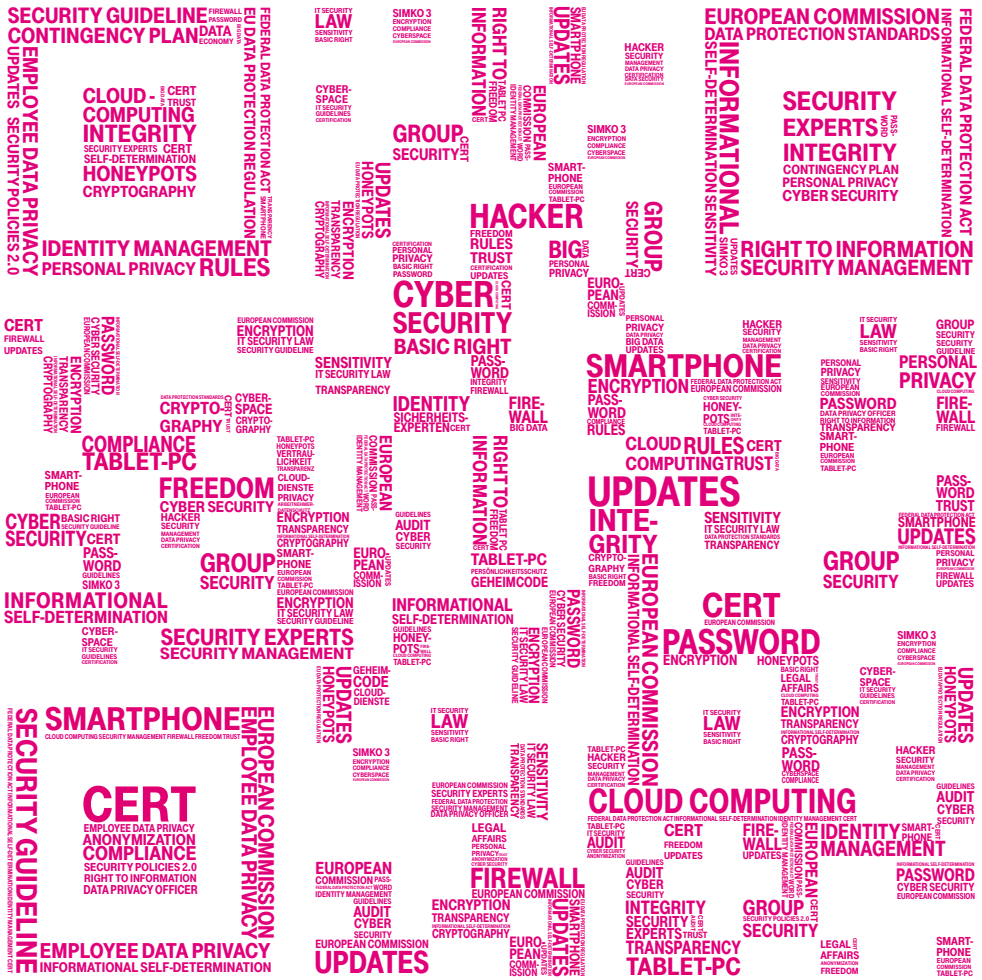


DATA PRIVACY AND DATA SECURITY

Report 2013

LIFE IS FOR SHARING.

CONTENTS

“WE MUST RESTORE CONFIDENCE.”

Politics, business and science must take the crisis of confidence as an occasion for developing new solutions, says Dr. Thomas Kremer, Board member for Data Privacy, Legal Affairs and Compliance.

A wake-up call, a thunderbolt, an earthquake. Some experts may say that Edward Snowden's revelations came as no surprise to them, but the breadth of media coverage on the activities of the NSA and its allies undoubtedly marked a turning point in the debate on data privacy and IT security in Germany. Never before had these topics commanded so much public attention. At the same time public confidence in telecommunications and the Internet declined significantly.

From Telekom's viewpoint the balance between security and freedom is upset when security agencies spy on and store personal data groundlessly en masse. Riding roughshod over rights of privacy is not the way to defend freedom. That is why Telekom took a clear stand on the issue and came in for a great deal of criticism as a consequence. But we were not prepared to make do with mere appeals to politicians to clarify matters. We see protecting our customers' personal data as our mandate.

There are a number of specific measures we can undertake to regain people's confidence. Better encryption of emails and cell phone calls were measures that Telekom implemented immediately. The proposal for an "Internet of short distance" can also be put into practice swiftly and easily. Why must an email from Bonn to Cologne be routed via London or New York?

