO THE DIGITAL ECONOMY – ESPECIALLY WHEN COMPETING WITH THE USA.

If we consider trends such as the fourth industrial revolution, big data and cloud services then one point becomes strikingly clear. If Europe fails to retain ultimate sovereignty over the data generated within its borders then it will quickly degenerate into a digital colony. In this context, a key part is played by data protection legislation, where there are considerable differences between the European Union and the US. With hindsight, the Safe Harbor model, now 15 years old, was a poor attempt to overcome the systemic differences between EU and US laws. It was tantamount to a blank check for US companies to import data as they saw fit. The first critical voices were raised in Europe in 2005. And in 2010 Germany's data protection agencies decided that German-based data exporters could not give complete credence to Safe Harbor certification of US companies.

ACHIEVING CONSENSUS WITHIN SOCIETY

In 2015 the European Court of Justice put the matter beyond doubt, ruling that the US did not currently have a degree of data protection comparable with that of the EU. As a result, the European Commission had little choice but to revoke Safe Harbor. But the decision comes far too late. Moreover, it is not just about whether and how European civil rights can be accommodated in the USA. It is about what kind of digital world we wish to live in. In Europe we must achieve a broad consensus across society with regard to the constellation of this world. This requires us to consider how we Europeans can, on the one hand, maintain control over our data, yet at the same time strengthen and develop transatlantic trade.

The success of negotiations on the transatlantic free trade agreement is being made dependent upon quickly finding a replacement for Safe Harbor by key decision makers. This is not an unnatural link to make, in light of the commercial importance of data – quite the opposite. The EU-US Privacy Shield unveiled in early February is intended to establish a data transfer model that establishes a secure shared data space. Within the scope of the TTIP negotiations and the efforts to put the EU-US Privacy Shield into writing, the European Parliament and the member states need to focus on the strategic significance of the digital economy.

For many years US companies were able to collect huge volumes of European data, and sell the digital products enhanced in this way back to us at a high price – via a process directly or indirectly legitimized by the US supposedly being a "Safe Harbor". This development increasingly relegates Europe to the role of a digital sales market. Furthermore, the economic consequences are worrying, as it goes hand in hand with a painful loss of skills and innovativeness. Without this ability to innovate, especially on the part of Germany's Mittelstand, an economy cannot grow, and this will have a direct negative impact on our standards of living.

USER-FRIENDLY SOLUTIONS FOR TRANSATLANTIC DATA EXCHANGE

We must act quickly to eliminate the legal insecurity created by the Safe Harbor ruling, as it has huge ramifications, especially for small and medium-sized enterprises (SMEs). SMEs need user-friendly solutions for transatlantic data exchange. Whether the new Privacy Shield can live up to its name, remains to be seen – starting with the final text of the agreement, expected in the next few weeks. It will need to prove itself in practice, and withstand renewed scrutiny through the ECJ.

The debate surrounding these issues, and the systemic differences that exist must not be allowed to damage transatlantic trade or to harm investment. At the same time the provisions of the new General Data Protection Regulation must be rigorously enforced. This is important if we are to regain the trust of Europe's citizens. We need to create a level playing field for European and non-European companies. This will only be possible if the renegotiated agreement fully complies with the ECJ's ruling – including effective data privacy. Only when the USA provides a level of protection equivalent to that of the EU, approval should be given for data to be exchanged between companies operating in separate economic areas. However, there are grave doubts to whether the new Privacy Shield will deliver on this point. The information we have is still too vague, and the commitments are too hazy, above all on the part of the USA.

INSIST ON THE POINT-OF-CONSUMPTION PRINCIPLE

Notwithstanding the above, we must, where personal data is key to a company's central business model, robustly implement the General Data Protection Regulation and the point-of-consumption principle embedded within it. The "I agree" checkbox business model of the big platforms must be consigned to history. This will require Europe to assert itself and its sovereignty in the digital arena. The companies affected are certainly equipped to fulfil these requirements, as they have ample computing resources in Europe.

The ECJ judgment is a prime opportunity to make good lost ground by at last obligating non-European businesses to observe a degree of data protection that has long existed in Germany and Europe – something that will be reinforced by the new regulation. Trust is not open to negotiation. And it would be a welcome move if political decisionmakers would act and not leave the responsibility exclusively to the judiciary. But industry players, too, are called upon to create the products that give companies genuine options. In this regard, Deutsche Telekom has been a pioneer in the cloud service space. For example, we host data for Microsoft and other global players helping to build trust. Because data that resides in Deutsche Telekom's data centers in Germany is subject to German law, safeguarding the rights of European citizens.

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.

TEN-POINT ACTION PLAN FOR GREATER CYBER SECURITY

FOREIGN INTELLIGENCE AGENCIES HAVE BEEN HARVESTING HUGE VOLUMES OF SURVEILLANCE DATA, AND CYBER CRIME HAS BECOME COMMONPLACE. THESE DEVELOPMENTS IMPERIL DIGITIZATION. SECURITY IS THE ACHILLES' HEEL OF A CONNECTED SOCIETY. IF WE ARE TO EFFECTIVELY PROTECT OUR DATA AND INFRASTRUCTURE, WE NEED GREATER TRANSPARENCY, CLEARLY DEFINED ROLES AND RESPONSIBILITIES, AND NEW SKILLS. AGAINST THIS BACKDROP, DEUTSCHE TELEKOM HAS DEFINED A TEN-POINT ACTION PLAN:

1. Edward Snowden's insights must be made public in their entirely. This is vital to identifying, and eliminating, online vulnerabilities.

2. EU member states should undertake to desist from spying on each other's telephone and Internet communications. The EU should continue its efforts to conclude a similar agreement with the US.

3. Security agencies should provide visibility into the information they request and receive on telecommunications and Internet users. This should include the quantity and type of information requests, and the quantity and type of connections monitored.

4. Business organizations must provide visibility into their security standards and the cyber attacks they suffer. The only way to ensure robust protection against online threats is to pool the information available to us. Deutsche Telekom has publically disclosed its technical security standards (www.telekom.com/sicherheit) and cyber attacks (www.sicherheitstacho.eu).

5. We must improve cyber security research and education. Deutsche Telekom has funded a department for data protection and security at the Leipzig University of Applied Sciences for Telecommunications (HfTL). Moreover, the company has launched Teachtoday.de: a platform that provides practical educational resources on cyber security and privacy for schools and others.

6. We must improve cyber analytics and forensics. To this end, companies need to reinforce their cyber emergency response teams (CERT), and foster greater inter-enterprise collaboration. Deutsche Telekom is actively pursuing this goal, and training the corresponding experts. In 2014, the company joined forces with the Cologne Chamber of Commerce to launch a new skills development program for cyber security professionals. In the near term, Deutsche Telekom will equip several hundred employees with the skills they need to become IT security experts.

7. In the mid-term, data should be encrypted at all stages of transmission, from end to end. The onus is on vendors, network operators and service providers to find simple, customer-friendly solutions. Deutsche Telekom is actively promoting the adoption of uniform encryption technologies in the standardization bodies where it is represented.

8. Network operators must avoid dependency on individual manufacturers of critical infrastructure components. Deutsche Telekom, for example, has a geo-redundant dual-vendor strategy in place – meaning it sources products from at least two manufacturers from differing regions.

9. Hardware vendors, software vendors, network operators and service providers must eliminate known weaknesses without delay. Deutsche Telekom will contractually oblige its suppliers to do so. In the case of especially critical components, product security should be verified by an independent body. The German IT Security Act (IT-Sicherheitsgesetz) and the corresponding EU directive need to address this issue.

10. Data transmitted over the Internet should not be routed via other jurisdictions. Deutsche Telekom's own network puts this principle into practice. And the company is urging all Internet service providers to undertake a voluntary commitment to do the same. This would make unauthorized external access of data transmitted within Europe far more difficult. ■

SECURITY FOR THE FOURTH INDUSTRIAL REVOLUTION

THE CONNECTED CAR PERFECTLY EMBODIES THE FUTURE OF DIGITIZATION, THE INTERNET OF THINGS (IoT) AND THE FOURTH INDUSTRIAL REVOLUTION. IT CAN REQUEST ASSISTANCE IN AN EMERGENCY, ORDER ITS OWN SPARE PARTS, ALERT OTHER CARS TO DANGERS IN REAL TIME – AND ULTIMATELY, WILL BE CAPABLE OF DRIVING AUTONOMOUSLY. BUT IT ALSO REQUIRES AN ENTIRELY NEW APPROACH TO SECURITY.

The vision of the connected, self-driving car suffered a minor setback in 2015. Chrysler recalled 1.4 million vehicles after hackers wirelessly hijacked a Jeep's brakes and air-conditioning system. And this was not just a one-off. On multiple occasions, hackers have managed to crack in-vehicle electronic control units in models from various marques. Thankfully, their only aim was to show it was possible.

These incidents shine a harsh light on the emerging risks confronting manufacturers in an era of increasing connectivity – of devices, machines, and even entire production processes. Industry stakeholders have recognized the dangers, viewing IT security as a major challenge en route to the fourth industrial revolution. According to a study published by VDE, Germany's leading association of engineers, 70 percent of decision makers believe IT risks are the greatest obstacle to connected manufacturing.

The kinds of attacks common today have the potential to seriously impact industrial manufacturing processes. They can result in theft of intellectual property and commercial secrets, disruption to production, physical damage to plant and machinery – and even falsified sensor data, and manipulated signals in control and instrumentation systems.

Comprising multiple active and passive elements, industrial IoT solutions are complex phenomena that pose significant security challenges. On the one hand, companies must safeguard their software, infrastructure and computing systems. On the other hand, they need to address how cyber attacks might impact the operational reliability of plant and equipment connected to the Internet. And security in the IoT age does not stop at an enterprise's front door, as corporate networks and systems are gradually opened to customers, suppliers and partners.

This makes end-to-end security management absolutely vital. Access to interfaces, systems, devices, sensors and (remote) maintenance ports must be limited to an authorized group of individuals and/or to defined processes. To ensure IoT solutions are both successful and safe, relevant features need to be preemptive, incorporated at the development stage. To date, security mechanisms have generally been reactive, added after the fact. What we need in the future is a proactive, integrated approach to product and process development – protecting both IT infrastructure, and industrial plant and equipment.

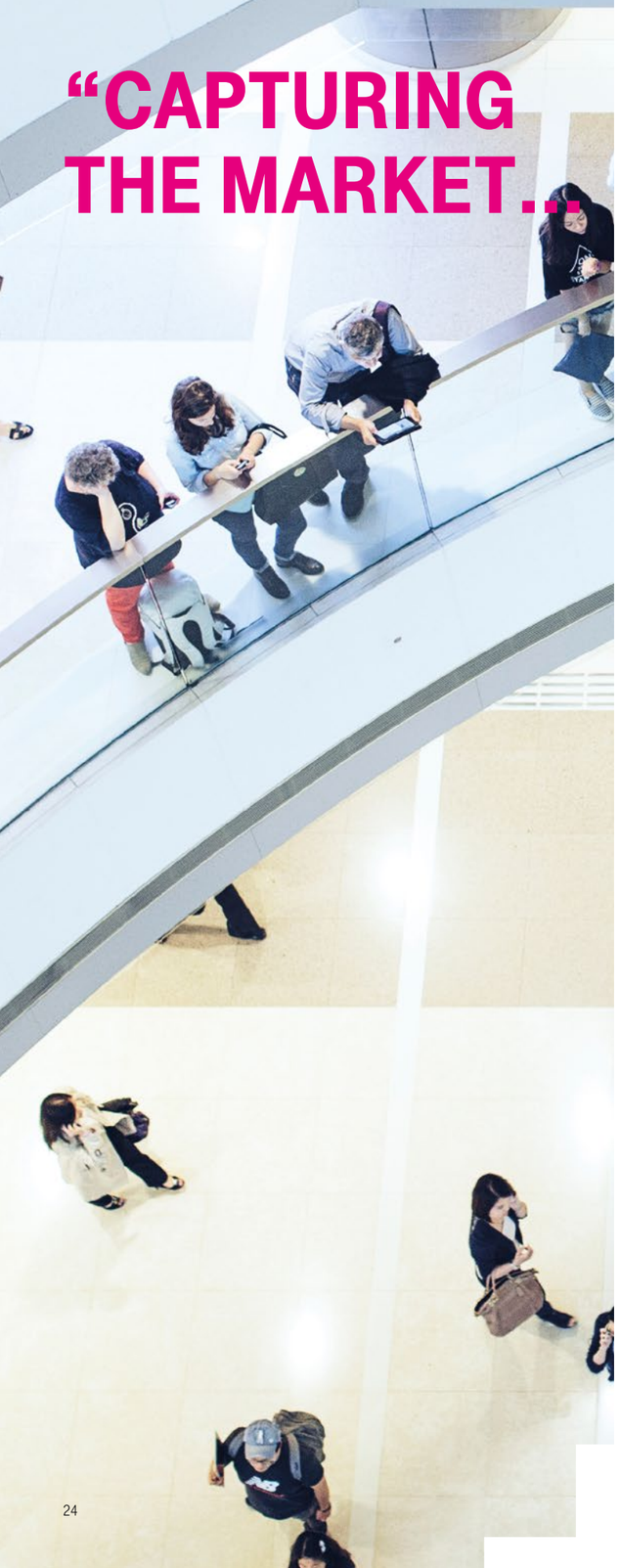
Industrial players are already taking action. The 2015 Cyber Security Report states that over half of all manufacturing companies are responding to growing digitization with IT security concepts tailored to their production processes. 45 percent have solutions in place to safeguard data exchange between production control systems and manufacturing equipment. A good thing, too, with Bitkom reporting that 44 percent of enterprises in key sectors are already deploying connected manufacturing technology. Moreover, according to a recent PwC study, industrial players plan to invest more in digital applications over the coming five years – to the tune of 3.3 percent of annual revenues on average.

If security fails to keep pace, the fourth industrial revolution could soon run out of steam. And this will have repercussions for growth in plant, mechanical and electrical engineering, the automotive and chemicals industries, agriculture, and information and communication technology. We must join forces across all sectors to prevent this from happening – the competitiveness of our manufacturing industry is at stake. ■

Reinhard Clemens

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

“CAPTURING THE MARKET...



UP UNTIL RECENTLY, DEUTSCHE TELEKOM’S INTERNAL AND EXTERNAL SECURITY ACTIVITIES WERE SPREAD ACROSS MULTIPLE DEPARTMENTS. NOW THEY HAVE BEEN BUNDLED WITHIN A NEW ORGANIZATIONAL UNIT: TELEKOM SECURITY. DR. FERRI ABOLHASSAN IS A MEMBER OF THE T-SYSTEMS BOARD OF MANAGEMENT AND DIRECTOR OF THE IT DIVISION AND TELEKOM SECURITY.

Mr. Abolhassan: Why is the decision for the market entry of Telekom Security so important, and why now?
Ferri Abolhassan: Because the time is right, in three senses: for the market, for our customers and for us. First, the market is growing – because cyber threats are growing, for consumers and for businesses alike. More than a third of German enterprises are, by their own admission, subject to cyber attacks several times a week or daily. And nine out of ten have fallen victim to IT criminals. Secondly, companies are under pressure to digitize their business models. According to our latest Cyber Security Report, almost 90 percent of business and political decisionmakers believe that IT security is the greatest challenge to implementing the fourth industrial revolution. And, third, as Deutsche Telekom we have the advantage, so to speak, that comes from encountering and managing cyber threats on a daily basis. It is precisely this expertise and experience gained over many years, that we are now combining with our security skills in terms of networks, data centers and customer-facing consulting services. This will be complemented by Germany’s strict data protection legislation and our own high security standards – to just mention the most important points. This mix is what makes us distinct and what gives us clear competitive differentiation.

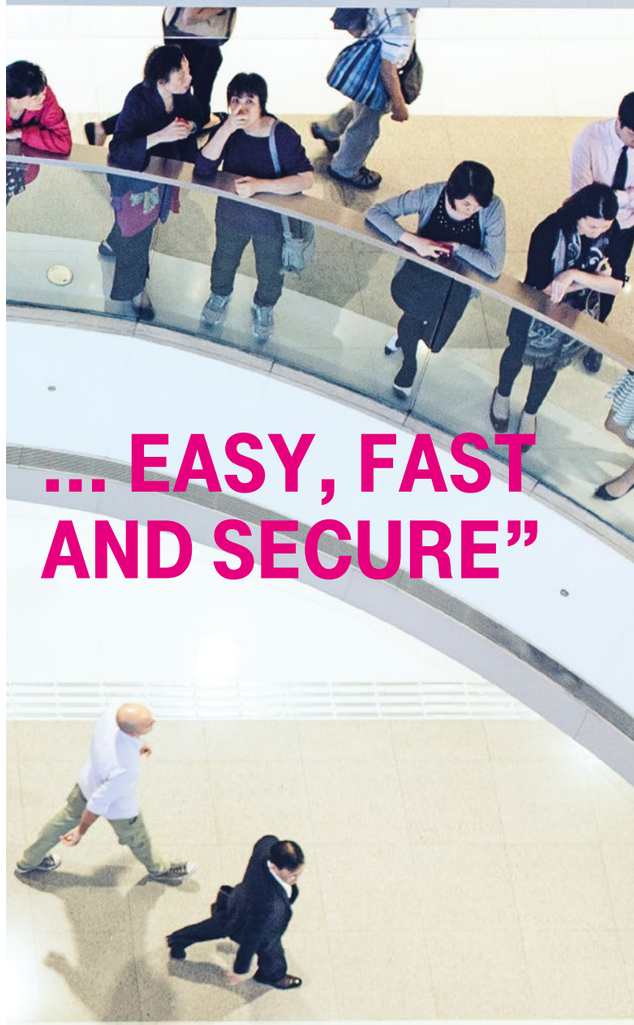
Apropos digitization – why is Deutsche Telekom the best choice to help companies achieve digital transformation?
Ferri Abolhassan: Experton very recently named us as just one of seven IT providers from a field of almost 600 to have a comprehensive offering in this space. In other words, they are saying that only this small group of players is capable of providing end-to-end support for digital transformation. That underlines the quality of our work, and is proof positive of our key role in digitization. We have the complete package: a secure network infrastructure, more than ten years of cloud computing experience with our customers, including the largest single SAP HANA installation for big data, high-performance data centers and SI expertise – to name just a few key elements. And very significantly, the whole thing is married to our own high standards in terms of quality and security. Security is part of our DNA. Data protection and security have always been part and parcel of what we do – that includes our own internal cyber defenses, our data centers, and the products and solutions we offer to our customers, both consumers and businesses.

As Director of the IT Division you are responsible for 6,000 business customers, including DAX-listed and Fortune-500 companies – what kind of challenges do heavyweights of this kind face?
Ferri Abolhassan: Let us face the facts: our customers’ overriding concern is to run a successful business. That applies as much to a mid-size player as it does to a global giant. So they need their conventional IT environment to continue to operate reliably and securely. But they also need to reinvent themselves as digital enterprises; to launch new business models and services, to innovate. That means IoT technologies, big data, the cloud and so on. But security is a precondition for digital transformation. The CIO of one of the world’s largest companies recently summed up the dilemma as follows: security slows down innovation, but a cyber attack slows down innovation even more. When it comes to digital transformation, one cannot exist without the other.

... which means?
Ferri Abolhassan: ... which means Telekom Security’s mission will be to rapidly provide end-to-end solutions. We will make digitization secure and reliable. Telekom Security will make it possible to offer and implement security across the entire value chain. But as is the case with many other core business markets, we are not doing it all on our own. I am a firm believer in smart partnerships that are disruptive and capable of capturing market share more quickly ...

... market share is the watchword ...
Ferri Abolhassan: Exactly, the German IT security market is currently worth 10.8 billion euros and expanding by 7.5 percent annually. We are already No. 1 in Germany, but want to extend our lead with new solutions and disruptive partnerships. Telekom Security will enable us to monetize our knowledge, and to convert it into business and growth. Our objective is to achieve international market success by means of a comprehensive offering for consumers, mid-size companies and global corporations. Our stated goal is to become No. 1 in Europe.

With what kind of solutions?
Ferri Abolhassan: A prime example is Cyber Defense as a Service. This delivers context-sensitive real-time monitoring of networks and systems. This enables us to identify and counteract attacks far faster – before any damage can be done. This is provisioned as a standardized service from the cloud, or on premises, and aimed particularly at mid-size players. We have already successfully piloted the offering with a number of customers. Overall, our range of products and services makes us uniquely equipped to provide end-to-end security – including end-points and cloud-based applications at the customer site, within the network infrastructure and at our data centers.



... EASY, FAST AND SECURE”

Dr. Ferri Abolhassan

Is a Member of the Management Board of T-Systems International and Director of the company’s IT Division. Between 1992 and 2001, and again from 2005 he held a number of senior management positions at SAP, most recently as Executive Vice President, Large Enterprises, EMEA. In 2008 he was named Chief Systems Integration Officer at T-Systems and appointed to the Management Board.

DATA – A RAW MATERIAL WITH A DIFFERENCE

MANY DIGITAL BUSINESS MODELS REVOLVE AROUND PERSONAL DATA – FROM SEARCH ENGINES TO ONLINE STORES, SOCIAL MEDIA TO APPS. ENTERPRISES MUST PROTECT THIS DATA, WITHOUT FALLING BEHIND AS THE ECONOMY EVOLVES.

For tomorrow's businesses, one ingredient will be key to success: data. Speaking in mid-September 2015 at a CDU party conference on digital transformation, German Chancellor Angela Merkel predicted that data will become as integral to the economy as coal and steel. An apt comparison for what many call the 'raw material of the future' – and an assessment that is hard to dispute. There can be no doubting the importance of data. Whether they are capturing, analyzing, processing or managing bits and bytes, firms across industries are witnessing a revolution in their business models.

Yet there is one major difference separating this resource from the raw materials of the past. Unlike steel and coal, personal data is generated by living people – and inextricably linked to their lives. Moreover, even after this information has passed into a company's possession, it continues to be protected by law. While business has a justifiable interest in the wealth of information being produced, individuals must be able to retain ultimate control of their data. Because in reality it is not a raw material like any other. And if consumers are to trust digital business models, privacy and security must be guaranteed.

BALANCING INTERESTS WITH THE RIGHT LEGAL FRAMEWORK

In Germany personal information is safeguarded by the Federal Data Protection Act, and most key aspects of this law will be upheld by the European General Data Protection Regulation. Negotiations on this EU legislation were concluded in late 2015, although its provisions will not come into effect until 2018. For the majority of citizens and the European business community the regulation's harmonized approach to personal data is a welcome development.

However, some critics in the corporate world continue to express concerns. In spite of all we learned from Edward Snowden, they fear stringent data protection rules could jeopardize the future viability of the German and European economies. Particularly during negotiations on the EU regulation, they repeatedly rolled out the same simple argument: data is the lifeblood of digital business models – and if restrictions within Europe are tighter than elsewhere, EU-based companies will fall behind the global competition.

BUILDING PRIVACY INTO BUSINESS MODELS

Data differs from conventional raw materials. Companies cannot simply extract and use it as they wish – they must respect the fact that under German legislation, citizens have the right to retain ultimate control of their data. Against this background, it becomes crucial to handle personal information with utmost care to maintain customer loyalty, and ensure long-term business success. As long as a company does not have a de facto monopoly, consumers are free to place their data with other providers. With coal and steel, it was a different story.

The German Federal Data Protection Act and the forthcoming European General Data Protection Regulation deliver legal security. They make data protection a key element of any business model, just like cost control, market analysis or marketing strategies. If data is a resource, it should be treated accordingly – sparingly and with care. Maximum transparency is a must. People need to understand what is happening to their information, so they can say 'no' if they wish.

THINK BEFORE YOU ACT

In business as in life "think before you act" is advice well heeded. If at an early stage enterprises spend time identifying how exactly they will use the data they gather, they will save money in the long run. After all, data is only worth something if you understand how it will benefit your business ideas. Data protection officers are not the only employees who require robust solution planning. The IT department, too, needs to know what they should develop in terms of application functionality.

For many digital business models it is unnecessary to process personal information as identifiable data. If you wish to improve public transport planning, say, you do not need to know exactly who is travelling. In such cases, personal data can be anonymized or pseudonymized. With pseudonymization it is possible to trace data back to the person it came from. However, customers must give their permission for this, which they are more likely to do if data analysis benefits them directly – for example, if it helps improve their medication.

TRANSPARENCY AND CONTROL FOR INDIVIDUALS

Data privacy and transparency can be competitive advantages, too – something US businesses have already recognized. Take Microsoft, for instance, which has selected Deutsche Telekom as the data trustee for its cloud offering in Germany. Microsoft customers can now opt to have their data safeguarded in line with the stringent requirements placed on German businesses. Moreover, they have full visibility into how data is managed. This arrangement gives customers a choice regarding the level of protection they require. For all companies, transparency should be the guiding principle when working with personal information. If default settings are geared toward privacy, consumers have the power to decide for themselves – increasing customer acceptance and satisfaction.

However, that is just the beginning. With the dawn of Industry 4.0 and the Internet of Things, business models will emerge based on ever more complex data relationships. It will be difficult to determine who has permission to access what information, when and where – and what they may do with the data they capture. This makes it essential to create a legal framework that will provide companies with legal security and transparency when designing new products. To do that, it is crucial to clearly define who is responsible for which data.

GREATER DATA PROTECTION EXPERTISE

To make this scenario a reality, companies must enhance their expertise. Data protection officers should be actively involved in implementing all business ideas. Just as some companies now have a Chief Digital Officer (CDO), it is becoming increasingly important to appoint a CDPO – a Chief Data Privacy Officer. Deutsche Telekom is a pioneer in this regard, and by taking this step we have gained an edge in the ICT sector when it comes to customer trust. The only way to achieve genuine sustainability is by ensuring transparent data management – and certainly not through unbridled exploitation of information for short-term success.

So which core principles should form the foundation of the digital economy? Care, when dealing with data that has been entrusted to us; transparency, toward the individuals affected; and privacy by design when it comes to technology, including deploying pseudonymization and anonymization as required. If all companies apply these principles across the board, competitive disadvantage will not be a concern.

Dr. Claus-Dieter Ulmer

is Senior Vice President of Group Privacy at Deutsche Telekom. He holds a doctorate in law and has worked as a corporate lawyer. Dr. Ulmer was previously responsible for data protection at T-Systems International and debis Systemhaus.

INDEPENDENT WATCHDOGS

Deutsche Telekom's Data Protection Advisory Board is an independent body that offers guidance to the Board of Management. It also facilitates constructive dialog on relevant issues with recognized experts and opinion leaders from the worlds of business and politics, universities, and non-governmental organizations. Established in February 2009, the Board complements Deutsche Telekom's internal privacy and security specialists by providing an autonomous, external perspective, and insights from diverse stakeholders.

The Board has wide-ranging responsibilities. It assesses business models and processes in terms of how customer and employee data is handled, evaluates the status of IT security and whether current mechanisms are suitable and reasonable. It discusses international data privacy issues and the implications of new legislation. In 32 meetings held over seven years, the Board has formulated 158 recommendations. To date, Deutsche Telekom has implemented or started to implement all proposed changes.

In 2015 the original twelve-member board was expanded to include former Federal Commissioner for Data Protection, Peter Schaar. Four meetings were convened during the year. The main topics of discussion were new digital business models (for connected health, for example), the new process for detecting data misuse, and the impact and imperatives of current regulatory issues. The latter include the European Court of Justice ruling on Schrems versus Facebook, Germany's IT Security Act (IT-Sicherheitsgesetz), the German data retention act, and last but not least, the EU General Data Protection Regulation.

STATUS REPORT ON DATA PRIVACY

Immediate termination of contract – A call-center partner was audited in December 2015 and found to be employing an unauthorized subcontractor, who had been provided with customer data. This serious violation of the company's data-processing agreement with Deutsche Telekom led to the immediate termination of the contractual relationship.

Customer Center app – The Customer Center app lets users manage their cellular and landline accounts from any location. A small number of users reported that the cellular functionality of the app displayed incorrect data. In May, Deutsche Telekom disabled the entire app as a precaution and subsequently reactivated landline account management. The cellular portion remained offline. No other Deutsche Telekom applications were impacted. Customers using Android and iOS devices were offered an update that restored the app's full functionality.

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, and Rapporteur of the European Parliament for the EU General Data Protection Regulation
- **Wolfgang Bosbach**: CDU, Member of the Bundestag and Chairman of its Committee on Internal Affairs
- **Peter Franck**: Board Member of the Chaos Computer Club (CCC)
- **Professor Dr. Hansjörg Geiger:** Guest Professor of constitutional law at Goethe University Frankfurt and State Secretary at the Federal Ministry of Justice from 1998 to 2005, former President of the Federal Office for the Protection of the Constitution, and of the Federal Intelligence Service
- **Professor Peter Gola:** Honorary President of the German Association for Data Protection and Data Security (GDD), author/co-author of numerous publications on German data-privacy legislation
- **Bernd H. Harder:** Attorney, Board Member of Bitkom, Germany's leading IT industry association, professor at Stuttgart Media University and the Technical University of Munich (TMU).
- **Gisela Piltz:** Member of the FDP's national executive and Deputy Chair of the FDP in North Rhine-Westphalia
- **Gerold Reichenbach**: SPD, Member of the Bundestag, Member of its Committee on Internal Affairs (rapporteur on data protection and privacy, and on civil protection and disaster management)
- **Peter Schaar:** Former Federal Commissioner for Data Protection and Freedom of Information (BfDI), and Chairman of the European Academy for Freedom of Information and Data Protection (EAID)
- **Dr. Gerhard Schäfer:** Former Presiding Judge at the Federal Court of Justice (BGH)
- **Lothar Schröder:** Chairman of the Data Protection Advisory Board, Member of the National Executive of ver.di labor union, and Deputy Chairman of the Supervisory Board of Deutsche Telekom, Member of the Bundestag's Committee of Inquiry on the Internet and Digital Society
- **Halina Wawzyniak:** Die Linke (The Left Party), Member of the Bundestag, Spokesperson of the Committee on Legal Affairs and Consumer Protection, Member of the Committee on the Digital Agenda
- **Professor Dr. Peter Wedde:** Professor of Labor Law and Law in the Information Society at Frankfurt University of Applied Sciences, Director of the European Academy of Labor (EADA) at Goethe University Frankfurt

DATA PRIVACY AND DATA SECURITY REPORT 2015

CREATING TRUST

In mid-December 2015 news broke that the trilogue negotiations on the EU General Data Protection Regulation (GDPR) had reached a positive conclusion. The skeptics were quick to respond. The BVDW (The German Association of the Digital Economy wrote "European legislators have not succeeded in defining up-to-date and future-proof rules for handling data in the 21st century". And the German Advertising Federation (ZAW) believes the regulation means significant legal insecurity for businesses.

Why does the business community find it so hard to embrace data protection? Is the problem privacy per se or is it the frequently cited lack of a level playing field – especially for companies whose business models are based on data?

The GDPR is designed to overcome this disparity. It will force non-European companies to handle personal data in the same way as European, and in particular German companies who had previously been at a competitive disadvantage. But the regulation goes further. It focuses on the consumer – quite rightly. Because consumers are more concerned about their personal data than businesses think.

This is underlined by the disastrous findings of consumer trust surveys. A representative study into big data carried out by TNS Infratest generated the following headlines: "Distrust reigns in Germany", "Almost half of all citizens distrust companies when it comes to data privacy" and "Germans concerned about their data being passed on to third parties". TNS Infratest polled more than 8,000 people in eight European countries. Most respondents are wary of almost everyone: the government, banks, telecommunications carriers, search engines, social network providers. In other words, trust has been shaken to the core.

So on one side there are cantankerous representatives of the business world; on the other distrustful consumers. And how do we resolve this paradox? Businesses should serve society and its needs, not the other way around. Ultimately, data protection is customer service. If citizens and customers want greater privacy, then businesses are best advised to supply it. They need to regain the trust they have lost. And it is important to note that Deutsche Telekom set out on this journey a long time ago. The company has undertaken to robustly protect its customers' data, and often shows greater sensitivity in its application of privacy rules than the law demands. This ensures that its business model will last. In fact, I am convinced that sooner or later Germany's and soon Europe's strict data protection provisions will prove to be a popular export. The EU General Data Protection Regulation, that is likely to be enacted in 2018, is being used as a template by non-European nations.

Photo credit: Kay Herschelmann

One thing is for sure: Deutsche Telekom already benefits from its sensitive management of data. This is reflected in the 2015 Security Report, which found that of all telecoms and Internet providers, Deutsche Telekom enjoys by far the greatest degree of trust amongst the German population when it comes to handling personal data. The organization secured the confidence of 46 percent, far more than the two companies in joint second on 24 percent. In other words, Deutsche Telekom is travelling in the right direction, but there is still a way to go. Our goal must be to persuade even more people of our trustworthiness through secure systems, the forward-looking design of new products, and through employees and senior executives who are both knowledgeable and sensitive to the issues. To this end, the Data Protection Advisory Board formulates recommendations. The body comprises experts with a variety of perspectives; its members are drawn from many work groups and institutions. But we all have one thing in common: the belief that robust data protection generates competitive advantage and serves people's interests.

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.

THE UNWELCOME RETURN OF TELECOMMUNICATIONS DATA RETENTION

IT'S OFFICIAL: DATA RETENTION IS BACK ON THE AGENDA. ON DECEMBER 17, 2015 NEW LEGISLATION MANDATING EXTENSIVE CAPTURE AND STORAGE OF TELECOMS AND INTERNET METADATA CAME INTO FORCE IN GERMANY.

From July 1, 2017 onwards, providers of public telephony services will again be legally obligated to record phone numbers and other identifiers of individuals making and receiving calls, together with call times and duration. Internet providers must store users' IP addresses. For mobile telephony it will also be mandatory to retain data on the cell phone tower accessed at the start of the connection.

Will forcing telecoms firms to store data on their customers' communications activities make Germany a safer place? The primary argument of the supporters is that it is a vital weapon in the fight against terrorism. And since the attack by Islamist terrorists on the Paris offices of the satirical magazine Charlie Hebdo in January 2015, calls from German politicians to reintroduce this legislation have been growing louder.

A BREACH OF FUNDAMENTAL RIGHTS

On March 2, 2010 the German Constitutional Court struck down the 2006 telecommunications data retention act, declaring it incompatible with the country's constitution. On April 8, 2014 the Court of Justice of the European Union (CJEU) declared the EU's Data Retention Directive invalid, as it was in clear breach of the Union's Charter of Fundamental Rights – both with regard to the respect for private life guaranteed under Article 7 and the protection of personal data safeguarded under Article 8. The court ruled that extensive, long-term retention of an individual's information, applied indiscriminately and not restricted to a particular geographic zone represents a far-reaching infringement of basic rights that cannot be justified by legitimate aims of criminal prosecution, protection against genuine threats, and counter-terrorism. The crucial point to the court was that the overwhelming majority of citizens affected by this legislation are not suspected of any crime.

Calls for a new data collection regime are part of a pattern that emerged in response to 9/11. This prompted an expansion of surveillance across the globe. However, we know today that the world was not made any safer as a result. In fact, data retention practices were never suspended in France, and remained in place even during the most recent attacks. But although French legislation requires data to be stored for a full 12 months, it was not possible to prevent the horrific murders of January and November 2015.

SIGNIFICANTLY SHORTER RETENTION PERIODS

Despite ever more studies attesting to the futility of blanket data retention in the fight against terrorism, a majority of Bundestag members voted to reintroduce the data retention act. Although the periods mandated – ten weeks for communications traffic data and IP addresses, and four weeks for location data – are significantly shorter than with previous legislation, the text has still come under fire. And rightly so, for the following reasons:

- It is an indiscriminate mechanism that overwhelmingly targets users of electronic services who have not committed any crime. Even normally privileged communications on the part of professionals such as doctors and lawyers are not exempt. Legal provisions restricting use of this data do not provide adequate safeguards.
- No evidence has been submitted to demonstrate the necessity of blanket data retention, and the encroachment on fundamental rights it represents.
- Terrorists and other criminals can evade the data retention provisions in a variety of ways – by using unregistered prepaid cards, for example, or over-the-top (OTT) services such as Skype, which are not under the same obligation to store data.
- As the volume of retained data grows, so does the risk of unauthorized access by perpetrators within and outside the telecoms company storing it. Combating these threats demands significant technological and human resources, the costs of which must ultimately be borne by customers and, in part, by taxpayers.

Seen in this light, it is completely understandable that appeals against the new legislation are to be brought before the Constitutional Court – with good prospects of success.

Peter Schaar

was the German Federal Commissioner for Data Protection and Freedom of Information (BfDI) from 2003 until 2013. In this role, Schaar was a member of the Article 29 Working Party comprising representatives from the data protection authority of each EU member state, and was Chairman from February 2004 to February 2008. Schaar is actively involved with the European Academy for Freedom of Information and Data Protection (EAID), and has been its president since September 2013. He is a member of the German Society for Freedom of Information (DGIF), the Hamburg Data Protection Society (HDG), the Humanist Union and the German Informatics Society (GI). Moreover, he is a Member of the German Green Party.

SMART ANALYTICS. SMART IT SECURITY.

PROTECTING PERIMETERS REMAINS A KEY PRINCIPLE IN TODAY'S IT WORLD. BUT WHAT PROTECTION CAN CONVENTIONAL DEFENSES, SUCH AS FIREWALLS, PROVIDE AGAINST PROFESSIONAL HACKERS? BUSINESSES TODAY MUST ALSO BE PREPARED FOR ATTACKS FROM WITHIN.

Many IT security mechanisms echo the fortress walls and moats of the medieval past – and have the same flaws. At some point, building thicker and higher walls and deeper moats no longer shields against evolving methods of warfare. Fortresses become anachronistic as soon as the latest weaponry simply circumvents these fortifications.

In the same vein, enterprises that are only equipped with conventional perimeter defenses, such as firewalls and virus scanners, risk going the same way as those medieval castles. Firewalls, for example, concentrate on the perimeters of the network. Anything external seeking to enter is flagged as suspicious, and barred from entry. Anything internal, sent outside the network, is assumed to be benign and is allowed to pass. The exception to the rule is e-mail which requires data transmission in both directions.

A DIGITAL ARMS RACE

These vulnerabilities can be exploited by skilled cyber criminals. They smuggle malware disguised as or embedded in e-mails and attachments into corporate networks. Inside, however, anti-virus scanners search for virus signatures and remove these threats. In the majority of cases this is successful. But when hackers design targeted malware for an attack on an enterprise, the shortcomings of anti-virus software are exposed. Furthermore, the type of file involved plays an increasingly minor role in detection; malware is now as likely to be hidden in MS Office documents as in PDF or multi-media files.

In response, IT security solution providers now offer mechanisms that inspect all e-mails, including any attachments, and analyze behavior. If, for example, a PDF file attempts to make changes to an operating system, it is highly likely to be malware – and the security solution renders it harmless. Yet the digital arms race between cyber attackers and their victims continues. Intelligent malware is catching up; it can now recognize when it is being opened, and suppress its function to avoid detection.