We are well aware, of course, that traffic routing alone will not solve the security problem. Telekom has for years backed a European general data protection regulation. We need uniform, high data privacy standards with which non-European providers must also comply if they want to offer their services in Europe. The General Data Protection Regulation debate will continue in 2014, and the same applies to data retention. The Federal Constitutional Court and, only recently, the European Court of Justice have each prescribed strict limits for legislation at the German and European level. This reflects the great importance that is attached to personal privacy rights in Europe. The debate on how much freedom should be foregone for the sake of security is by no means over. In the European Union we also ought to dispense entirely with reciprocal spying, and we also need a safe harbor agreement that is worthy of the name. Right now the United States is anything but a safe harbor for European citizens' data, so politicians will not be able to evade responsibility for restoring public confidence.

> "Snowden's revelations were a wake-up call."

And also companies can do more. It is incumbent on us as Deutsche Telekom to develop data privacy and IT security as competitive advantages. To this end we must apply high standards from the outset to the development of new products and services. Further development of European Cloud services is a case in point. An additional issue is how responsibly we deal with the technical possibilities that big data evaluation offers. And the joint fight against cybercrime and industrial espionage continues to head the agenda. How, above all, can we make small and midrange businesses more aware of the threat that cybercrime poses? And what are the specific solutions we offer as protection for business and private customers? The dialog between business, science and politics must be intensified. Telekom will continue to facilitate the sharing of news, information and views and will continue, for instance, to co-sponsor with the Munich Security Conference the Cyber Security Summit.

There is every opportunity to make the scandal the starting point for a positive development. Telekom has certainly gained good experience in the process. Edward Snowden's revelations were definitely a wake-up call, and we must now make sure that we don't fall asleep again.

ABOUT THE AUTHOR

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

"OUR REFORM IS A MARKET OPENER"

The European Parliament's Home Affairs Committee approved on October 21, 2013 by a substantial majority the long-disputed draft for a new General Data Protection Regulation, clearing the way for the first comprehensive amendment to European data protection regulations since 1995.

How satisfied are you with legislative progress so far on the EU's Data Protection Regulation?
Viviane Reding: The European Commission's proposals have been on the table for two years now. When the talks began, some countries stood on the brakes, but since one data scandal after another has come to light in recent months the negotiations have gained momentum. These scandals were a wake-up call. That is why it is good that our data protection reform has been a top-level priority since the EU summit at the end of October. At the summit the EU heads of state and government committed themselves to a "swift" acceptance of EU data protection regulations. I am now counting on the responsible national ministers to decide on a strong common data protection law for the EU before the May 2014 elections to the European Parliament. People are waiting for them to do so.

How do you see the role of data protection in future in the digital world?
Viviane Reding: Data protection is a fundamental precondition for further development of the digital world. Only when citizens, companies and other users feel confident that their data is always effectively protected the digital world, and with it the digital economy, will unfold its full potential.

Personal data is valuable. According to estimates by the Boston Consulting Group the value of EU citizens' data was around EUR 315 million in 2011. By 2020 it is forecast to increase to nearly EUR 1 trillion. Business will only be able to make full use of this potential if users are prepared to entrust companies with their personal data when, for example, they buy products on the Internet.

Shouldn't companies have developed and implemented risk-based approaches to data protection long before now?
Viviane Reding: Companies that handle their customers' data responsibly enjoy a clear competitive advantage. That is why strong, uniform EU data protection regulations are also in the interest of European business.

The scandals of the last half-year are already having an effect. A survey by the Cloud Security Alliance has found that 56 percent of respondents are now hesitant about using Cloud providers based in the United States, and the Information Technology and Innovation Foundation think tank estimates that these revelations will cost the U.S. Cloud computing industry between USD 22 billion and 35 billion in sales revenue over the next three years. That is an enormous opportunity for our European companies.

How have you perceived the role of countries and business in the context of the legislative process to date?
Viviane Reding: At the beginning of the legislative process some member states were not especially helpful, but with the disclosure of a number of undercover activities, mainly by the U.S. and the UK, that has changed. Many politicians have come to understand that citizens have a right to high data protection standards and are demanding this right. It is now up to the governments to act.

For a while business, or parts of business, threw a spanner in the works. U.S. corporations launched a gigantic lobbying campaign that has since run out of arguments. It backfired because the effect of too much lobbying was that the European Parliament made the rules even stricter.