A PARADIGM SHIFT IS NECESSARY

There has to be a paradigm shift: away from shutting oneself off from the outside world and towards robust protection against internal threats. Enterprises have to assume that sooner or later their networks will be breached. When that happens, pinpointing and mitigating the danger gain top priority. And the best way to identify an intruder is to scour for anomalies, i. e. unusual behavior. In contrast to normal user activity, criminals tend to move "laterally" – meaning they scour the network for files that could yield key passwords and user credentials. Using purloined details, the attacker can "legally" enter the network at a later time. However, by predicting this behavior, the intended victims can ensnare the intruder – and nip the problem in the bud.

Smart analysis and artificial intelligence are important in watchdogging a network. The key is to distinguish between authorized users and the bad guys – ideally, by using behavioral analysis. In this scenario, attacker activity is compared to a baseline of user profiles, and differences are identified – similar to a physician looking at two ECGs to identify unhealthy heart rhythms. Future solutions will be capable of recognizing anomalous behavior and preventing attacks. To maintain privacy, these are fully automated and the behavior of an individual user is irrelevant.

A COMPLETE SOLUTION AVAILABLE ON SUBSCRIPTION

The latest security mechanisms for smartphones already harness this technology. Each smartphone is a highly advanced computer, but users rarely take advantage of security software and updates. With this in mind, hackers have increasingly focused on these devices. However, smartphones generate ongoing records of behavior via parameters such as storage capacity, power consumption and processor load; any unusual activities are easily detected.

Smart analysis will not replace conventional anti-virus software, firewalls, and regular updates, but it will strengthen users' defenses. And though critics argue that this analysis is too complex and difficult for enterprises themselves to manage, providers can implement this safeguard on their behalf. This lets users rest assured that they are running the latest versions of security products. They have peace of mind, thanks to a complete solution available on subscription. In addition, businesses and consumers enjoy protection for connected devices, such as machines and TVs, – which are not typically shielded by security software. ■

Thomas Tschersich

is Senior Vice President, Group Security Services, at Deutsche Telekom. He holds a degree in electrical engineering, and was previously responsible for IT security and information protection. Since 2000 Tschersich has advised government agencies at federal and state level on IT security issues.

DATA PRIVACY AND DATA SECURITY REPORT 2015

FACTS & FIGURES

THE NUMBER OF ATTACKS FROM THE INTERNET CONTINUES TO INCREASE. THE METHODS THAT THE ATTACKERS USE ARE CHANGING CONSTANTLY AND BECOMING INCREASINGLY PROFESSIONAL. TELEKOM IS DOING ITS UTMOST TO ANALYZE AND REPULSE CYBERATTACKS.

67 TELEKOM EMPLOYEES WORK IN GROUP PRIVACY

3,428

DEVELOPMENT PROJECTS HAVE UNDERGONE PRIVACY AND SECURITY ASSESSMENT (PSA)

97

DATA PRIVACY AND DATA PROTECTION AUDITS WERE PERFORMED BY IN-HOUSE AND EXTERNAL AUDITORS

96

PERCENT OF MALWARE AFFECTS THE ANDROID OPERATING SYSTEM BECAUSE IT IS SO WIDESPREAD

847 CRITICAL VULNERABILITIES WERE IDENTIFIED IN THE 11 MOST WIDESPREAD SOFTWARE PRODUCTS ALONE *

175

DATA PROTECTION COORDINATORS IMPLEMENT DATA PROTECTION TASKS ACROSS THE GROUP

13,334

DATA PROTECTION INQUIRIES WERE MADE TO DATENSCHUTZ@TELEKOM.DE

7 INCIDENTS WERE REPORTED BY TELEKOM

80

DATA PRIVACY OFFICERS ARE RESPONSIBLE FOR DATA PROTECTION IN THE TELEKOM GROUP

439 MILLION MALWARE VERSIONS FOR PCS ARE CIRCULATING ON THE INTERNET

70

PERCENT OF DECISION MAKERS IN BUSINESS AND POLITICS RATE COMPUTER VIRUSES AS A MAJOR THREAT FOR GERMANY ****

18/18

PERCENT OF COMPANIES FACE CYBERATTACKS DAILY AND A FURTHER 18 PERCENT ONCE OR MORE PER WEEK ****

50

PERCENT OF GERMAN COMPANIES HAVE ALREADY BEEN VICTIMS OF INDUSTRIAL ESPIONAGE, STUDIES SAY, AND THE DAMAGE DONE IS BETWEEN EUR 50 BILLION AND EUR 80 BILLION A YEAR ***

60

PERCENT OF COMPANY EXECUTIVES ARE CONVINCED THAT THEIR COMPANY IS WELL PREPARED TO DEAL WITH IT SECURITY RISKS ****

84

MILLION NEW MALWARE VERSIONS WERE IN CIRCULATION, AN INCREASE OF NINE MILLION ON 2014 **

88

PERCENT OF COMPANY EXECUTIVES SEE EFFECTIVE PROTECTION FROM CYBERATTACKS AS A MAJOR CHALLENGE TO THE IMPLEMENTATION OF INDUSTRY 4.0 ****

371

HOURS, OR OVER 15 DAYS, WAS THE LENGTH OF TIME OF ONE DISTRIBUTED DENIAL OF SERVICE ATTACK IDENTIFIED BY KASPERSKY LAB

48 PERCENT OF GERMANS HAVE ALREADY BEEN AT THE RECEIVING END OF INTERNET CRIME

* Source: Die Lage der IT-Sicherheit in Deutschland 2015, BSI
** Source: PandaLabs Annual Report 2015
*** Source: Hans-Georg Maaßen, President of the Bundesverfassungsschutz
**** Source: Cyber Security Report 2015

DATA RETENTION LAW PASSED

ON 18 DECEMBER, 2015 THE GERMAN GOVERNMENT PASSED AN ACT MANDATING RETENTION OF TELECOMMUNICATIONS DATA ON THE PART OF CARRIERS. FOR DEUTSCHE TELEKOM, HOWEVER, THE SAME OVERRIDING PRINCIPLE APPLIES: TRUST REMAINS ALL-IMPORTANT.

Under the new legislation, telecoms carriers are obliged to capture and store data on telephone calls and Internet usage for ten weeks. However, only metadata is captured – not content. The legislation stipulates a shorter period of four weeks for data indicating location, as generated by cell phones. E-mail communication and information on websites visits are exempt from retention requirements. The data captured may only be accessed by law enforcement agencies, and only once authorization has been secured from a judge.

IMPLEMENTATION BY JULY 2017

Before the law can be implemented on the ground, the German Federal Network Agency must publish detailed specifications of the kind of data required before January 1, 2017. Carriers – including Deutsche Telekom – will have to fulfill these obligations by July 1, 2017 at the very latest.

Section 113d of the German Telecommunications Act (TKG) stipulates that providers must use state-of-the-art technologies and organizational measures to prevent unauthorized parties from gaining access to retained information. Action to be taken includes the following:

- Highly secure encryption processes must be deployed
- Data must be stored in dedicated facilities, segregated from those used for typical operational tasks
- Data processing systems must be shielded from access via the Internet
- Physical access to data processing systems should be limited exclusively to authorized employees of the provider
- At least two people must be participants in any data access activity (dual control)

Deutsche Telekom already meets many of these requirements – and will continue to build and uphold customer trust by safeguarding security with due care and diligence. A large proportion of the estimated costs for implementing the retention provisions (totaling tens of millions, to be borne by Deutsche Telekom) will be invested in efforts to strengthen data security.

SECURITY VERSUS PERSONAL LIBERTY

The reintroduction of mandatory data retention is a political decision, and one that has been hotly debated. In its role as a telecommunications provider serving the general public, Deutsche Telekom will fulfill these legal obligations – securely storing data, preventing misuse, and deleting all information once the applicable retention periods have expired. However, the state must strike an appropriate balance between its need for security on the one hand, and the privacy and personal liberty of users on the other. Citizens must feel that they can communicate freely, without being subject to surveillance.

While fulfilling its obligations under law, Deutsche Telekom will continue to uphold its commitment to transparency – especially when it comes to sensitive issues such as telecommunications monitoring and surrender of data to government agencies. Transparency creates trust and trust is vital if citizens are to actively embrace the use of digital services. One key element of Deutsche Telekom's efforts is a transparency report detailing mandatory cooperation with security agencies. This publication was updated in 2016 and includes information on international subsidiaries within the Deutsche Telekom Group for the first time.

IT SECURITY ACT CREATES NEW REQUIREMENTS

THE IT SECURITY ACT (IT-SICHERHEITSGESETZ) CAME INTO FORCE ON JULY 25, 2015. THE GERMAN GOVERNMENT HOPES THIS NEW LEGISLATION WILL STRENGTHEN IT SECURITY IN GERMANY.

A key focus of the German government's cyber security strategy is the protection of critical infrastructure. A key aim of the new IT Security Act is to create a consistent level of protection for IT systems in critical industries: energy, transportation, water, financial services, including insurance, healthcare, food and agriculture, telecommunications and information technology.

Deutsche Telekom provided expert advice and was actively involved in drafting the legislation – in particular provisions governing operators of critical infrastructure. And this new legislation brings new responsibilities. These include a statutory obligation to disclose information to the German Federal Network Agency (BNetzA) and the German Federal Office for Information Security (BSI). In other words, Deutsche Telekom is required to report the occurrence, or probability, of an ICT equipment or service failure.

Threats to ICT are often concealed in end-user hardware and software. These can easily and rapidly spread via social network sites and messaging platforms, in particular via over the top (OTT) services. It is therefore vital that the IT Security Act applies to software and hardware vendors, and to OTT players. Europe is a step ahead of the rest when it comes to taking OTT into account. But German lawmakers, too, must take steps to include all relevant market participants.

A STATUTORY DUTY TO DISCLOSE INFORMATION

SURVEILLANCE BY GERMAN AND NON-GERMAN INTELLIGENCE AGENCIES AND THE EXTENT OF THEIR STATUTORY POWERS REMAINED THE SUBJECT OF INTENSE DISCUSSION IN 2015. DEUTSCHE TELEKOM PARTICIPATED ACTIVELY IN THIS DEBATE. IT WAS CRITICAL OF US AGENCIES AND CALLED FOR GREATER VISIBILITY INTO THEIR ACTIVITIES.

Deutsche Telekom has urged greater transparency with regard to carriers' statutory obligation to help domestic intelligence agencies with surveillance activities.

The company grants access to communications traffic and data only where obligated to do so by law. Collaboration with non-German intelligence services is strictly prohibited. There was and has been no evidence of tampering that would have given intelligence agencies unauthorized physical access to Deutsche Telekom equipment.

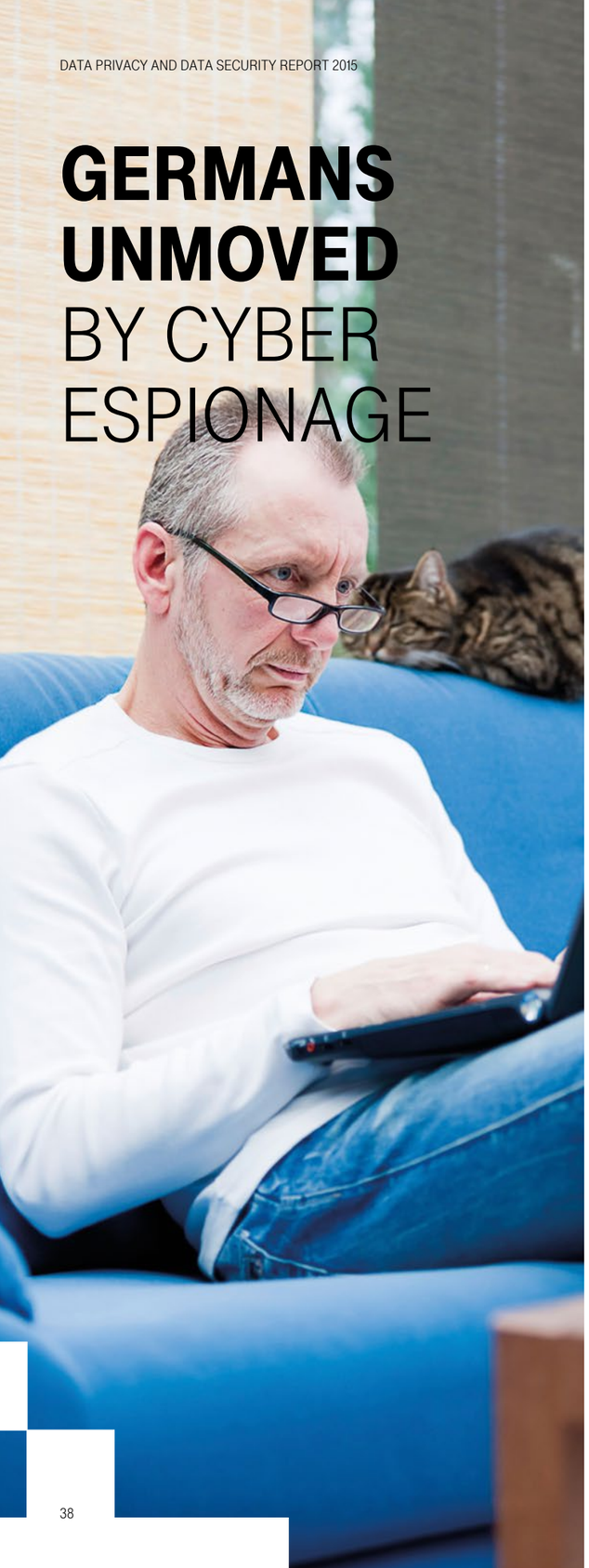
The Federal Intelligence Service Act (BNDG), the Article 10 Act (G10-Gesetz) and the German Telecommunications Act (TKG) (Sections 110 et seq.) require all telecommunications providers to cooperate with German security agencies. This legislation describes in detail what agencies are permitted to do and what Deutsche Telekom is obliged to do. The technical parameters are described in the Telecommunications Interception Ordinance (TKÜV).

The BND (Germany's foreign intelligence service), for example, can demand submission of a complete record of all communications subject to a surveillance order at a named location in Germany. Moreover, carriers must grant the BND physical access to their facilities and allow the service to install equipment. But in this context as well, Deutsche Telekom adheres strictly to the applicable legal principles, observes the constitutional right to confidential telecommunications and protects customer data.

Telecommunications providers are prohibited from disclosing or discussing specific surveillance activities. Any breach makes the carrier liable to prosecution. Deutsche Telekom complies with this requirement while striving for transparency. When giving evidence of a type that fell foul of these provisions to the German Bundestag's committee of inquiry on the NSA, Deutsche Telekom representatives gave testimony in camera.

Deutsche Telekom has established dedicated regional offices for liaison with security agencies. These offices carry out court and intelligence agency orders, and provide IP addresses to the holders of film and music rights (in accordance with Section 101, Copyright Act [UrhG]). They also cooperate with the BND, although this work takes up less than one percent of their time.

As far as possible, Deutsche Telekom verifies that court and government-agency orders fulfill all legal preconditions. The individual steps involved in complying with mandated surveillance are documented in detail. Furthermore, activities are subject to regular review by Deutsche Telekom's Security Officer, the German Federal Network Agency, by the internal auditing department and by Deutsche Telekom's Data Protection Officer.



GERMANS UNMOVED BY CYBER ESPIONAGE

DEUTSCHE TELEKOM'S 2015 SECURITY REPORT REVEALS A REMARKABLE NONCHALANCE TOWARDS CYBER RISKS ON THE PART OF GERMANY'S GENERAL PUBLIC – DESPITE A TORRENT OF MEDIA REPORTS ON HACKING, STOLEN LOG-IN CREDENTIALS AND NSA EAVESDROPPING.

Currently, only 28 percent of Germans are greatly concerned about online fraud. Between 2011 and 2014 the share fluctuated between 27 and 31 percent. The proportion worried by the possible abuse of personal information by businesses or social network users is at the lower end of the range recorded. Similarly, just 21 percent of respondents considered computer viruses to be a real threat – a figure that has barely increased over the last two years.

LESS CONCERN ABOUT SURVEILLANCE

The percentage of Germans who fear their phone or Internet communications might be hacked by nations such as China or the United States has, surprisingly, fallen from 19 to 15. When asked what risks are likely to increase in the future, 70 percent named the misuse of personal data by enterprises and online fraud.

There would seem to be something contradictory about these findings. On the one hand Germans are aware of online threats, and believe the risks are growing in a general sense. At the same time the number who feel personally at risk is not rising; in fact, it is waning in many instances. The Allensbach Institute (IfD), that conducted the survey, concluded that these results were caused by a wide-spread indifference within society towards the problem, and to a lack of information in some areas. Moreover, the researchers believe that people have resigned themselves to the issue, and feel they are not personally affected.

PEOPLE TRUST DEUTSCHE TELEKOM

Amongst telecommunications carriers and Internet service providers, Deutsche Telekom enjoys by far the greatest degree of public confidence when it comes to handling personal data. 46 percent believe the company is trustworthy – almost twice as many as for the competitors ranked in joint second place (on 24 percent).

The 2015 Security Report was produced by the Allensbach Institute (IfD) and the Center for Strategy and Higher Leadership on behalf of Deutsche Telekom. It was based on a representative survey of Germans aged 16 and over, comprising almost 1,400 interviews carried out in the summer of 2015.

COULD CYBERCRIME PUT THE BRAKES ON THE FOURTH INDUSTRIAL REVOLUTION?

CYBERCRIME COULD POTENTIALLY JEOPARDIZE THE SUCCESS OF INDUSTRY 4.0, THE FOURTH INDUSTRIAL REVOLUTION. ACCORDING TO THE CYBER SECURITY REPORT 2015, ALMOST 90 PERCENT OF POLITICAL AND BUSINESS LEADERS VIEW IT SECURITY AS THE GREATEST OBSTACLE TO WIDESPREAD IMPLEMENTATION OF CONNECTED MANUFACTURING CONCEPTS.

Over half (53 percent) of manufacturing companies have implemented IT security concepts in their production processes as part of the race to embrace the digital age. 45 percent have introduced solutions that safeguard data transfer between production control systems and manufacturing equipment. These steps are crucial, with over one-third (36 percent) of German enterprises reporting that they are targeted by cyber criminals several times a week, if not daily. Moreover, nine out of ten businesses have already fallen victim to e-crime. "We should assume that the actual figure is higher, as many attacks go undetected," remarks Anette Bronder, Director of the T-Systems Digital Division, whose responsibilities include Industry 4.0-related activities. "Studies have shown that it often takes businesses several months to establish that an attack has taken place."

However, it seems many enterprises still trust their defences to hold firm. Just twelve percent believe there is a very high risk of e-criminals severely damaging their company. By the same token, 60 percent of business decisionmakers consider their IT to be as fully fortified as possible. These findings confirm the clear link between perceptions of the threat and the number of incidents reported. If only few attacks occur, or no particularly significant cases reach the public domain, businesses tend to downplay the risks – with many remaining reluctant to address the issue of IT security.

92 percent of senior managers at mid-sized and large enterprises claim that IT security is a high-priority or top-priority issue at their organization. In some cases, businesses have significantly upped their investment in this area; 29 percent now spend far more than in previous years, with almost half (49 percent) increasing their outlay to some extent. Meanwhile, the notion that cloud-based services are vulnerable remains hard to shift. Just 24 percent of top-level managers deem cloud computing to be secure – indicating little change in attitudes over the past five years.

This representative study was administered by the Allensbach Institute and the Center for Strategy and Higher Leadership on behalf of Telekom. Between late August and early October 2015 a total of 645 decisionmakers were polled by telephone – including 113 members of the Bundestag and 532 top executives at medium- and large-sized enterprises.

EUROPEAN IT SECURITY DIRECTIVE

EFFORTS ARE BEING MADE TO TIGHTEN IT SECURITY IN MANY AREAS – INCLUDING AT EUROPEAN LEVEL. AT THEIR MOST RECENT TRILOGUE MEETING IN DECEMBER 2015 THE COUNCIL OF THE EUROPEAN UNION, EUROPEAN PARLIAMENT AND COMMITTEE OF PERMANENT REPRESENTATIVES REACHED A COMPROMISE AGREEMENT. THE EU INTENDS TO ADOPT A EUROPE-WIDE DIRECTIVE THAT DEFINES A HIGH COMMON LEVEL OF NETWORK AND INFORMATION SECURITY (NIS).

Both providers of 'traditional' essential services – such as telecommunications, IT, energy and water – and digital service providers (OTTs) – would be required to comply with the agreement. Examples of digital service providers include e-commerce platforms such as eBay and Amazon, plus search engines such as Google, and cloud service providers. However, these enterprises would be subject to less stringent regulations than telcos. OTTs were completely omitted from the first reading of the draft agreement. Deutsche Telekom was among those who called for OTTs to be incorporated into the scope of NIS.

However, the new agreement does not apply to hardware and software manufacturers, or to social media networks. The goal is to introduce new, tighter data protection regulations that apply to these organizations. In this regard, existing German and European IT security regulations do not go far enough. The German IT Security Act gives government agencies the scope to request that hardware and software manufacturers take action to eliminate faults. However, the legislation does not legally compel these companies to act. Social networks have not yet been incorporated into either of these legal instruments, even though they represent potential attack vectors for cybercriminals seeing to access networks and parts of the infrastructure of ICT enterprises. Against this background, Deutsche Telekom firmly believes that these organizations must be obliged to comply with the legislation.

The European Parliament and Council will formally adopt the new directive in early 2016. Member states will then have 21 months to implement the necessary national provisions to comply with the NIS directive. However, the hope among all stakeholders – from businesses and customers to society as a whole – is that the obligation to ensure satisfactory IT security will be extended to all relevant market participants as quickly as possible.

DEFINED ROLES FOR DAY-TO-DAY DATA PROTECTION

WHAT IS THE BEST WAY TO ENSURE THE PROTECTION OF PERSONAL DATA IN IT AND COMMUNICATION SYSTEMS ON AN OPERATIONAL BASIS? DEUTSCHE TELEKOM HAS INTRODUCED A SYSTEM OF CLEARLY DEFINED ROLES AND RESPONSIBILITIES TO GUARANTEE EFFECTIVE GOVERNANCE.

What kind of data should human resource software access to process the payroll – and what data should remain private? How can you make sure a CRM solution has the facts and figures needed to increase the success of a marketing campaign while safeguarding customers' privacy? Questions such as these arise time and again in day-to-day business – questions that need concrete, reliable answers and effective governance. And policies and methods applied vary from one company to the next. Deutsche Telekom is taking steps to ensure there is a consistent approach throughout the organization. In early 2016 the telecommunications giant will implement a system of clearly-defined roles and responsibilities that will subsequently be rolled out to all international subsidiaries.

Each subsidiary appoints a data protection executive (DPE) at the very highest level of management. This person holds overall responsibility for data protection, not just in the sense of privacy but also with regard to confidential business information. The DPE is not to be confused with the data protection officer (DPO). The latter is an oversight role mandated by EU law. The appointee is independent and tasked with monitoring compliance with all legal obligations and internal policies. The DPE, by contrast, is tasked with putting these requirements into practice. And they must, in turn, designate a data protection professional for each solution that processes sensitive information.

This data protection professional determines what data the system is permitted to process. In line with the applicable external and internal constraints, they define which information can be accessed to effectively support the required business functionality. To take the first example cited above, the HR system would only retrieve employee names and bank account details to perform payroll, and no further data.

The data protection professional is assisted by a designated IT professional. This person codes or configures the requirements within the corresponding system. They are typically employed by the IT provider. The provider is responsible for guaranteeing all data protection requirements are carried out in full, and that all technical and organizational mechanisms are effective.

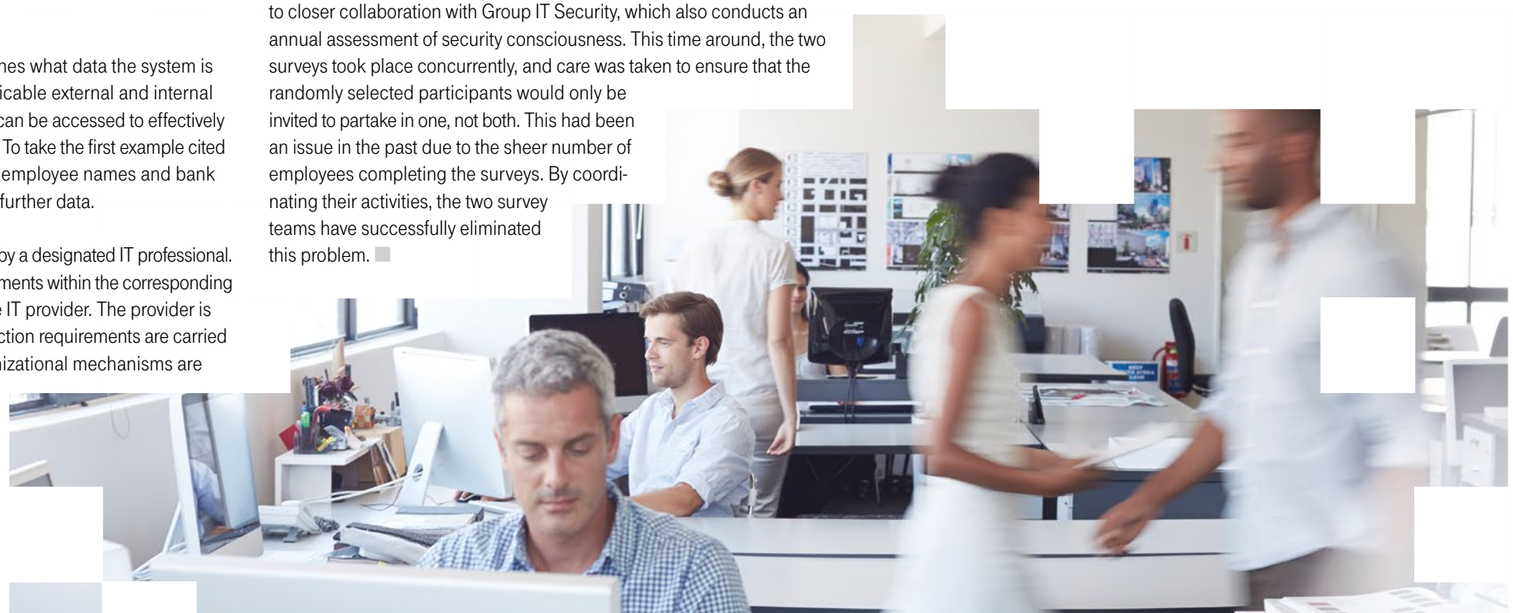
EMPLOYEE KNOWLEDGE AND AWARENESS REMAIN HIGH

JUST HOW INFORMED ARE EMPLOYEES REGARDING DATA PROTECTION? AND HOW WELL DO THEY PUT THEIR KNOWLEDGE INTO PRACTICE? THE MOST RECENT ANNUAL DATA PROTECTION AWARENESS SURVEY, CARRIED OUT IN 2015, CONFIRMS THAT DEUTSCHE TELEKOM'S STAFF REMAINS VIGILANT AND KNOWLEDGEABLE.

Are sensitive e-mails being encrypted properly? What information is considered confidential? And what is considered highly confidential? Questions like these are the focus of the Deutsche Telekom data protection awareness survey. The online questionnaire is used to assess employees' knowledge of data protection and their corresponding real-world behaviors. It also considers how well theory is put into practice on a day-to-day basis. For example, do respondents take advantage of useful tools provided by Deutsche Telekom, such as password management software?

The 2015 findings confirm that Deutsche Telekom continues to perform strongly in terms of employee awareness of data protection imperatives. Individual results were combined to create an aggregate score. This metric was on par with the numbers from the previous year, both nationally (9.5 of 10) and internationally (7.8 of 10). A representative sample comprising 51,000 employees were asked to participate. The response rate increased across the board – most significantly in Germany. At 86 percent it was four percentage points higher than in 2014.

Deutsche Telekom's data protection experts attribute this improvement to closer collaboration with Group IT Security, which also conducts an annual assessment of security consciousness. This time around, the two surveys took place concurrently, and care was taken to ensure that the randomly selected participants would only be invited to partake in one, not both. This had been an issue in the past due to the sheer number of employees completing the surveys. By coordinating their activities, the two survey teams have successfully eliminated this problem.



GLOBAL, COLLABORATIVE GOVERNANCE OF DATA PROTECTION

DEUTSCHE TELEKOM IS EXPANDING THE ROLE OF THE DATA PROTECTION OFFICERS AT ITS INTERNATIONAL SUBSIDIARIES. MANY OF THEM ARE INVOLVED IN INSPECTIONS IN THIRD COUNTRIES.

In 2015 Deutsche Telekom's Group Privacy team began to involve data protection officers at international subsidiaries in inspections in third countries. More and more of them are taking the opportunity to exchange insights and information with their counterparts across national boundaries. Last September, for example, a member of the Romanian data protection team helped colleagues from Group headquarters to conduct audits in Sweden and Denmark.

International deployments of this kind are part of an empowerment program to improve the knowledge and skills of Deutsche Telekom's specialists worldwide. The goal is to more closely involve local officers in the work of the team at group level. Another key element of the program is multinational work groups tasked with addressing current issues of global relevance. These include big data analytics and the new EU General Data Protection Regulation.

The expansion of cross-border teamwork means that national data protection officers now play a role in planning inspections. Furthermore, Deutsche Telekom's specialists in this field are increasingly looking beyond departmental boundaries. To improve efficiency, they are cooperating closely with fellow professionals at Group IT Security and Auditing to coordinate audits and inspections. As a result, in 2015 the data protection awareness survey (see article opposite) and the security consciousness survey conducted by Group IT Security were carried out jointly.

CONSISTENT POLICIES AROUND THE GLOBE

DEUTSCHE TELEKOM'S BINDING CORPORATE RULES FOR PRIVACY (BCRP) ENSURE UNIFORM DATA PROTECTION POLICIES AT ALL SUBSIDIARIES WORLDWIDE. BOTH CUSTOMERS AND EMPLOYEES HAVE BENEFITTED.

In late 2015 OTE, Deutsche Telekom's Greek affiliate, signed up for the Group's new data protection policies, bringing these procedures not only to Greece but to OTE's subsidiaries in Romania as well. Previously, almost all Deutsche Telekom national subsidiaries in Europe, Africa, Asia and Latin America had begun observance of these new provisions. Likewise, the rules are already in force in the United States, at Deutsche Telekom Inc. and T-Systems North America – ensuring robust protection for data transferred from the European Union.

The BCRP superseded 2004's Privacy Code of Conduct. The new policy governs the handling of information on customers, employees and business partners. The BCRP provides detailed guidance on how personal data may be gathered, stored and processed. The rules are in accord with Germany's Federal Data Protection Act (BDSG) and the European Data Protection Directive. Moreover, they go a long way towards satisfying the requirements that will be introduced by the European General Data Protection Regulation.

Deutsche Telekom customers will benefit – but so, too, will the company. Following the successful conclusion of a European approval process, the BCRP are recognized by all European data protection agencies. As a result, Deutsche Telekom subsidiaries throughout Europe will be permitted to transfer personal information to non-European affiliates, without requiring separate and prior approval in each instance.

The BCRP comply with European data protection legislation, which is comparatively wide reaching. In fact, in some cases the BCRP go above and beyond EU imperatives. Deutsche Telekom's non-European entities are therefore well placed should stricter laws be enacted in their local market. For example, in South Africa, there had long been no statutory data protection whatsoever. Against this background, the local subsidiary began handling personal information according to the BCRP. As a result, when the South African government passed new legislation in 2014, with relatively little forewarning, the Deutsche Telekom subsidiary was well equipped to satisfy the new requirements.

DEUTSCHE TELEKOM APPS UNDER THE MICROSCOPE

DO MOBILE APPS PROVIDE ADEQUATE PRIVACY SAFEGUARDS? ARE THEY LESS SECURE THAN CONVENTIONAL PC-BASED SOFTWARE? TO FIND ANSWERS TO THESE AND SIMILAR QUESTIONS, DEUTSCHE TELEKOM PUT ITS 30 MOST POPULAR APPS TO THE TEST.

The app market is growing in leaps and bounds. In 2015 Germany's consumers downloaded 3.4 billion apps to their smartphones and tablets – according to Bitkom, the country's leading ICT industry association. The barriers to entry for new market players are relatively low. Moreover, agile development methods enable the quick and easy launch of new programs. In this environment vendors may be neglecting privacy and security issues. And since apps can access significant volumes and types of personal data, this could have serious repercussions.

In October 2015 Deutsche Telekom's data privacy and security specialists took a critical look at its own apps – focusing on the ones most frequently downloaded from Apple and Google stores. Among the 30 products tested were a cloud storage solution, an e-mail app, and a smart-home tool that lets users remotely control heating, lighting and appliances.

CHECKING AGAINST THE FACTS

The first step was to define an exhaustive list of criteria based on Deutsche Telekom's dataprotection specifications for app development. Product managers then self-assessed their software against these criteria. The project team then verified the submissions. For instance, they looked at how and when apps display privacy notices. They checked whether customers were adequately informed in advance of downloads, and how detailed privacy notices were. They noted the number of clicks needed to access notices, and whether apps featured Deutsche Telekom's privacy icon, making information easier to find.

The tests were based on Deutsche Telekom's security specifications for iOS and Android code, employing both static and dynamic analysis. Dynamic methods involve executing an app under controlled conditions to evaluate how it behaves in practice – in terms of encryption and network traffic, for example. Static analysis, by contrast, focuses on the code itself, and what the app is permitted to do. In addition, back-end servers were checked for vulnerabilities.

Overall, the investigators were satisfied, although they did recommend some improvements. Intriguingly, they also discovered that in certain instances results differed for the Android and iOS versions of the same app. For example, some apps performed relatively well under iOS, but their Android equivalents displayed weaknesses.

DATA MINIMIZATION AND PURPOSE LIMITATION

The most common target for criticism was privacy notices – both their content and the difficulty in locating them. Unfortunately, not all apps employed the Deutsche Telekom privacy icon – a symbol specially developed to highlight privacy-by-design functionality. Importantly, data minimization and purpose limitation were found to be satisfactory; the apps only store and process personal data required in order to function.

Testing also identified aspects of data security that could be improved. To ensure the latest threats were taken into account, Deutsche Telekom's experts sought and gained the support of the Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT). The organization provided software that checks for critical vulnerabilities. The project team presented their findings to the product managers in great detail, enabling them to systematically address all identified weaknesses.

TÜViT CERTIFICATION FOR BILLING PROCESS RENEWED

A TELEPHONE BILL YOU CAN TRUST. IN 2015 TÜVIT, AN INDEPENDENT GERMAN EVALUATION BODY SPECIALIZING IN IT, RENEWED CERTIFICATION OF DEUTSCHE TELEKOM'S BILLING PROCESS. AUDITORS PAID PARTICULAR ATTENTION TO DATA PROTECTION AND SECURITY.

Each month Deutsche Telekom issues approximately 27 million invoices for the consumer market alone. Hundreds, often even thousands of communications transactions must be precisely measured and charged for each individual customer. And everyone expects their information to be managed with due care and sensitivity. This is no simple task. It includes capturing and processing relevant data, creating the bill, and addressing, mailing and archiving the corresponding documents. This requires multiple IT solutions to interoperate. In 2015 TÜViT audited the entire billing process and the corresponding IT systems – including data protection and IT security. Deutsche Telekom was again awarded TÜV certification – in recognition of its secure handling of customer data, in full compliance with German legislation.

DATA PROTECTION IN THE CLOUD

GERMANY'S TRUSTED CLOUD PROGRAM AND NETWORK HAS DEVELOPED A SET OF CRITERIA TO COMPREHENSIVELY ASSESS THE DATA SECURITY LEVEL MAINTAINED BY CLOUD SERVICE PROVIDERS. TÜVIT – THE SPECIALIST IT UNIT WITHIN THE TÜV CERTIFICATION AND TESTING ORGANIZATION – IS CURRENTLY EVALUATING THE PRACTICALITY OF THIS NEW PROCEDURE.

The German Federal Ministry for Economic Affairs and Energy (BMWi) launched the Trusted Cloud program to support development and testing of innovative, secure cloud solutions that fulfill Germany's strict data protection legislation. The test criteria are based on the 2700x series of ISO/IEC IT security certification standards. In many instances, however, the requirements of the German Federal Data Protection Act go a step further – and this is reflected in the new parameters which were first presented by the ministry in spring 2015. To define the criteria, the Trusted Cloud competence center met with representatives from relevant government agencies, plus experts from research institutions and the fields of law and business. Deutsche Telekom data security specialists provided real-world insights that helped the group to categorize what kind of data requires what kind of protection. The new parameters represent the final part of a comprehensive certification framework in accordance with German legislation. Now, Trusted Cloud has tasked TÜViT with performing six pilot certifications in the run-up to CeBIT 2016. This includes a SaaS (software as a service) offering from Deutsche Telekom that allows businesses to complete financial accounting tasks in a secure Internet environment. TÜViT is currently assessing the software solution being used, and the overarching data storage method.

DIGITIZATION AND DATA PROTECTION IN HEALTHCARE

IN TERMS OF DIGITIZATION, THE HEALTH INDUSTRY LAGS FAR BEHIND OTHER SECTORS – DESPITE THE FACT THAT DIGITAL PROCESSES CAN IMPROVE HEALTHCARE PROVISION, AND ENHANCE DATA PROTECTION.

Just a few short years ago, mention of the quantified self movement would have raised a weak smile. Today, it is a full-fledged trend. An increasing number of people – particularly the young – record data on their activities, behaviors and bodies. This includes parameters such as their weight, heart rate, blood sugar and adrenaline levels, sleeping patterns and lung capacity. They then use these metrics for "self-tracking". However, whether this data collection and analysis serve a useful, medical purpose remains in doubt. A remarkable aspect of the movement is its advocates' willingness to publish their personal data on the Internet – to exchange and make comparisons with similar-minded followers, for example. In other words, Generation Y, who embraced Facebook and other social networks from their and its infancy, have no qualms about sharing data on their physical fitness with others.

DIGITIZATION OFFERS A NUMBER OF BENEFITS

We live in an interconnected world and often take the benefits for granted. Connectivity provides many conveniences and makes life easier – and that includes healthcare. For example, Deutsche Telekom has equipped many hospitals with digital information systems and tablets for doctors doing their rounds. These devices help cut costs, make the work of physicians and nurses easier, and improve quality of care. Telemedicine – leveraging ICT to provide healthcare at a distance – is another example. There is a shortage of medical professionals in many regions of Germany. Telemedicine makes it possible to provide first-rate services to patients who would otherwise have to travel long distances for attention.