Furthermore, our reform is good for both citizens and business. Why? Because we are reducing bureaucracy and making life easier for companies. Instead of 28 national laws, companies must in future abide by just one Europe-wide law. One continent, one law. That saves around EUR 2.3 billion a year. Our reform is a market opener.

But European data protection offers no protection from a possible lack of observation of data protection rules by non-European companies.
Viviane Reding: Oh but it does. Our reform ensures that non-European companies must also abide by European data protection regulations if they offer products and services to our 500

ABOUT THE AUTHOR

Viviane Reding
Studied humanities at the Sorbonne in Paris. She embarked on her career in 1978 as a journalist with the Luxemburger Wort. A year later she was elected to the Luxembourg Parliament and ten years later to the European Parliament. In 1999 Viviane Reding was appointed a member of the European Commission, where she was first in charge of Education, Culture, Youth, Media and Sport and, from 2004, for the Information Society and the Media. Born in Esch-sur-Alzette, Luxembourg, Reding has been Vice-President of the European Commission and Commissioner for Justice, Fundamental Rights and Citizenship since February 2010.

> **“ OUR REFORM IS GOOD FOR BOTH CITIZENS AND BUSINESS BECAUSE WE ARE REDUCING BUREAUCRACY AND MAKING LIFE EASIER FOR COMPANIES. ”**

million-plus EU citizens. If they breach the exacting European data protection standards they risk fines of up to two percent of their global annual sales revenue. We are thereby creating a level playing field for European and non-European enterprises.

Is the EU's Data Protection Regulation a blueprint for international collaboration beyond the European Union?
Viviane Reding: Strong, uniform data rules will enable us to set standards at the global level. That is why it is so important for us to have these regulations soon. If we speak with one voice at the international level we can enforce our high standards. That applies to our relations both with the United States, which are naturally the focus of attention at present, and with other states.

Only a uniform, robust framework will enable us, for instance, to counter the NSA and call on the U.S. to make urgently required legislative changes that, for example, give European citizens the right to take legal action in the United States against abuse of their personal data. Conversely, U.S. citizens can already do that in the EU, as can everybody else who lives here.

The Regulation is an important building block to help protect European citizens from arbitrary surveillance and espionage by third-party states. What other measures ought to be undertaken?
Viviane Reding: It is important for us to distinguish between rules for the work of intelligence services and rules to uphold data protection. Nobody needs to be surprised that secret services act in secret. But if a secret service operates in the territory of a member state the governments in question should ensure that national regulations are observed.

There are things that cannot be justified by the war on terror. States have no unrestricted right to practice undercover surveillance. What we need is to strike the right balance between combating terrorism and protecting personal data. Security and freedom are two sides of one medal. It is a matter of proportionality.

As for the rules to ensure data protection, our Regulation will ensure that foreign secret services can no longer simply require companies to disclose data or indeed to tap it without their knowledge. We ensure that by requiring all companies that do business in Europe to abide by European regulations. We also ensure legal certainty in data traffic. EU citizens' data may only be passed on to law enforcement authorities outside of Europe in clearly defined exceptional circumstances. There must be effective legal protection from unrestricted international data transmission.

Of Safe Harbor it is known that regulations are not implemented consistently and that there are no sanctions against infringements. What does the Commission propose to do about that?
Viviane Reding: On data protection we are no longer prepared to rely on self-regulation and codes of behavior that are not strictly controlled. In view of what has come to light in recent months the Commission has taken a close look at Safe Harbor. We have concluded that data of European citizens transmitted by U.S. corporations to the United States under the terms of Safe Harbor is indeed not always safe from abuse. It is not uncommon for U.S. agencies to access this data and use it in ways not always consistent with Safe Harbor principles.

At the end of November we made 13 recommendations to the United States to make the 'Safe Harbor' safer. The ball is now in the U.S. court.

TRIAD OF FREEDOM, SECURITY AND BUSINESS

By **Dr. Klaus Kinkel**
Former German Federal Foreign Minister and President of the Deutsche Telekom Foundation

ABOUT THE AUTHOR

Dr. Klaus Kinkel

After studying law at the universities of Tübingen, Bonn and Cologne, and receiving his doctorate, Dr. Klaus Kinkel embarked on a civil service career at the Federal Ministry of the Interior in 1965, transferring to the Foreign Office in 1974. He was in charge first of the management staff and then of the planning staff. From 1979 to 1982 he was President of Germany's Foreign Intelligence Agency, the Bundesnachrichtendienst, then Undersecretary at the Federal Ministry of Justice and from 1990 to 1992 Federal Minister of Justice. From May 1992 to October 1998 Dr. Kinkel was Federal Minister of Foreign Affairs, and from 1993 to 1998 also Vice-Chancellor of the Federal Republic of Germany.