Consider another example: telematics infrastructure enables the highly secure exchange of data required for Germany's innovative electronic healthcare cards. And such safeguards are key. Many doctors' offices and hospitals already use digital communications, but a number of them still resort to fax machines (that are less reliable and not secure) to share information with peers or other facilities. In Western Europe, Germany is the only nation whose healthcare sector lacks a secure means of online data exchange. Yet connectivity means faster communications, greater cost efficiency and tangible medical benefits. Doctors can access electronic data at any time, ensuring potentially life-saving information is available. In fact, in Germany more people die from the unintended side-effects of medication than in traffic accidents. A simple digital overview and online resources would prevent deaths.

HIGH-QUALITY SAFEGUARDS FOR PATIENT DATA ARE KEY

Currently, the quantified self philosophy is not particularly relevant to mainstream healthcare – not least because patients continue to demand maximum security for their data. At Deutsche Telekom we see this as part of our mission: better safe than sorry when it comes to healthcare digitization. Consequently, we always encrypt sensitive data in motion and store it in our highly secure German data centers. In addition, Deutsche Telekom is certified to process data for other organizations, and to provide IT services for medical image archiving.

Some people may argue that data can be misused, even IT environments with sophisticated security mechanisms. However, that is no reason to forgo digitization. State-of-the-art ICT systems support clearly defined rights, log all user activities, meet extremely strict security standards and encrypt data. And if fundamental statutory safeguards are sidestepped or ignored, there are legal consequences. Implementing these processes is actually better for data protection – and ultimately better for patients.

Dr. Axel Wehmeier

is a member of the Management Board for Deutsche Telekom's Healthcare Solutions. Born in 1966, he studied economics and business management at the University of Texas and the University of Cologne. Wehmeier worked as research associate before earning his doctorate in 1998, and began his career at Deutsche Telekom as a pricing officer. He has held a variety of positions at the corporation; in 2010, he became Head of Connected Health Care at T-Systems, and joined the Management Board for Deutsche Telekom's Healthcare Solutions in 2014.

DATA PRIVACY AND DATA SECURITY REPORT 2015

SEAL OF APPROVAL FOR ARCHIVING SERVICE FOR MEDICAL IMAGES

SECURITY AND PRIVACY ARE TOP PRIORITIES WHEN MANAGING SENSITIVE MEDICAL DATA. AN ARCHIVING SERVICE FOR MEDICAL IMAGES FROM TELEKOM HEALTHCARE SOLUTIONS (THS), A SUBSIDIARY OF DEUTSCHE TELEKOM, HAS BEEN CERTIFIED BY DSZ.

DSZ auditors assessed the data management processes employed by the Study-Based Archiving Service. This THS offering allows hospitals and other healthcare facilities to securely archive images and make them available to other medical professionals in digital form. This eliminates the need for the repetition of expensive scans and x-rays, and allows rapid access to vital medical information. Moreover, the solution ensures all content is reliably stored in the long term – in line with statutory retention periods (e. g. 30 years in Germany). And, certification means hospitals, doctors and patients can be sure that Deutsche Telekom fully complies with Germany's stringent standards of data protection for personal information.

Telekom Healthcare Solutions is the first healthcare industry organization to be certified in accordance with the DS-BvD-GDD-01 standard. Dr. Niels Lepperhoff, CEO of DSZ, stated: "We were pleasantly surprised by the high priority Deutsche Telekom gives to data protection, and the outstanding expertise the company possesses. As a result, we were able to complete certification quickly and simply."

The DS-BvD-GDD-01 standard was jointly developed by Germany's two leading data protection associations – the BvD (the Professional Association for Data Protection Officers) and the GDD (the Association for Data Protection and Data Security). The two organizations also jointly founded DSZ. The certification process satisfies all requirements defined by German government data protection oversight bodies – guaranteeing its reliability. Certification confirms the presence of the necessary data protection skills, and of robust implementation in line with applicable legislation. Deutsche Telekom plans to secure certification for other healthcare solutions within its portfolio.

ANONYMIZED SIGNALING DATA PROVIDES VALUABLE INSIGHTS

ANALYSIS OF PERSONAL DATA IS SUBJECT TO STRICT DATA PROTECTION CONSTRAINTS. DEUTSCHE TELEKOM HAS DEVELOPED AN ANONYMIZATION SOLUTION FOR CELLPHONE SIGNALING DATA APPROVED BY THE FEDERAL COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION (BFDI). THE PROCESS IS ALSO SUBJECT TO INDEPENDENT EXTERNAL AUDITING AND CERTIFICATION.

Motionlogic, a wholly-owned subsidiary of Deutsche Telekom, uses anonymized data to analyze people movements and traffic patterns. The insights are gained from signaling data from cellular and Wi-Fi networks. This information is generated whenever someone makes a call, sends a text message or surfs the Internet with their phone. The data is captured via the base station for network management purposes. Even when not in use, phones communicate with the cellular network at regular intervals. In addition, certain socio-demographic attributes, again anonymized, can be combined with the signaling data – for example age group, gender, federal state and city.

Anonymization removes personal information, including names and telephone numbers, prior to analysis. It is therefore not possible to track the movements of an individual person. This process takes place in a highly secure Deutsche Telekom data center that Motionlogic cannot access directly.

Analysis can provide up-to-the-minute metrics on movements and patterns. This offers valuable insights into traffic flows, including speeds, point of origin/destination, and the means of transport used by certain groups of people. The Motionlogic solution opens up new possibilities – for example, it supports more efficient management of local public transportation during peak travel times.

Visibility into people's movements is also extremely useful for urban and mass transit planners: accurate information on traffic flows is vital to aligning road and rail infrastructure with actual demand, and to the efficient deployment of trains and buses, including routes. Findings can also be leveraged to reduce traffic congestion and, in some instances, to eliminate them entirely. Until recently, planners had used manual counts, census data or surveys to gather these figures. But these methods require significant time and effort, and the results often generated little genuine enlightenment. ■

DON'T JUST DO IT, TALK ABOUT IT

Deutsche Telekom delivers exceptional data protection and data security. Its credentials in these areas have been confirmed by numerous independent institutions. In some aspects, the company's organizational measures and technological mechanisms exceed those required by lawmakers. And this has not gone unnoticed. According to the Security Report, a representative survey of the German population, Deutsche Telekom is far more trusted than its competitors.

However, the organization's external communications on data protection have been limited. Moving forward, this is set to change. In 2016 not only will communication efforts increase, they will better reflect the company's high level of expertise. The first order of business is a new online portal. Deutsche Telekom will use this platform to shed light on all the ins and outs of data protection. Further communication initiatives are in the pipeline. Sometimes it's not enough to just do something well; you also need to talk about it. ■

DATA PROTECTION AND INFORMATION SECURITY TRAINING

In March 2015 Deutsche Telekom launched an online program for all employees, comprising instruction on data protection and information security. Training is provided on best practices and statutory requirements. Updated every two years, the program is obligatory for all staff in Germany. A key focus is the company's most important internal data protection policy, the Binding Corporate Rules on Privacy. In addition, guidance is offered on the correct handling of sensitive information and documents. This training guarantees consistent security standards for processing customer and employee data throughout the entire worldwide Deutsche Telekom organization. ■

SOUND ADVICE VIA CARTOONS

IT IS EASY TO SLIP INTO SLOPPY HABITS. DEUTSCHE TELEKOM INVITED EMPLOYEES TO PROVIDE EXAMPLES OF OFFICE BEHAVIORS LIKELY TO ENDANGER SECURITY AND PRIVACY. THE BEST ENTRIES WERE TURNED INTO ANIMATED FILMS.

In early 2015 Deutsche Telekom created a cartoon character dubbed Dataslob, whose risky behavior helps raise awareness of data protection issues among employees. The series of animated films was a big hit, prompting the company to launch a worldwide competition, inviting staff to submit further examples of perilous practices. It attracted 150 suggestions, including written descriptions, drawings and even videos.

Many entries shined a critical light on situations outside the normal office environment. Examples included a road warrior who pulls up confidential information on a laptop without a thought to who may be taking a sneak peek over their shoulder. Or an employee at a crowded bus stop chatting away a mile-to-the-minute to their neighbor about sensitive projects and proposals – matters that are no business of the other passengers.

One by one, the winning submissions are now being turned into short animated videos. These will be shown around the globe as part of Deutsche Telekom's internal awareness campaign. ■

ON THE RADAR OF SOCIALLY RESPONSIBLE INVESTORS

SOCIALLY RESPONSIBLE INVESTORS MAKE A VITAL CONTRIBUTION TO DEUTSCHE TELEKOM'S LONG-TERM FINANCING. THEY VIEW THE GROUP'S ACTIVE COMMITMENT TO DATA PRIVACY AND SECURITY AS A CRUCIAL ELEMENT OF BUSINESS SUSTAINABILITY – AS BIRGIT KLESPER, SENIOR VICE PRESIDENT OF GROUP TRANSFORMATIONAL CHANGE AND CORPORATE RESPONSIBILITY, EXPLAINS.

Ms. Klesper, you oversee Deutsche Telekom's corporate responsibility activities. Where do you see the link between CR, and data privacy and security?
Birgit Klesper: At Deutsche Telekom we make it our mission to run our organization in a responsible way. We are committed to fulfilling our business, ecological and social duties at every stage of the value chain – in our internal processes, and in our dealings with customers, suppliers and society as a whole. This philosophy applies to our investors, too. As a socially responsible business it is in our DNA to ensure robust security for customers, and to vigilantly safeguard user data and infrastructures against unauthorized access. And investors are increasingly turning their attention to how the ICT industry is addressing these key issues.

Which investors are most interested in data privacy and security, and why?
Birgit Klesper: Many of our investors – especially those with a long-term strategy – focus on an organization's development and the returns it delivers over time. In the corporate lingo we talk about SRI: socially responsible investment. SRI products generally comprise securities from companies that aim for strong financial performance, while also fulfilling certain business, ecological and social criteria. As SR investors plan to be in for the long haul, they are particularly concerned with eliminating risks, and identifying market opportunities – and data privacy and security play a role in both regards.

Does Deutsche Telekom take a particular interest in socially responsible investors?
Birgit Klesper: Yes. Their contribution is key to securing reliable funding, as they make 'sustainable' – that is, long-term – investment decisions. At present, 21 percent of Deutsche Telekom shares are held by investors who manage at least part of their portfolio in line with sustainability criteria – and for 2 percent it is their primary consideration. And the SRI market is growing all the time. In Germany the value of socially responsible investments and clients has more than doubled since 2010 – totaling almost 53 billion euros in 2014 (FNG market report, 2015). Moreover, a number of studies indicate a correlation between good SRI scores and low capital cost.

How do you demonstrate to socially responsible investors that Deutsche Telekom is well prepared in terms of data privacy and security?
Birgit Klesper: Deutsche Telekom's comprehensive approach to data security – including our honey pots and our cyber security center – minimizes business risks such as cyber attacks. Investors are impressed to learn that we instantly fend off 99 percent of all threats, and rapidly resolve any remaining incidents. At the same time, we are quick to seize opportunities. Customers choose Deutsche Telekom because they believe our products and services will deliver privacy and security. As digitization generates ever-greater volumes of data, these issues will become increasingly important to our customers – and to our business success.

Data protection and privacy have become highly relevant for children and teenagers, too. Our Teachtoday platform provides teachers, parents and students with resources and practical advice designed to ensure safe, responsible use of ICT.

They are all good arguments – but how exactly do you get them across to socially responsible investors?
Birgit Klesper: In a variety of ways – ranging from public reporting to personal conversations. When issuing capital market guidance to be published externally, we liaise closely with the Group's Investor Relations team.

The Deutsche Telekom annual report and CR report provide comprehensive information and transparency to investors and other stakeholders. Prepared in line with the highest industry standards, both publications received the ECON Award this year (gold and platinum respectively). This Data Privacy and Data Security Report is a further key source of information, and we always refer to it when interacting with investors. Moreover, Deutsche Telekom regularly features in selected sustainability rankings. These ratings are based primarily on information in the public domain, such as the CR report, for example. If necessary, an agency will request more details directly from the organization under review. This input is consolidated in a company profile, which gives a precise evaluation of performance across a range of categories – either as a percentage or on a scale from A to D. In addition to rating agencies specializing in sustainability, traditional analysts like Bloomberg and ThomsonReuters are increasingly taking CSR criteria into account.

Investors can purchase these profiles from rating agencies. Generally, they buy reports from multiple sources and combine this information with in-house research using publically available material. Data privacy and security have long been key considerations in determining these ratings – and Deutsche Telekom regularly performs exceptionally well, scoring far above the industry average. We received a 97-percent rating from RobecoSAM this year, for example, while oekom research awarded us the best score (A+) in the data protection and information security category. Likewise, Sustainalytics has been full of praise for our "very strong data privacy and security programs".

Do you also speak directly with socially responsible investors?
Birgit Klesper: Our reporting activities and ratings are just a starting point – and we build on this by means of direct interaction with SR investors. Deutsche Telekom's Investor Relations team manages this form of communication. We regularly hold SRI calls and roadshows, together with Simone Schlief from this department. These enable us to engage in person and to answer specific questions. Increasingly, we are addressing mainstream investors in this way, too.

An SRI roadshow – that sounds like you are going on tour. What does it involve exactly?
Birgit Klesper: A tour is a valid comparison. It is a very intense undertaking: around two to three times a year we travel with the Investor Relations team to a series of European cities, one day after another. We organize individual meetings and lunches, where attendees eat while we give presentations and answer tricky questions. During these face-to-face meetings we are witnessing a spike in interest in data privacy and security.

Is it worth the effort?
Birgit Klesper: A roadshow certainly requires a great deal of time and effort, and thorough preparation is crucial. Once at our chosen venue, we must focus intensely on answering the precise, carefully considered questions posed by attendees. After the fifth conversation on a day like that, it is no surprise that we are exhausted – but yes, it's definitely worth it. These roadshows allow us to gain first-hand insight into investors' views on what Deutsche Telekom is doing right, and which issues are important to which types of financial stakeholders. And we harness the direct feedback from roadshows to fine-tune our CR strategy.

How can you tell that you have made a convincing case?
Birgit Klesper: Our goal is to make Deutsche Telekom shares attractive to investors so they will prioritize them in their portfolios. During direct interaction it soon becomes apparent whether we have met or perhaps exceeded their expectations – this sort of insight is not possible from a rating.

Moreover, the broker who organizes and supports the events usually prepares a short report after each roadshow. When it comes to data privacy and security, we have received particularly positive feedback for our decision to create a Board of Management department specifically for data privacy and security (DRC) back in 2008. Investors also highlight our robust, group-wide policies, and our comprehensive system of regular activities, training courses and audits. They expressly praise our in-house training programs for IT experts, the leading role Deutsche Telekom assumes in industry initiatives, and our ability to unlock business opportunities in the data privacy and security space. We pass on this positive investor feedback directly to our data privacy team. I am proud that Deutsche Telekom is viewed as a data protection pioneer in the ICT industry.

Birgit Klesper

has been Senior Vice President of Group Transformational Change and Corporate Responsibility at Deutsche Telekom since 2012. After training as a journalist she worked in corporate communications at Wella and Tchibo before joining the telecommunications company in 2006.

DATA PRIVACY AND DATA SECURITY REPORT 2015

TEACHTODAY – PROMOTING DIGITAL LITERACY

Cell phones, the Internet and social media are very much a part of everyday life for children and teenagers. They spend much of their time online or otherwise connected. According to a long-term study (known as JIM) conducted jointly by the government agencies of two German states (Forschungsverbund Südwest), 92 percent of 12- to 19-year-olds have a cell phone and three quarters access the Internet under a flat-rate plan. The same percentage have their own PC or laptop, and more than half (57 percent) have their own television.

In the case of even younger children, more than half of eight-year-olds (55 percent) are already online, while almost a third of six-year-olds and one in ten three-year-olds use the Internet. These are the findings of a study by DIVSI, an organization dedicated to promoting trust and security on the Internet. Parents believe that imparting Internet proficiency to children is primarily their responsibility. But they also feel that schools and businesses have a role to play in teaching age-appropriate use of digital media.

Teachtoday is a Deutsche Telekom initiative to promote safe and proficient Internet use. It offers guidance to children and young people – but also to parents, grandparents and teachers. It provides online resources, and organizes educational events. www.teachtoday.de is geared to adults, with extensive resources on the responsible usage of new information and communication technologies.

Teachtoday addresses typical scenarios drawn from everyday life – at home, at school, and elsewhere. These include a child's first cell phone, the question of the amount of time spent online, and Internet etiquette. Materials are designed to be highly practical, allowing parents, grandparents and teachers to put the advice to immediate use.

There is a dedicated portal for children and young people at www.scroller.de. Visitors can order a print magazine or browse through an online version. They discover how to best safely navigate the world of digital media – through a variety of entertaining resources, including puzzles and stories.

PRIZES FOR OUTSTANDING EDUCATIONAL PROJECTS

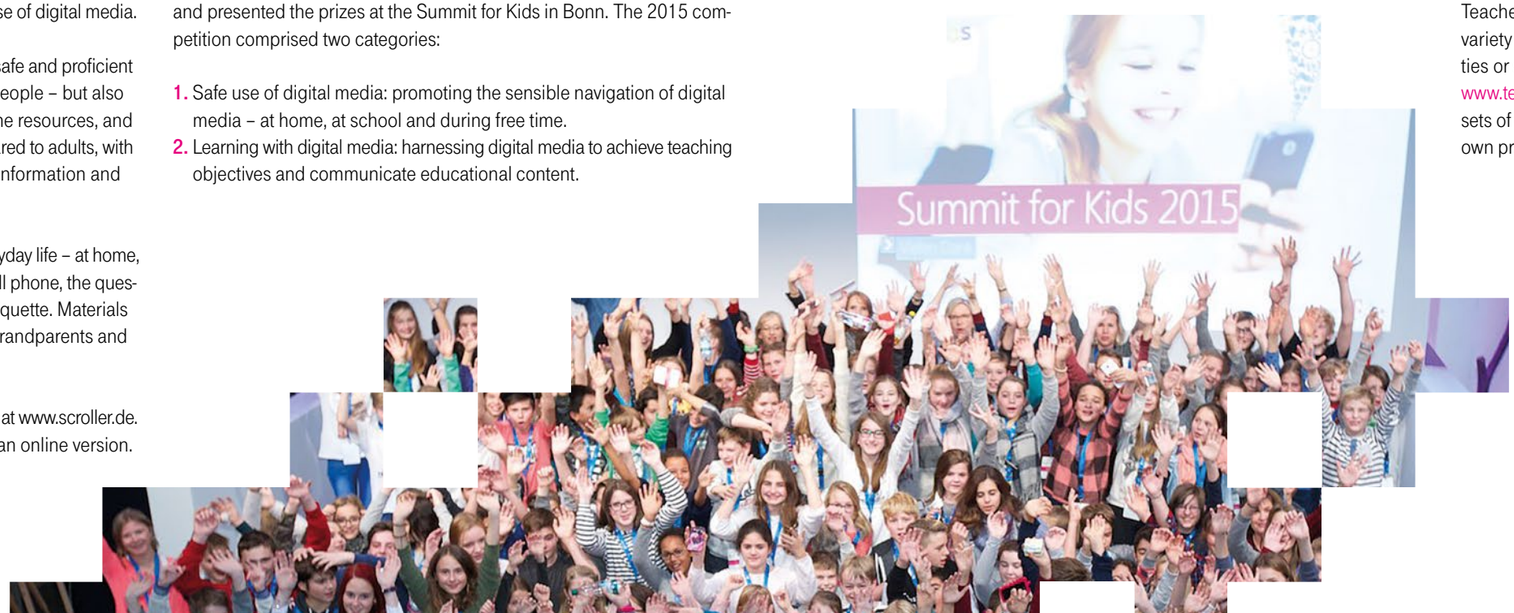
Teachers are keen to incorporate digital media into their lessons. And they play a key role in promoting digital literacy, and helping students to sensibly deploy today's technologies. However, there is often little awareness among the general public of many excellent educational projects. An international competition (entitled Media, sure! But secure.) has been launched to raise visibility. It awards prizes to teachers who have successfully carried out digital media projects, and acts as a platform for the exchange of ideas and insights.