Digitilization of society offers us unique opportunities. International collaboration achieves a new dimension by means of globalized communication in real time. New forms of economic cooperation and development and of political and private exchange are possible. New risks are the downside of the digital revolution. Industrial espionage is a low-risk, high-profit option. Neither individual citizens nor governments are safe from espionage and surveillance. Increasing networking makes critical infrastructures more vulnerable to cyberattacks, be they by civilian or military hackers.

International politics and the business community urgently need to take up the challenge of cybersecurity. That is why one of the most important tasks for cyber foreign policy is to ensure global preconditions for a secure and stable cyberspace. The crucial task primarily consists of applying existing rules to the digital world and setting new rules where they are required.

UTILIZE IMMENSE POTENTIALS, REDUCE RISKS

As with every innovation it is important to undertake a level-headed analysis of the opportunities and risks. On the basis of the findings of this analysis, German foreign policy for cyberspace must contribute toward utilizing and increasing its immense potentials while at the same time reducing its significant risks. Specifically, there is a triad of interests that requires a fair balance. Cyber foreign policy must responsibly protect and make use of the freedom and the freedom-promoting effects of the Internet. It must extend the economic opportunities that it presents. And it must protect the security of cyberspace insofar as it is able to do so.

When it comes to the economic dimension, German cyber foreign policy faces a twofold challenge. It must keep an eye on the opportunities that the Internet and new information and communication technologies present for German businesses. It must also bear in mind their use as a driving force of global development. By advocating fair and open competitive conditions, by pursuing an open visa policy, by taking part in international research programs and by promoting foreign trade, it can contribute toward the success of Germany's IT industry.

SURVEILLANCE AND CONTROL TECHNOLOGIES CAN POSE A THREAT TO FREEDOM

States should not respond to the threat of a cyberattack by pursuing an offensive cybersecurity policy. Those who seek to establish security in cyberspace by means of deterrence and retaliation may well find themselves barking up the wrong tree. Furthermore, a constant search for attackers can easily lead to the blanket use of surveillance and control technologies on the Internet and thus pose a threat to its freedom.

In contrast, a defensive cybersecurity strategy as pursued by the German federal government and the EU aims to avoid conflict and promote stability. It has two mainstays: one is the use of high-security IT to enhance the resilience of our networks to such an extent that they can withstand technologically sophisticated attacks. For another, the federal government initiates and supports international agreements that contribute toward the creation of a regulated cyberspace by establishing a system of "preventive arms control". They include agreements on confidence and security building measures, agreements on international hard- and software approval standards, standards of responsible government behavior and agreement on the application of the rules of international law to cyberspace.

THE STATE, BUSINESSES AND CIVIL SOCIETY MUST WORK TOGETHER

When we consider the triad of freedom, security and business in cyber foreign policy, we need to network and link both these areas of politics and the players involved. The state, businesses, and civil society must work together to combine national and international measures. That is the only way we can protect Germany from the negative effects of cyberattacks while aiming for a free, open, stable and secure Internet.

Edward Snowden's revelations have brought the issue of data protection, privacy, and security of information to the forefront of the debate on cyber foreign policy. It is a matter of trust that the closest of partners must have in each other and that we must not betray. It is also a matter of handling new technologies responsibly. Not everything that is technically possible for a government is ethically right or politically wise. In cyber foreign policy we also need reliable principles that reconcile values and interests.

Despite the rapidly changing environment, we have to bear in mind that too stringent nation-state control of the Internet in response to NSA activities would not constitute progress. Fragmentation of the Internet weakens its economic dynamism and plays into the hands of authoritarian regimes for which the open nature of the Internet is in any case a thorn in the flesh. We must nevertheless also think in terms of an Internet of short distances. Local data streams need not make global detours.

MAKE "IT SECURITY MADE IN GERMANY" AN INTERNATIONAL BRAND

That is why, from my viewpoint, the following measures must have priority:

First, we must have modern agreements on data protection that are in tune with the age of digitilization. Germany is currently advocating these intensively both in the EU and at the United Nations.

Second, we must hold intensive discussions with our European partners. We need an ambitious IT strategy at the European level that makes Europe independent of Chinese and U.S. providers especially of data storage and data processing technologies, and enables us to become competitive in the world market.

Third, we must enter into negotiations with the United States. They must involve reciprocal undertakings by the U.S. and the EU to dispense with political and industrial espionage against each other and to end the mass collection of data about European citizens.

Fourth, we must extend our talks on Internet governance to new agenda-setting powers such as India or Brazil. This means that we must overcome one-sided dominance by certain states or societies.

Fifth, politics and business must come to a close understanding on security technology. "IT Security Made in Germany" can and should become a brand with an international appeal.

BACK TO THE PURPOSES OF PRIVACY

U.S. privacy campaigner **Martin Abrams** aims for accountability-based information governance. Once data processing organizations are fully answerable, Abrams sees data protection as being effective at facilitating information-driven innovation while protecting individuals' rights to dignity and not being harmed. It might then also be possible to establish interoperability between the U.S. and Europe.

Martin, you are familiar with the approach to privacy on both sides of the Atlantic. Many Europeans suggest that the way Americans look at the use of data is highly different from the way that Europeans do. Do you think so, too?

Martin Abrams: From my perspective there are some fundamental differences but important commonalities, too. The biggest difference is in the way we think of the balance between privacy and free expression. In the United States free expression is guaranteed by the first amendment to the constitution. The founders of this country were saying that the guaranteeing of free expression was a preeminent protection that must be put in front of other protections. So, it is incredibly strong. And free expression includes a number of components. The first is the ability to observe. Thus, the ability to observe behavior and to record that behavior is constitutionally protected in most cases.

The U.S. Constitution guarantees the right to freedom of expression, starting with the right to observe and record behavior.

Are there limits to the ability to observe and record behavior?

Martin Abrams: If you are in a public commons I am free to observe. That public commons includes the front lawn of your house or even the backyard when I fly overhead looking. On the other hand I cannot stick my head in the window of your house uninvited. That comes down to the question of what is the public commons in which you are able to observe. The court system in the United States has limited reasonable expectation of privacy when data is shared with a third party, and is therefore no longer subject to privacy protection. Despite this tradition there are more and more people in the U.S. who are discussing the need to narrow the commons in the digital space. You begin to see the movement towards that in initiatives like Do Not Track, where it's been suggested that the ability of organizations to track online should be more limited.

In Europe, organizations need a legal basis to process if they are going to take observations and to make them digital. Do you see this obligation as the most fundamental difference between the regions?

Martin Abrams: Particularly in the age of big data this difference becomes incredibly material. Still it is not at all the only fundamental difference. We have to look at the exploration of data as well. In the U.S. I am free to explore the data. The processing of recorded data to gain insights

ABOUT THE AUTHOR

Martin Abrams
is Executive Director and Chief Strategist at Information Accountability Foundation. He was formerly President of the Center for Information Policy Leadership and Vice President Information Policy at Experian.

INFORMATION ACCOUNTABILITY FOUNDATION

In 2012 a number of companies from the global accountability project founded the Information Accountability Foundation to focus on institutionalizing accountability in business practices, regulatory oversight and the next generation of privacy law. The Foundation's stated mission is to further accountability based information governance through active consultations and research, in collaboration with governments, enforcement agencies, business and civil society.
More information: **http://informationaccountability.org/**

is also guaranteed by the first amendment to the constitution: both thinking and manipulating data is covered by free expression. This is in full contrast to the situation in Europe. If Europeans want to use data to get new insights they need to determine that the data is compatible for a research purpose. Furthermore, they need to determine whether they have a legal basis before they can actually conduct the research.

So far the situation appears to be very much divided. But you've already mentioned important commonalities, too. Where do they come in?
Martin Abrams: It's the acting on the data where you come up with the similarities between the European and the American system. In the U.S. I can't use the data for something that is precluded or inconsistent with my purpose specification notice. I will give you an example. If I process observation data and find that women between the age of 25 and 35 bring greater credit risk I am not allowed to use that knowledge. The law in the U.S. says you can't make a decision based either on gender or age. Even though I have that insight, I cannot apply it. So the fact is, when we actually go to the use of data we begin to have common interests between Europe and the U.S.

Without Safe Harbor much of the data traffic between Europe and the United States would take place in a legal vacuum.

What role does Safe Harbor play in this context?
Martin Abrams: While not perfect, the program has provided real protection to millions of Europeans. Safe Harbor is a self-certification program but one with teeth. A corporate officer must personally certify to the program's integrity and may be prosecuted under the False Statements Act if the Safe Harbor documents are not a reflection of policies and programs to put those policies into effect. Without Safe Harbor much of the data from Europe to the U.S. would flow without any governance at all. So when one looks at the weaknesses, one also needs to focus on the fact that Safe Harbor has been an effective data protection tool.