The judges recognized the work of seven schools and other organizations, and presented the prizes at the Summit for Kids in Bonn. The 2015 competition comprised two categories:

1. Safe use of digital media: promoting the sensible navigation of digital media – at home, at school and during free time.
2. Learning with digital media: harnessing digital media to achieve teaching objectives and communicate educational content.

SUMMIT FOR KIDS

On November 18, 2015 the Teachtoday Summit for Kids took place in Bonn, attended by more than 150 children and young people. The event was organized with the aim of promoting responsible use of digital media. It included workshop sessions, culminating in a "manifesto" of needs and wants. The children were organized into four groups, each addressing digital media usage in a specific context: in the family, at school, in free time and in the wider world. The workshops resulted in lively debates among the children.



VIRTUAL OBSTACLE COURSE

Deutsche Telekom has created a "virtual obstacle course" that helps children acquire essential digital media skills. In 2015 this unique event toured schools throughout Germany, with the participation over 4,900 children aged nine to twelve. It helped attendees to navigate the online world intuitively and proficiently.

The virtual obstacle course comprises five sets of educational and entertaining exercises and tasks. They highlight issues such as the time children spend gaming, data protection and cyber bullying. As with a jump-and-run computer game the children need quick reaction speed and dexterity. The focus is on subjects such as the time spent playing games, data protection and cyber bullying.

Teachers can implement the virtual obstacle course themselves in a variety of environments, for example in youth centers, recreational facilities or schools. Explanatory videos and resources are available at www.teachtoday.de. The virtual obstacle course can be run with all five sets of exercises, or selected sets can be incorporated into the teacher's own program.

DATA HACK AT T-MOBILE USA'S IT SERVICE PROVIDER

IN SEPTEMBER 2015 THE IT SERVICE PROVIDER EXPERIAN DISCOVERED AN UNAUTHORIZED ACCESS TO ITS SERVERS. THE DATA HACKED INCLUDED DATA THAT EXPERIAN STORES AND PROCESSES FOR T-MOBILE USA, BUT T-MOBILE USA SYSTEMS WERE NOT COMPROMISED.

Investigation by Experian found it to have been an isolated hacker attack over a period of around two weeks between September 1 and 16, 2015. No access was gained to credit card or bank data. The servers contained data of a number of T-Mobile USA customers and of customers who had the purchase of terminal devices financed, which involves a credit check. Data of German customers was not affected by the incident.

The information affected by the hack included data such as name, address, social security number, date of birth and ID (driver's license or passport) numbers, plus additional information that T-Mobile stores as part of the credit check. According to Experian there was no indication that T-Mobile USA data had been put to inappropriate use. Yet the fact remains that for the customers affected the risk of identity theft was increased.

In a statement published shortly after the discovery of the incident, John Legere, CEO of T-Mobile USA, had this to say: "I am incredibly annoyed about this data breach and we will be looking very closely at further cooperation with Experian. As a first step, however, my main concern is to support all customers who might have been affected by this incident in any way. I take our customers and the protection of our customers' data very seriously, so for us this is not just a minor incident. I can assure our customers that neither IT systems nor networks of T-Mobile were affected by the hack and that no credit card number or bank account information was affected by the incident at Experian."

Experian informed international law enforcement authorities about the incident and announced that additional security measures were to be undertaken at short notice in order to prevent incidents of this kind in the future. Experian is also trying to identify the hackers and is collaborating closely with international law enforcement authorities in its endeavors to do so. ■

SYNTHETIC DATA FOR ANALYSIS

WHICH DATA CAN COMPANIES EVALUATE AND HOW? THIS QUESTION IS PRETTY MUCH WHAT DATA PROTECTION IS ALL ABOUT. SYNTHETIC DATA THAT REVEALS ABSOLUTELY NOTHING ABOUT REAL PEOPLE COULD BE A SOLUTION.

What use are countless items of information – customer data, for example – if we are not allowed to use them? That is a question companies in the U.S. do not necessarily have to ask themselves because the way personal data is handled there is seen differently. In Germany, in contrast, data protection law prohibits a number of analyses that might well prove profitable. That is why companies generally decide to use anonymized data. But the production of anonymized data is technically complex. The result is that, subject to the processes and technology used, there can be partial deviations in quality, meaning the degree to which the data is made not to resemble that of a real person. End users and the media are therefore not unreservedly positive about anonymization processes of this kind even if they are certified to be satisfactory because cases are conceivable in which specialists might be able, at great expense and with additional knowledge, to restore individual data as being related to a specific individual.

Researchers at T-Labs in Berlin, Telekom's central research and innovation division, are instead developing analytical methods that ensure data privacy and allow no inferences to be drawn as to individuals. Synthetic data is the solution. It is based on real personal data over which the researchers have run a mathematical algorithm that they have devised. This process abstracts personal data and transforms it into synthetic data.

Even in large amounts of data the algorithm recognizes specific patterns and clusters them in groups such as male, age 30 to 39, from Charlottenburg, goes to work at 8 a.m. These patterns are comparable to templates from which the researchers go on, in the next step, to produce synthetic data of a quality that is similar to that of genuine data, but does not permit inferences to be drawn to an individual person.

Production of synthetic data is still at the research stage, but the process might lead to specific products, so that every company that would like to obtain new information from sensitive personal data can use synthetic data produced as a service. ■

DATA PROTECTION FOR CONNECTED PRODUCTION

DEUTSCHE TELEKOM HAS DRAWN UP DATA PROTECTION GUIDELINES FOR THE INTERNET OF THINGS AND INDUSTRY 4.0. THEY DESCRIBE THE PREMISES FOR THE DESIGN OF INTERNET OF THINGS SOLUTIONS SUCH AS THE CONNECTED CAR OR THE SMART HOME.

1. Deutsche Telekom is taking forward the successful development of new Internet of Things and Industry 4.0 business models. It includes establishing a uniformly high level of data protection when connecting a large number of devices and production processes and the people behind them. In all of these cases Telekom's main concern is to ensure that people have confidence in the protection of their data. We develop the data protection-friendly solutions that our customers want.

2. Several companies are often involved in data processing for Internet of Things and Industry 4.0 business models, so the responsibilities of the companies involved must be described transparently and understandably across all process chains. Deutsche Telekom stands for that.

3. Deutsche Telekom processes personal data with which it is entrusted to meet its contractual arrangements with customers or to fulfill its obligations as a contract data processor.

4. Furthermore, we use as a matter of principle data that has been anonymized or, if in an indirect personal reference must be retained, that has been pseudonymized. Pseudonymization is achieved, for example, by means of high-level encryption. If the personal reference is to be restored, that person's consent must first be sought and received. That is what we mean by a culture of consent.

5. Deutsche Telekom will only ever pass data on in a form that makes it impossible for third parties to draw inferences as to an individual's identity. Telekom only passes on data with a direct personal connection with the customer's consent or if it is legally authorized to do so. ■

WELCOME TO THE ZETTABYTE AGE

DIGITAL TRANSFORMATION PRESENTS BUSINESSES AND SOCIETY WITH HUGE OPPORTUNITIES, BUT HARBORS SIGNIFICANT RISKS, TOO. WE NEED STANDARDS AND CLEAR-CUT RULES THAT PROVIDE PROTECTION – WITHOUT STIFLING INNOVATION.

Just five years ago the term Industry 4.0 did not mean much to anyone. Now, everyone is talking about it. Going digital involves interconnecting machines, objects and people, and is expected to raise efficiency in manufacturing, and bring businesses closer to customers. Production systems in smart factories do not need to be centrally controlled – they manage themselves. Parts, and the machines making them, exchange information via IT interfaces and the Internet. As they move along the conveyor belt, components fitted with RFID tags tell the production system where they want to go and how they are to be processed when they get there. Mass customization is swift and simple.

Smart, integrated processes are already commonplace in many German businesses – in manufacturing, warehouses and transportation, for example. They save time and conserve resources, driving down costs. However, they are point solutions, limited to specific operations and industries. End-to-end interconnectivity scenarios, such as driverless vehicles, call for much larger quantities of data to be transferred and processed. And that requires an infrastructure consisting of high-speed networks, high-availability cloud platforms, and data analytics tools that yield accurate knowledge and insights. Deutsche Telekom offers all of these things, and has become a key partner to public and privatesector organizations embracing digitization.

DATA BYTES AS NUMEROUS AS GRAINS OF SAND

Experts predict that more than a zettabyte of data (one followed by 21 zeros) will flow through the Internet in 2016. That is about the number of sand grains on all of the world's beaches. IDC market researchers estimate that in the next five years some 40 billion objects – from tractors to flower pots – will be sending real-time data over the Internet to a cloud for immediate analysis and processing. The larger the data basis, the more accurate findings will be.

In the future, smart analysis will not only benefit industrial players but ordinary consumers, too. And they will not need to lift a finger. It is already possible, without compromising data privacy, to use anonymized swarm data from cell phones to, for example, optimize bus and train schedules. That can benefit operators and passengers, particularly when major events take place. Emergency services likewise can employ swarm data to better estimate the number of persons potentially injured in an accident, and get help to them faster.

The general public stands to benefit enormously from medical data analytics. Important information is often locked away in hospital filing cabinets. Giving researchers easy digital access to this data – and the insight it contains – could dramatically improve our understanding of many conditions and how to treat them. Sadly, the reality is very different: there must be tens of thousands of hardcopy records stacked in the basements of hospitals that have filed for bankruptcy and closed down. Moreover, that data is neither anonymized nor adequately protected against theft.

DIGITIZATION SHOULD NOT BE SEEN AS A THREAT

The potential benefits of digitization are clear. But there are hazards, too – such as cybercrime. Innovation must go hand in hand with security. There is a need for clear-cut rules and standards – especially with regard to data processing. At the same time, those rules and standards must not stifle innovation.

Who should be permitted to use what kinds of data and for how long? What purposes are legitimate? What security standards should govern the Internet of Things? Specific answers to these vital questions must be found – and the issues they raise need to be debated frankly and openly. The public must be involved and kept informed about digital transformation, in order to allay doubts and fears. Industrial players and IT providers must clearly communicate the tangible benefits, stressing the safeguards that exist to guarantee personal privacy and keep data secure. Passing the EU General Data Protection Regulation was a first milestone. We must now set about shaping our digital future on these foundations. ■

Anette Bronder

has been a Member of T-Systems International's Board of Management and Director of its Digital Division since August 1, 2015. An economics and social science graduate, she began her career with Hewlett Packard, where she held a number of management positions. From September 2010 to July 2015 she headed up the Technology Enterprise Division at Vodafone Germany before being appointed its Director of Group Enterprise Solutions.

VIGILANCE REQUIRED WITH ONLINE BILL SCAMS

CYBER CRIMINALS CONTINUE TO ISSUE FAKE DEUTSCHE TELEKOM BILLS AS A MEANS TO SPREAD MALWARE. SINCE FEBRUARY 2015 THE COMPANY HAS INCLUDED ADDITIONAL SECURITY FEATURES IN ITS ONLINE BILLS AS A SAFEGUARD AGAINST FRAUD.

Online bills are personalized and include a salutation, a customer account number – and now, their street and house number. These new details appear in the e-mail's subject line and in the first sentence of the text. In addition, a fraud-proof verification symbol authenticates the e-mail, so customers can confidently distinguish a genuine bill from a scam. The symbol is visible when customers access their bill online via http://telekom.de/email or with Deutsche Telekom's mobile e-mail apps.

It comprises a blue @ overlaid with a check mark, and is displayed next to the sender name. It is compatible with GMX, WEB.DE, freenet and 1&1 accounts. However, for technical reasons the image cannot be shown in some e-mail programs – including Microsoft Outlook and Mozilla Thunderbird.

Deutsche Telekom has also created a new digital signature for its online bills. Although not visible, the signature can be detected by Internet service providers – enabling them to differentiate between authentic Deutsche Telekom files and e-mail from imposters.

Deutsche Telekom also includes a personal salutation and customer account number for the specific landline or cell. If a customer is unsure of a bill's authenticity, they can access the correct document via the online Customer Service Center. If the suspicious bill is not there – or requests payment of a different amount – then it is clearly a fake. Additionally, a request for an electronic transfer should be a red flag to any customer who has opted for direct debit payments.

It is highly advisable that e-mail recipients carefully inspect inbox items, particularly online bills and other personal documents. Anyone who is not a Deutsche Telekom customer, but receives a bill, should delete the e-mail unread. And genuine customers should by leery of any bill sent at an unusual time of month, or requesting an unexpectedly high payment – the recipient should scrutinize the e-mail for authenticity, and avoid opening any attachments.

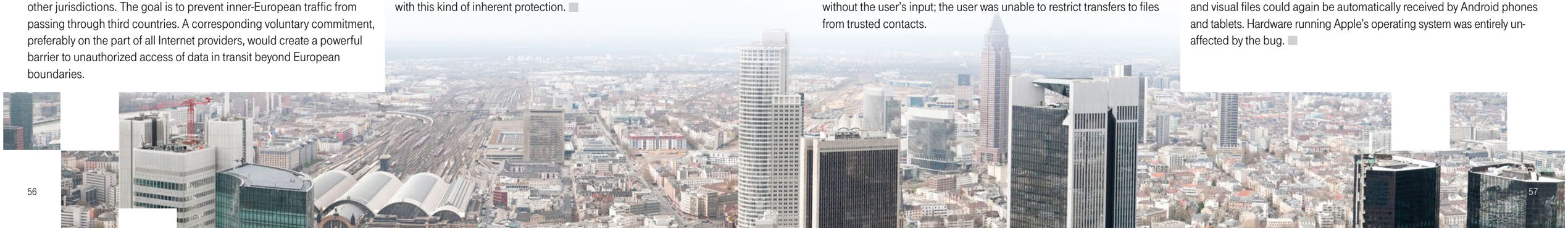
The sender's e-mail address can also be used to pinpoint a hoax. For landline accounts, the correct address should be rechnungonline@telekom.de and the sender should be given as "Telekom Deutschland GmbH {No-Reply}". With several e-mail programs the entire e-mail address becomes visible when the mouse cursor is hovered over the sender name. For cell phone accounts, the address should be Kundenservice.Rechnungonline@telekom.de. Business clients receive their online bills via servicecenter.gk@telekom.de. These addresses are displayed in full. ■

GREATER USE OF THE DE-CIX INTERNET EXCHANGE

DEUTSCHE TELEKOM HAS GREATLY INCREASED ITS USE OF THE DE-CIX NODE IN FRANKFURT AND CAN NOW EXCHANGE LARGER QUANTITIES OF DATA WITH OTHER PROVIDERS.

Within Germany Internet service providers route data streams among themselves through the country's commercial Internet exchange (DE-CIX). To improve online security, data should always be transmitted via the shortest possible route between sender and recipient – without diversions through other jurisdictions. The goal is to prevent inner-European traffic from passing through third countries. A corresponding voluntary commitment, preferably on the part of all Internet providers, would create a powerful barrier to unauthorized access of data in transit beyond European boundaries.

The direct-route approach described above is part of Deutsche Telekom's ten-point program for greater cyber security, and is already implemented within its own network infrastructure. Other providers have cited greater use of the DE-CIX exchange as a vital step towards building an Internet with this kind of inherent protection. ■



ENCRYPTED E-MAILS – FOR EVERYONE

IN MID-2016 DEUTSCHE TELEKOM AND THE FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY SIT WILL LAUNCH VOLKSVERSCHLÜSSELUNG, A SOLUTION THAT WILL ENABLE USERS OF ALL TECHNOLOGICAL BACKGROUNDS TO EASILY ENCRYPT THEIR E-MAILS.

In the past, widespread uptake of e-mail encryption technology has been limited by the principles of 'security by design' and 'usability by design'. Now, however, Deutsche Telekom has joined forces with the Fraunhofer Institute for Secure Information Technology SIT to develop a tool that will bring end-to-end e-mail encryption to a wider audience – not just IT experts. The solution – named Volksverschlüsselung, which roughly translates as 'encryption for the people' – is free, transparent and easy to use, and will be operated by Deutsche Telekom at a high-security data center. The goal is to make the latest cryptographic encryption methodologies accessible to all.

The new software solution generates all relevant encryption data automatically, and also pre-configures the user's e-mail clients. The majority of users will not require any additional software, as most e-mail programs are capable of encrypting messages once a suitable key is available. As a result, Volksverschlüsselung enables even relatively inexperienced users to send encrypted e-mails. Windows users will be the first to benefit from this innovative solution, which is compatible with e-mail clients such as Outlook and Thunderbird. The software will subsequently be rolled out to Mac OS X, Linux, iOS and Android. Volksverschlüsselung will initially support the S/MIME standard, with OpenPGP compliance due to follow soon after. Once the software has been released, Fraunhofer SIT will publish its source code – giving experts the opportunity to verify the robustness of the solution for themselves.

Volksverschlüsselung generates cryptographic keys on the user's end device. These private keys remain in the sole possession of the user at all times and are never passed on to the operator of the infrastructure. To deploy the technology, all users need to do is install the software and complete a straightforward and secure identification process. In the first phase of the project users will be able to authenticate using Deutsche Telekom's established registration process, or with an electronic ID card. Additional secure identification methods are set to be added in the future.

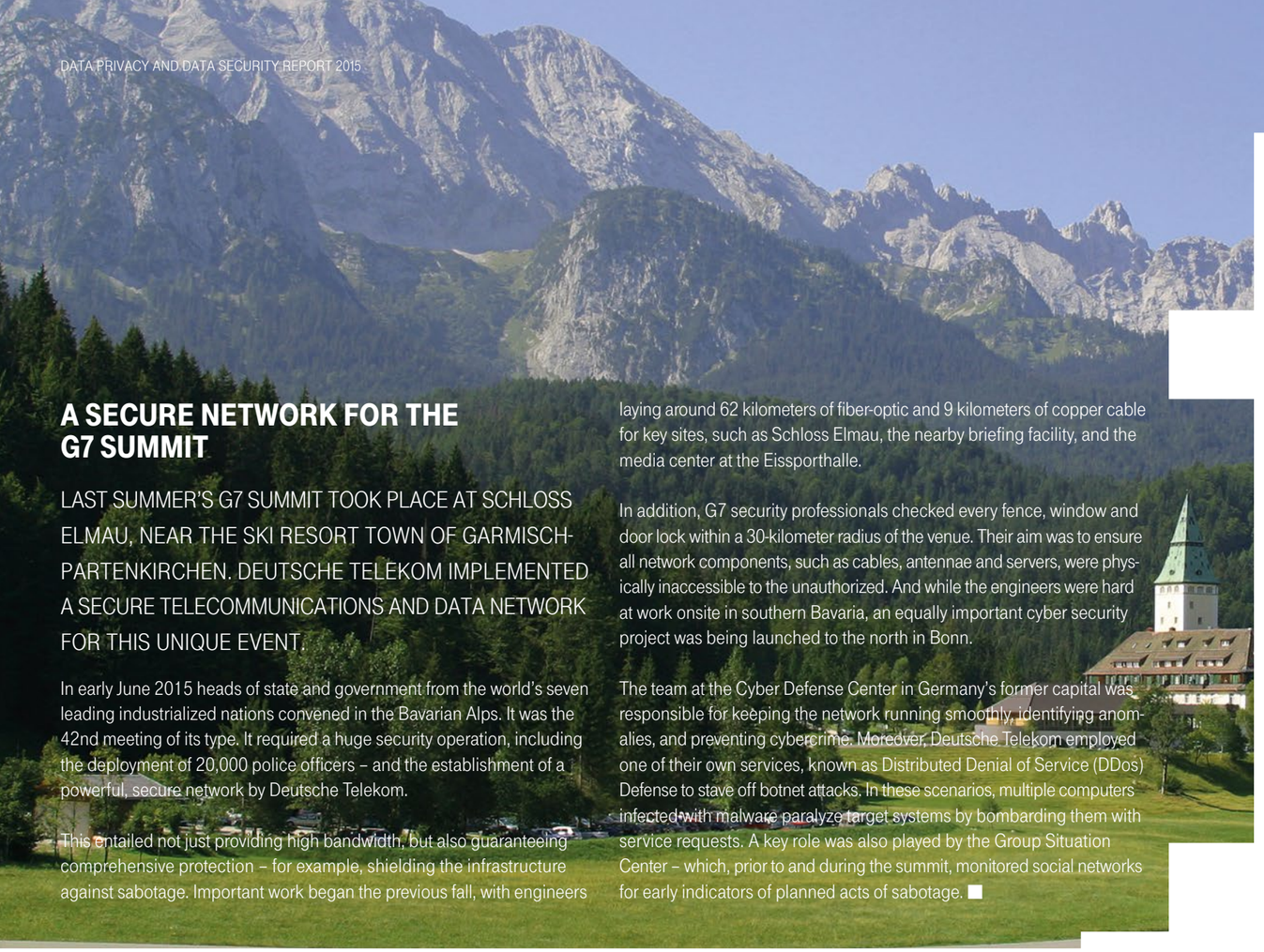
To find out more about the Volksverschlüsselung solution – and about encryption in general – visit www.telekom.com/verschluesselung or www.volksverschluesselung.de (in German only). ■

OVERCOMING ANDROID'S STAGEFRIGHT FLAW

AN ERROR FOUND IN ANDROID'S OPERATING SYSTEM IN SUMMER 2015 POSED A THREAT TO DEVICES ON NETWORKS WORLDWIDE. IT LEFT CORRESPONDING SMARTPHONES OPEN TO THIRD-PARTY CONTROL VIA INFECTED MULTIMEDIA (MMS) MESSAGES.

The vulnerable part of the operating system, known as Stagefright, is needed to play multimedia content. The malware was able to spread through a variety of channels, including WhatsApp, Hangouts, Facebook, MMS, Web browsing, file downloads and more. It was also able to access the user's address book and propagate to other endpoints by this means. The bug was particularly dangerous in the case of MMS messaging: multimedia messages were automatically downloaded from the server without the user's input; the user was unable to restrict transfers to files from trusted contacts.

To protect their customers, Deutsche Telekom temporarily switched from automatic to manual downloading. As a result users were fully aware of the content they were loading onto their devices. Moreover, the company implemented additional security mechanisms within their network infrastructure; if files were seen to be exploiting the Stagefright weakness, they were flagged as dangerous and not forwarded to the recipient. Any non-infected content was sent as usual. With this constraint in place, audio and visual files could again be automatically received by Android phones and tablets. Hardware running Apple's operating system was entirely unaffected by the bug. ■



A SECURE NETWORK FOR THE G7 SUMMIT

LAST SUMMER'S G7 SUMMIT TOOK PLACE AT SCHLOSS ELMAU, NEAR THE SKI RESORT TOWN OF GARMISCH-PARTENKIRCHEN. DEUTSCHE TELEKOM IMPLEMENTED A SECURE TELECOMMUNICATIONS AND DATA NETWORK FOR THIS UNIQUE EVENT.

In early June 2015 heads of state and government from the world's seven leading industrialized nations convened in the Bavarian Alps. It was the 42nd meeting of its type. It required a huge security operation, including the deployment of 20,000 police officers – and the establishment of a powerful, secure network by Deutsche Telekom.

This entailed not just providing high bandwidth, but also guaranteeing comprehensive protection – for example, shielding the infrastructure against sabotage. Important work began the previous fall, with engineers laying around 62 kilometers of fiber-optic and 9 kilometers of copper cable for key sites, such as Schloss Elmau, the nearby briefing facility, and the media center at the Eissporthalle.

In addition, G7 security professionals checked every fence, window and door lock within a 30-kilometer radius of the venue. Their aim was to ensure all network components, such as cables, antennae and servers, were physically inaccessible to the unauthorized. And while the engineers were hard at work onsite in southern Bavaria, an equally important cyber security project was being launched to the north in Bonn.

The team at the Cyber Defense Center in Germany's former capital was responsible for keeping the network running smoothly, identifying anomalies, and preventing cybercrime. Moreover, Deutsche Telekom employed one of their own services, known as Distributed Denial of Service (DDos) Defense to stave off botnet attacks. In these scenarios, multiple computers infected with malware paralyze target systems by bombarding them with service requests. A key role was also played by the Group Situation Center – which, prior to and during the summit, monitored social networks for early indicators of planned acts of sabotage. ■

CYBER SECURITY AWARENESS IN GERMANY

DEUTSCHE TELEKOM IS A HIGHLY ACTIVE PARTICIPANT IN THE GERMAN INTERNET SECURITY INITIATIVE DEUTSCHLAND SICHER IM NETZ (DSIN). AT A MEETING OF ITS MEMBERS, THOMAS KREMER, MEMBER OF THE BOARD OF MANAGEMENT FOR DATA PRIVACY, LEGAL AFFAIRS AND COMPLIANCE AT DEUTSCHE TELEKOM, WAS ELECTED CHAIRMAN.

"As a central platform for consumers and businesses, DsiN provides guidance and information on safely navigating the digital world," explains new chairman Thomas Kremer. In the future, DsiN will place greater focus on emerging topics, such as smart homes, connected vehicles and digital education. "We invite any organization that recognizes the key role played by security and trust in digitization to join DsiN."

DsiN was established nine years ago within the scope of Germany's first National IT Summit. The initiative is operated under the aegis of the German Federal Ministry of the Interior, and offers consumers and enterprises practical advice and resources on cyber security issues. DsiN works hand in hand with its members and partners to develop new strategies and mechanisms for Web security. For example, Deutsche Telekom contributed to DsiN's Security Barometer, a section of its website that provides trafficlight warnings of current Internet threats. 2016 marks DsiN's tenth year of activity – to commemorate this milestone, the initiative produced a special publication describing key aspects of its work (available in German only). Themes include mobile security, e-government and connected health. ■

DEUTSCHE TELEKOM'S ONLINE IT SECURITY GUIDE

IN TODAY'S IT WORLD CYBERCRIME, MALWARE AND PHISHING ARE EVER-PRESENT PERILS. WEB USERS MUST ARM THEMSELVES AGAINST MULTIPLE THREATS, INCLUDING VIRUSES, WORMS, PERSONAL DATA MISUSE AND THEFT OF BANK DETAILS.

The Internet offers a wealth of advice on IT security, yet this content is dispersed across thousands of Web pages. But help is at hand for German-speaking Web users. The website www.sicherdigital.de consolidates this information and presents it in a style that explores and addresses the real-world imperatives of multiple user groups – from the young to the elderly, from parents to professionals. The site offers hints and tips to keep users and their data safe and secure at all touchpoints with the digital world. Lena and Lukas represent the younger generation, while parents will relate to Sandra and her son Max. The example of entrepreneur Matthias illustrates the priorities of today's business leaders, and the online experiences of Renate and Horst will strike a chord with older generations.

The intuitive guide offers visitors a fun way to engage with these scenarios and become familiar with the associated security risks. Users are prompted to ask themselves what they should look out for, and to consider how they can effectively shield themselves against threats. Possible solutions include adjusting basic smartphone settings and creating restricted accounts for children and teen users. In addition to informative articles, the site includes a series of checklists that provide an at-a-glance overview of the most important advice for each security topic. Users can complete interactive questionnaires to assess their own level of protection, and watch video clips that illustrate how each user group should tackle IT security issues.

Visitors can also browse content by topic. This alternative structure allows users to quickly locate information on specific issues, such as basic protection for PCs and laptops, e-mail security and safe online banking. This method is also available on the smartphone-friendly version of the website.

www.sicherdigital.de serves as a single, easy-to-use resource for information on online security. The goal is to enable users to safeguard themselves and their data against the perils of the digital age. What's more, visitors can click on links embedded into articles to access more in-depth content from across the Web. ■

AWARD-WINNING SECURITY

BERLIN WAS HOST TO THE 2015 OUTSTANDING SECURITY PERFORMANCE AWARDS, HELD ON THE EVE OF A CONFERENCE STAGED BY ASW BUNDESVERBAND (AN ALLIANCE DEDICATED TO PROMOTING SECURITY IN BUSINESS). DEUTSCHE TELEKOM WAS RECOGNIZED IN THREE CATEGORIES, WITH ACCOLADES GOING TO THEIR FACEBOOK PRIVACY APP, THEIR WORK ON THREAT MANAGEMENT AND THEIR ROLE IN PREVENTING METAL THEFT.

Deutsche Telekom was named Germany's Outstanding Security Installer by the OSPA judges in recognition of its Facebook privacy app. This allows the user to identify who can view their personal information, who can search for them, and who is able to post on their timeline. It also supports one-click configuration of privacy settings.

Deutsche Telekom was also shortlisted in the category of Outstanding Security Consultants for its threat management. The corresponding processes are designed to ensure that all employees enjoy a working environment free from violence and harassment. Any member of staff can seek help from the in-house threat management team if they are subject to unwanted advances or stalking, or are in fear of physical threats or psychological intimidation. They are also encouraged to come forward if they observe colleagues behaving suspiciously or expressing violent thoughts. In little more than two years, Deutsche Telekom's certified threat managers have come to the assistance of around 200 employees.

Furthermore, the judges shortlisted Deutsche Telekom for its contribution to SIPAM, a partnership established to prevent theft of metal, in the category of Outstanding Security Partnership. SIPAM is an alliance of companies and industry associations in logistics, telecommunications, mining and energy. This initiative was formed in 2012 with the cooperation of Deutsche Telekom, German railway operator Deutsche Bahn (DB), utility RWE and the Association of German Metal Dealers (VDM). The majority of SIPAM's members operate critical infrastructure – resources that are of vital importance to the general public, the economy and the government.

Members of the judging panel included Michael Henge, the former President of the German Federal Office for Information Security (BSI), and Dr. Hans-Georg Maassen, President of Germany's domestic intelligence service (BfV). The very first OSPAs to be presented in Germany honored individuals and businesses in the security industry for exceptional achievements. The awards are held in various countries, in collaboration with a variety of security associations and groups. ■

“IT’S A MATTER OF TRUST”

IN DECEMBER 2015, ANONYMOUS HACTIVISTS TRAINED THEIR CROSSHAIRS ON TURKISH INTERNET SERVICES. GHOSTSEC DECLARED DIGITAL WAR ON THE ISLAMIC STATE. AND THE GERMAN BUNDESWEHR ESTABLISHED A DEDICATED UNIT OF CYBER DEFENSE EXPERTS. SOME THREE YEARS AFTER THE EDWARD SNOWDEN REVELATIONS CYBER WAR HAS BECOME A SERIOUS THREAT TO SOCIETY. AXEL PETRI, SENIOR VICE PRESIDENT OF SECURITY GOVERNANCE, SHEDS LIGHT ON THE CHANGES.

Mr. Petri, when will conventional warfare be rendered obsolete by its digital equivalent?
Axel Petri: There is no doubt about it: the Internet is now an established platform by which states and international organizations attack or paralyze other nations’ computer systems. It is an advanced form of warfare. This led to the discussion of hybrid warfare at the Munich Security Conference in early 2015 – in other words, the combination of conventional and non-conventional forms of warfare, including cyber attacks.

Has Edward Snowden contributed indirectly to the sharp increase in the number of cyberattacks?
Axel Petri: No, he simply exposed what had long been reality. Spies spy; that’s no great surprise. Snowden simply opened our eyes to the fact. But even post-Snowden, I see the need for intelligence agencies. However, the central issue is striking the right balance between security and privacy. The documents released by Snowden have revealed many activities that are beyond the pale – and pursued without the knowledge of the general public; not even of the corresponding governments.

What role do intelligence agencies play in attacks on German targets?
Axel Petri: In many countries industrial espionage falls within the national intelligence agencies’ official remit. Many foreign agencies devote significant financial and organizational resources to spying on Germany. The question is why? According to Germany’s domestic intelligence service (Bundesverfassungsschutz), they are primarily driven by geopolitical and commercial interests. We are a member of NATO and the EU, have a powerful economy, with innovative businesses. That is motivation enough for espionage. The concept of an Internet free from surveillance is therefore illusory; however, some activities seem excessive. Increasingly, security agencies are being perceived as perpetrators by the general public. That is an unhealthy development. Government institutions need to regain their citizens’ trust. And for me, a key element is increasing visibility into general surveillance activities. At Deutsche Telekom, we are already doing a great deal, for example with our report on lawful interception and data provision. But the security agencies could up their game considerably.

What other threats exist?
Axel Petri: Notwithstanding the debate surrounding Snowden, we should not lose sight of the rising number of conventional cyber criminals, their increasing professionalism, and the growing availability of simple but effective tools. There is a thriving market for malware: paying customers receive excellent around-the-clock service. And, ultimately, this has a far greater impact on consumers and businesses. All major companies are subject to cyberattacks. We cannot afford to drop our guard in the battle against hackers; we must continuously improve.

Will the number of cyberattacks continue to grow?
Axel Petri: We must assume that multidimensional attacks, comprising both physical and digital elements, will rise inexorably. Cyber space continues to grow in significance. Anything and everything that can be digitized, will be digitized. Anything and everything that can be connected will be connected. And the quantity of attacks will soar accordingly. But far more worrying is the improving quality of attacks. This will call for entirely new security strategies and solutions.

That smacks of defeatism.
Axel Petri: If you snooze, you lose! Although total security in our virtual world is unachievable. But we have to decide what kind of digital society we want, what security culture we want – and what we are willing to do to uphold it. At Deutsche Telekom we are taking an active part in this discussion, because we are very much active players.

How do people respond to news of governments and businesses being hacked?
Axel Petri: People are more and more distrustful of the digital world. And trust is one of the decisive success factors in the digital age – perhaps the single most important one. In 2011 42 percent of the German population had confidence in the security of their data on the Internet. A year later, that had plummeted to 29 percent, and to just 16 percent in 2013. This is terrible for a society building its future on digitization. Without the Internet there will be no progress. We need the Internet and we need people to trust the Internet, and to make use of the new digital opportunities.

How can we regain that trust?
Axel Petri: First of all we need more effective security processes. In other words, we need to combine physical security and cyber security at an organizational level. Once the processes are in place, you need to switch focus to technological innovation, for instance in the shape of a cyber defense center that observes all network activities and takes remedial action when required. This is the only way to keep pace with the attackers, and the only way for in-house security experts to provide employees with the information and tools they need to recognize dangers. We cannot stand still. We must significantly raise awareness of cyber security issues at a very early stage, in schools, and continue in universities. Very few of tomorrow’s executives and business leaders will study IT-specific subjects – so we must embed cyber security within more typical courses, such as business administration and law. People who recognize dangers will automatically adapt their behavior, improving their safety.

So businesses have a big part to play?
Axel Petri: We have to make the dangers more visible. Deutsche Telekom does this by means of its online overview of current cyber attacks (sicherheitstacho.eu), and by proactively warning customers of threats. And we need a level playing field: any company addressing the European market must adhere to our rules and standards. Hardware and software vendors, ICT providers and over-the-top services – the free transmission of text, video and audio – need to commit to security and privacy principles, to act transparently, and to be involved in counter-measures. We need to gain the participation of everyone in the value chain if we are to raise security to levels that build and rebuild customers’ trust in digital products and services.

Axel Petri

is Senior Vice President of Group Security Governance at Deutsche Telekom and the Group’s Security Officer in accordance with Section 109 of the German Telecommunication Act (TKG). Petri, who holds a degree in law, is tasked with coordinating and harmonizing security throughout the Deutsche Telekom Group. This includes strategy, policies, monitoring and enforcement of all aspects of security, and overseeing cooperation between all internal security units. Furthermore, he is responsible for protecting information and other valuable business assets, and for investigation and prevention

SECURITY WITHOUT BORDERS

DATA PRIVACY AND DATA SECURITY DO NOT END AT NATIONAL BORDERS. TELEKOM ENSURES THAT UNIFORM STANDARDS ARE OBSERVED AROUND THE WORLD.

Statutory data privacy and data security requirements differ from country to country. In Germany they are especially high and in many other countries relatively low. Telekom nevertheless endeavors to offer its customers all over the world the high level of protection and security that is typical of it and is a statutory requirement in Germany. Group Security Governance (GSG) ensures that all Group units around the world observe the same standards.

GSG ensures by means of continuous checks that all business units implement the security guidelines of Telekom's governance model, and that means not only all internal units and international country companies but also external suppliers that store or process data on Telekom's behalf.

SECURE AND WITHIN THE LAW EVERYWHERE

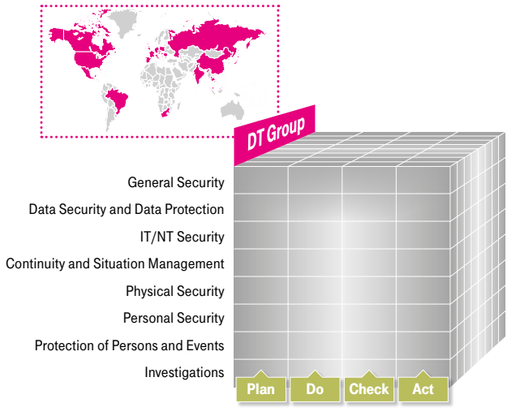
To complement this task meaningfully, GSG set up in 2009 the Audit Council, which brings together at regular intervals all Group units that are responsible for audits. The Audit Council shares national and international audit findings, and coordinates annual planning. This joint approach ensures that the right priorities are set and synergies are identified or put into practice.

Kai Stursberg, one of the Group Security Governance auditors, says: "Both at the operational and the strategic level we meet several times a year. For one we discuss the implementation of standards and control systems; for another we plan which security-relevant issues require special attention in the future." One of the important issues for the future is cross-border data traffic. The Connected Car is a graphic example of what this means. "Imagine," Stursberg says, "that you are driving a connected car across Europe, and that data is transmitted and received when you cross borders. We will ensure that Telekom handles this data securely and in compliance with statutory requirements everywhere."

Since January 2015 GSG has worked even more intensively with international colleagues. GSG specialists from Germany regularly visit country companies to review the status of policy implementation in governance checks lasting several days. With the help of the Audit Council they have already been able to bundle some activities, and undertake them jointly with other audit units.

THE TELEKOM SECURITY GOVERNANCE MODEL

The governance model defines the Group's entire organizational structure, and describes all the guidelines and measures required to manage and control it. The Group guidelines that it includes ensure the high level of security and data protection at Telekom.



REINFORCING THE HUMAN FIREWALL

DEUTSCHE TELEKOM HAS INTRODUCED A STRATEGY TO RAISE SECURITY AWARENESS THROUGHOUT THE GROUP.

Information is key to business success. And as a result data security and integrity are essential, particularly in electronic transactions. These parameters influence customer loyalty and purchasing behavior. However, security is not a matter of technical mechanisms alone – it is about the right combination of technology, processes and people. In fact, the human factor is vital to ensuring the availability, confidentiality, integrity and authenticity of information.

Cordula Tanner, a Member of the Communication, Training and Awareness team within Group Security Governance (GSG), explains: "Our employees represent a human firewall that we continue to strengthen and reinforce. This firewall is an integral part of end-to-end security."

THE MOST EFFECTIVE SECURITY MEASURE IS AWARENESS

Deutsche Telekom has been investing in security awareness campaigns, training courses and communication activities for a number of years – to ensure employees understand the key principles of data protection and information security, and how to implement them. In early 2015 the corporation introduced a Group-wide strategy with the aim of systematically and effectively raising security awareness among staff worldwide.

STRICTLY CONFIDENTIAL: CUSTOMER PRIVACY

CONFIDENTIALITY OF TELECOMMUNICATIONS, CUSTOMERS' PERSONAL DATA AND TELECOMMUNICATIONS AVAILABILITY ALL ENJOY SPECIAL STATUTORY PROTECTION IN GERMANY.

Network operators and providers of telecommunications services must abide by the provisions of the Telecommunications Act (TKG), which regulates protection and security requirements. Anyone who provides publicly accessible communications must ensure that customers phones cannot be tapped without authorization and that the confidentiality of telecommunications is observed.

For this purpose Section 109 TKG requires network operators and providers of telecommunications services to appoint a security officer and to draw up a security concept. The security concept must describe which technical provisions and measures the provider undertakes in order to fulfill statutory security and data protection requirements. At the official level the Federal Network Agency is responsible for checking compliance with security requirements. To do so, it carries out regular audits of providers.

CHECKS HAVE ALWAYS DRAWN A BLANK

Telekom's Group Security Governance team draws up and updates the security concept for Deutsche Telekom AG, Telekom Deutschland GmbH and T-Systems International GmbH. Whenever there is an organizational or technological change, the team revises the confidential contact and submits it to the Federal Network Agency.

As Germany's largest telco Telekom maintains close contacts with the authorities. Full security audits are undertaken annually or at least every other year. In addition, the Federal Network Agency continuously checks on a theoretical basis how Telekom deals with security-relevant issues and threat scenarios. All checks have always given Telekom a clean sheet and been entirely to the Agency's satisfaction, thereby confirming the concept and implementation of security measures at Telekom. And Group Security Governance ensures that it stays that way.

LEADING IT SECURITY SERVICE PROVIDER

AT EIGHT TIMES IN THE LEADER QUADRANT IN EIGHT SERVICE CATEGORIES, THE EXPERTON GROUP SEES DEUTSCHE TELEKOM AS THE LEADING PROVIDER OF SECURITY SOLUTIONS IN THE 2016 SECURITY VENDOR BENCHMARK.

In all categories the Experton analysts rate Telekom as being the "strategic pace setter and opinion leader among the providers with a highly attractive service offering and a particularly strong market and competitive position". The categories evaluated were Database Security, Cloud and Datacenter Security, Backup / Data-Recovery Services, Identity & Access Management, Mobile Security Services, Managed Security Service, Security Consulting and Disaster Recovery Services.

As in other areas, outsourcing is becoming increasingly popular in the security market. According to the benchmark Deutsche Telekom is "the measure of things in respect of both the attractiveness of its portfolio and its competitive strength in the market for managed security services". The reasons for outsourcing security include especially the lower investment costs and always up-to-date knowledge of the constantly changing cyber-threats. Telekom's portfolio also covers the entire bandwidth of security services, enabling it as a security provider to assume end-to-end responsibility. "An increasingly strong argument for Deutsche Telekom is the provision of services from Germany that are subject to the provisions of German data protection law," the Experton analysts found.

They emphasize in the benchmark that Telekom uses for all in-house security and customer projects tools of its own, such as the PSA (Privacy and Security Assessment) or ESARIS (Enterprise Security Architecture for reliable ICT Services). With these tools security vulnerabilities can be identified and, on the strength of the findings, a catalog of measures can be developed. The security products used are then chosen jointly with the customer on a vendor-independent basis.

In 2015 Deutsche Telekom again continued to expand its security services portfolio. In addition to solutions for Mobile Device Management (MDM), Telekom provides Symantec and Norton antivirus solutions and a corporate container solution, the Safe Mobile Business app, which it developed in-house. Using the Mobile Encryption app, telephone calls can be encrypted, now including conference calls with up to three participants. The highly secure Mobile Encryption app encrypts both phone calls and texts.

Telekom's Identity & Access Management service coverage deals in particular with Authentication and Identity as a Service. It includes two-factor authentication for authorizing users by smartphone, text or hardware token, and a validation service for authentication procedures such as by smart card or biometrics. Telekom also offers Single Sign-on as a Service for access to SaaS offerings, and Web services in the cloud as well as local applications.

Telekom can hold its own in the concert of major international players in the area of security consulting, too. In this area the three best set themselves apart from other providers in the leader quadrant because they are a little stronger than the competition in local market position, sales and marketing strength, awareness, and overall customer satisfaction. ■

DATA PRIVACY AND DATA SECURITY REPORT 2015

CONTINUOUS ASSESSMENT AND IMPROVEMENT

DEUTSCHE TELEKOM CONDUCTS REGULAR SURVEYS TO ASSESS THE QUALITY OF INFORMATION SECURITY AND THE LEVEL OF AWARENESS THROUGHOUT THE GROUP. THE RESULTS SERVE AS A BASIS FOR CONTINUOUS IMPROVEMENT.

Once a year the Group Security Governance (GSG) team conducts an enterprise-wide survey to gauge security awareness. Worldwide, all organizational units with ten or more staff members take part. An online tool is used to assess security consciousness, and to verify the effectiveness of past awareness initiatives. The study tracks changes in security consciousness over time and allows comparisons between units. It also identifies weaknesses, indicating where action is required.

The results are anonymized and combined to create an aggregate score, reflecting the average level of security consciousness. The findings are discussed by all stakeholders, and serve as the basis for recommended activities such as training.

ALWAYS UP TO DATE

GSG also conducts a second survey, aimed specifically at the security officers in all units. The aim is to assess security maturity throughout the Group by means of self-evaluations. Each unit is assessed in its own right, and receives its own consolidated report. Furthermore, GSG forwards the aggregated results of all reports to the central security teams. This provides surveyed units and central security professionals with a transparent benchmark. It serves as a basis for discussing security issues and activities. All results are also complied into an annual international review of security. Senior executives use the insights they have gained to maintain a high level of security. ■

SECURITY AS A SUCCESS FACTOR

IS SECURITY A TIRESOME COMPULSORY DUTY OR A PROFITABLE FREESTYLE? FOR TELEKOM THE QUESTION DOES NOT ARISE. IT CONSISTENTLY ENDORSES DATA SECURITY AND PURSUES A GROUP-WIDE SECURITY STRATEGY.

For a leading European telecommunications provider security is one of the success factors in the market. Telekom has developed for it a strategy consisting of three strategic security streams, and based on the Group's comprehensive security excellence slogan "Protect – Enable – Monetize powered by Security Excellence". The strategy is based on protecting the company itself along with its network infrastructure, the IT solutions that it uses, and all of the data that is linked to it – especially customer data.

Protect comprises three areas: security culture, security operations and security compliance. Culture includes governance, responsibilities and uniform security specifications. Operations are preventive, defensive and reactive security measures. They include inter alia the use of defense technologies or the Cyber Defense Center. The compliance block ensures efficient observance of statutory, and regulatory provisions and requirements, and their implementation within the Group.

Enable, the second strategic security stream, is aimed at in-house Telekom areas, the general public and customers. In-house, security requirements are integrated seamlessly into products, services and solutions. An important process aimed at consistently incorporating security and data protection into products from the outset is the Privacy & Security Assessment (PSA) that accompanies all IT and network development processes at Telekom.

Positioning as a trustworthy company is undertaken by means of commitments to political debates, participation in bodies, or transparent description of data privacy and data security measures. It also includes gaining security certificates issued by recognized certification bodies and auditors after appropriate scrutiny. They testify to Telekom's security expertise and the use of security-compliant processes at the company.

The third strategic security stream is focused on bundling the Group's existing security know-how in a separate security division, and on marketing this comprehensive security accordingly (Monetize). In future, it will offer private, SME and large customers security products and services from a single source. The aim is to be a leading provider in the European security market. ■

RECERTIFICATION AND CONTINUOUS IMPROVEMENT

AN INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) IS DYNAMIC IN NATURE: IT IS ABOUT PROGRESSION, EVOLUTION AND IMPROVEMENT. IN 2015 DEUTSCHE TELEKOM'S ISMS WAS RECERTIFIED BY GERMAN AUDITING COMPANY DQS.

An ISMS models processes and defines rules which control, monitor and continuously improve information security. Deutsche Telekom employs an ISMS to manage security services across the entire Group. In 2015 DQS audited the solution and renewed its certification to ISO/IEC 27001:2013.

Recertification is proof positive of Deutsche Telekom's consistently high security standards and its ability to enhance existing mechanisms. It is also a way of building and maintaining customer trust. However, certification is only one aspect of an ISMS's lifecycle. This flexible and evolving system is subject to a continuous improvement process – which is essential to systematically identifying and eradicating residual risk.

In addition, Deutsche Telekom's certified security information management system plays a pivotal role in attracting business customers – for example, to its cloud-based solutions, hosted at the Group's German data centers.

SECURITY PROFESSIONAL DEVELOPMENT

SECURITY CANNOT BE ACHIEVED SOLELY BY MEANS OF TECHNICAL SOLUTIONS. COMPANIES NEED WELL-TRAINED SECURITY EXPERTS TO COPE WITH THE INCREASINGLY EXACTING REQUIREMENTS. TELEKOM HAS PUT IN PLACE AN IN-SERVICE FURTHER TRAINING PLAN TO DEVELOP SECURITY EXPERTS WHOSE QUALIFICATIONS ARE IN LINE WITH INTERNATIONAL INDUSTRY STANDARDS.

As in all industries and larger enterprises, security experts acquire appropriate qualifications. As a rule they correspond to national requirements. In view of the global cooperation of over 50 Telekom companies on security matters, extensive international expertise is required.

That applies especially to each and every Telekom company's Chief Security Officer, but also to experts in other security contexts such as business continuity or fraud managers. Annual courses are held accordingly, arranged alternately as on-site or online training. In 2015 over 60 employees from Germany and Telekom country companies attended different e-learning courses and workshops.

Enterprise Security Risk Management is an important and complex further education topic. Jointly with a UK partner, Telekom trained 24 Telekom employees per course who were engaged in international business. Risk managers analyze security risks at their specific companies and show how to handle them in order to reduce risks to a minimum.

As a consequence of the global increase in cybercrime, fraud plays an increasingly important role. White-collar crime is serious for companies in two respects. It causes specific damage and can be accompanied by a loss of trust and reputation. Training to tackled fraud is a correspondingly important part of the further training program for Telekom security experts. In 2015 nearly 50 people took Fraud Manager, International Certified Fraud Investigator and Advanced Certified Fraud Investigator courses.

In addition to in-house, further training as security professionals Telekom takes part in many cross-enterprise networks in which security experts and security professionals discuss current developments. It is also engaged in constant exchanges with university researchers and is, for example, developing with the Hochschule für Telekommunikation in Leipzig a cybersecurity online training course for non-technicians.

Furthermore, the security team is currently setting up a library focused on security issues, that contains a wide-ranging collection of specialist books both in print and online. It will also include a collection of white papers – because you can only take precautions if you know your subject. A danger recognized is a danger averted.

MORE CHECKS, FEWER RESOURCES

REGULAR CHECKS ARE THE ONLY WAY TO ENSURE LASTING COMPLIANCE WITH DATA PRIVACY AND DATA SECURITY PROVISIONS RIGHT ACROSS THE GROUP. SINCE 2015 THE TELEKOM CONTROL TEAMS HAVE BEEN WORKING ACROSS DEPARTMENTS.

Trust is good, control is better. That is why separate teams from Telekom's data privacy and data security departments have hitherto ensured by means of regular on-site checks, including checks of country companies, that data privacy and data security regulations are complied with. It was a time-consuming task for the two control teams that traveled separately around Europe, Asia and America.

Since 2015 Data Privacy and Data Security have carried out most of the checks jointly. To do so, they coordinate their dates and can carry out more checks with smaller teams. That is possible because data privacy and data security overlap. Without technical implementation data protection is impossible in the digital age.

The common dates are a win-win situation for all concerned. With personnel resources limited for preparing and supporting checks in Telekom countries, they now only have to make their resources available once. The control teams themselves are smaller, too, because there are overlaps. That frees up resources in order to carry out more checks or to support implementation of the measures agreed better.

TAKING ON THE FRAUDSTERS

DEUTSCHE TELEKOM HAS ASSEMBLED AN INTERDISCIPLINARY TEAM OF SPECIALISTS TO TACKLE FRAUD. THEIR TASK IS TO MAKE SURE SALES PARTNERS PLAY BY THE RULES, IN EVEN THE FIERCELY COMPETITIVE TELECOMS MARKET.

External sales partners have not always played fair. They have, on occasion, earned bonuses and commission by illegitimate means. This has included non-approved sales practices, employment of unauthorized sub-contractors, and the creation of phantom customers to manipulate sales figures.

In response, Deutsche Telekom formed an interdisciplinary "round-table", comprising representatives of various departments. Their mission is to tackle fraudulent conduct on the part of sales partners. Since 2012, members have been gathering every two weeks to discuss incidents and to agree and coordinate activities. The results of these meetings are reported to senior management.

The team brings together experts in sales, risk management, corporate criminal law, civil law, auditing, data protection and compliance. Its work is overseen by Deutsche Telekom's Security unit. It has, to date, identified more than 100 counts of fraud. The body has recommended a variety of responses, such as terminating contracts, bringing claims for damages, and reporting criminal activity to the authorities. These actions have proven effective in ensuring sales partners clean up their act.

DIGITAL EDUCATION: GETTING THROUGH TO CITIZENS AND BUSINESS

DEUTSCHLAND SICHER IM NETZ (DSIN) – LITERALLY "GERMANY SECURE ONLINE" – PROVIDES GUIDANCE ON SAFELY NAVIGATING THE DIGITAL WORLD. THIS NOT-FOR-PROFIT ORGANIZATION DEVELOPS IMPACTFUL CAMPAIGNS AIMED AT CONSUMERS AND AT SMALL AND MEDIUM-SIZED ENTERPRISES (SMES). TO MARK ITS TENTH ANNIVERSARY IN 2016, DSIN IS INVITING NEW PARTNERS AND COMPANIES TO GET ON BOARD.

The 2015 annual DsiN security index for consumers delivered a clear message: while people are increasingly concerned about online risks, they are unwilling to take the necessary precautions in their own lives. This trend is by no means limited to the subgroup dubbed 'fatalists' by the report – it also applies to users classified as 'over-trusting' and 'outsiders'.

For DsiN, this study provided further impetus to push ahead with its awareness raising work in Germany in 2015, and to continue to professionalize its activities in cooperation with its partners. To this end, the organization's Digitale Aufklärung 2.0 (Digital Education 2.0) initiative focuses on three joint activities:

1. Target-group-specific awareness raising – tailored to the needs of individual consumers, rather than a one-size-fits-all approach
2. Bringing together existing initiatives so that enterprises and consumers can find offerings more easily
3. Promoting discussion between stakeholders across research, business, society and politics – with the aim of better understanding and exploiting the potential of awareness-raising activities

One example of how DsiN unites various offerings is the Aktionsbund Digitale Sicherheit (Digital Security Action Group), established in the summer of 2015. This provides a platform where DsiN partners can draw attention to not-for-profit digital education initiatives, so that consumers and employees can easily find what they are looking for. In the first few months alone, the group has grown to comprise fifty organizations. The service can be integrated into any Web portal as an iframe free of charge.

Since November 2015 the SiBa-Sicherheitsbarometer (Security Barometer) app has delivered tailored advice to consumers on navigating the digital world. It offers an overview of cyber threats, drawing on information provided by partners such as the German Federal Criminal Police Office (BKA), the Federal Office for Information Security (BSI), the Association of German Banks (Bankenverband), the German Insurance Association (GDV), and DsiN members Deutsche Telekom, Microsoft and Nokia. The barometer can be configured to display information on specific topics such as the smart home or connected healthcare. And it has already taken off in a big way, with 25,000 consumers using the app in the first few weeks alone.

A key aspect of DsiN's approach is to address individual user groups – with exciting initiatives such as the myDigitalWorld competition. Staged for the first time in 2015, this contest recognizes outstanding Internet security efforts on the part of young people and school students. Winners received some great prizes, ranging from trips to London to support for their projects. Competition sponsor was the Federal Ministry of the Interior, which lauded the participants as role models for their generation.

But it is not only consumers that are unwilling to address security in more depth. Small and medium-sized enterprises, too, often struggle with these challenges and lack expertise. As such, DsiN's work in 2015 paid special attention to the needs of these organizations with activities including:

- IT-Sicherheit@Mittelstand, a program run by DsiN and the Association of German Chambers of Commerce and Industry (DIHK), offers guidance to SME decision makers and IT managers on IT security in their businesses. Patron is the Federal Minister for Economic Affairs, Sigmar Gabriel. The initiative is operated under the aegis of DsiN, and provides chambers of commerce throughout Germany with expert speakers and free documentation.
- A series of DsiN guides, published in conjunction with DsiN member DATEV, offers in-depth advice on enhancing business security. Last year, publications focused on combating social engineering in the workplace. These guides can be accessed from DsiN free of charge.
- The DsiN blog aims to promote dialog on IT security. For over four years it has featured regular expert contributions – and these articles are read and discussed by SME employees and decision-makers throughout Germany. The core team comprises 50 guest authors from the worlds of business, research and the security sector.

All DsiN initiatives are driven by the association's strong belief that the only way to ensure robust IT security is for all stakeholders to work together. The German government has expressed its intention to help DsiN spread its message to a greater audience. For example, the government is now sponsoring a number of exciting DsiN projects on digital security, including:

- Digitale Nachbarschaft (Digital Neighborhood) supports volunteer work and clubs/associations with funds from the Federal Ministry of the Interior
- DigitalKompass (Digital Compass) organizes get-togethers where older citizens can learn more about the online world, in cooperation with the National Association of German Senior Citizens' Organizations (BAGSO), and with funds from the Federal Ministry of Justice and Consumer Protection
- The Bottom Up project, designed to raise awareness of security issues among vocational school students, is funded by the Federal Ministry for Economic Affairs and Energy

As it celebrates its 10-year anniversary in 2016, DsiN is well placed to expand the scope of its work. This will include the latest developments, such as connected cars, connected healthcare and smart homes – and to gain the support and participation of new organizations. To continue on its successful path, the DsiN annual general meeting appointed Dr. Thomas Kremer, Member of the Board of Management at Deutsche Telekom, as its new chairman.

Following a successful year of active contributions from members, partners and supporters, the buzz around DsiN's 10-year anniversary has grown. The organization remains committed to meeting the growing demand for IT security, and the urgent need for guidance and reliable information – with targeted projects, studies and events that speak directly to consumers and businesses.

We invite you to join the cause.

Dr. Michael Littger

is Director of DsiN. Littger holds a PhD in law and has previously worked for the European Commission in Brussels. Moreover, he was actively involved in the Federation of German Industries (BDI) for a number of years, focusing on the digital economy, telecommunications and media.

PUBLICATION DETAILS

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

www.telekom.com/dataprotection

www.telekom.com/security

Date of publication:
February 2016

LIFE IS FOR SHARING.