Is there a way to overcome its weaknesses?
Martin Abrams: The European Commission makes some good suggestions for improvements. For example, more spot-checking by the U.S. Department of Commerce when reviewing self-certifications by companies requesting Safe Harbor listing and more testing by both the U.S. Federal Trade Commission and data protection authorities in Europe. This is an excellent suggestion but would require revenues to offset the costs. Currently the fees for Safe Harbor filing and renewal are fairly small, and, from my perspective, there should be moderately increased fees to pay for effective oversight.

In your blog you describe Safe Harbor as an early example of shaping a data protection means according to the principles of accountability. Why do you think so?
Martin Abrams: Safe Harbor was one of the first privacy governance programs that link to the essential elements of accountability, even though the program predates the publication of those elements by nine years. Safe Harbor requires an organization to (1) have a set of internal policies that link to the Safe Harbor principles, (2) publicly acknowledge that it will comply with those principles, (3) have mechanisms to put the policies in place, (4) monitor internal compliance, (5) assure consumers are able to exercise their rights, (6) have an accountable corporate officer and (7) be answerable to one or more regulatory bodies. All these requirements correspond to the essential elements of accountability we strongly advise every player in the big data galaxy to incorporate.

Why is it so important to follow the principles of accountability?
Martin Abrams: Today too many privacy programs are about completing bureaucratic tasks, such as writing purpose specification notices or managing preferences. I believe we have seen a similar trend at many enforcement agencies that have found it easier to measure technical compliance rather than compliance with the true purpose of data protection. So we return to the purposes of privacy protection. They are about dignity and prevention of harms that are constantly evolving. Our digital age requires data protection based on responsible organizations answerable to us, either individually or through enforcement agencies. Accountability is where organizations take ownership for the management of the information they collect and use, and understand and mitigate the risks they create for individuals. Furthermore, accountable organizations stand ready to demonstrate their data stewardship to privacy enforcement agencies. Accountability is the mechanism for organizations to become big data practitioners using data to be innovative while still protecting individuals.

REFLECT ON OUR VALUES

The increase in cybercrime and massive surveillance by intelligence services have unsettled the general public and companies. Yet, no matter how justified fears of the risks may be, we must not lose sight of the opportunities that the digital world provides, says Wolfgang Kopf, Senior Vice President Group Public and Regulatory Affairs at Deutsche Telekom.

Digital society's vulnerability has been plain to see since 2013, at the latest. It is not just the threats posed by cybercriminals that have increased enormously. The secret service activities revealed by Edward Snowden have brought to light a previously unthinkable dimension of spying on individuals, businesses, and politicians.

The erosion of confidence in the digital society, its products and services weighs heavily. We must ask ourselves whether we are doing enough to deal with the threats. Against this background, transparency and information, a reliable legal framework and the development of new and simple security solutions are preconditions for regaining people's confidence. We must formulate answers about how we can defend ourselves against cybercrime and surveillance. Only informed users of digital services and products can respond appropriately and protect themselves.

SECURITY MADE IN GERMANY

The threat outlined also represents an opportunity for Germany and for the entire European Union. Data protection and data security are developing into an important differentiator, competitive advantage, and additional sales argument for companies.

Germany is very well positioned in this respect. Our high data protection and data security standards are developing – to the surprise of many – into a genuine locational factor. In the past, this view was not shared by everyone. Many have perceived data protection and security authorities more as naysayers, which restrain companies in our globalized world.

Developments in recent months have been quite encouraging. A large number of initiatives in politics and business are looking into how we can protect ourselves better from the risks and at the same time extend the locational advantages of our data protection and data security competencies. Indeed, we ought to make use of the opportunity and develop "Security Made in Germany" into a brand. German companies used to have difficulties in marketing their security products and services, but interest has now increased sharply, especially among foreign companies that have great confidence in Germany as a location.

EUROPEAN DATA PROTECTION

Deutsche Telekom is developing solutions that provide enhanced protection from unauthorized access to our data. However, at the same time we need statutory provisions to increase protection for European citizens. In this connection we have, for example, made a proposal for "Schengen routing", i.e. keeping routing distances short on the Internet. If the sender and the recipient are both within the Schengen area, there should be a statutory requirement that data should not be routed unnecessarily via America or Asia. This is common practice in America. And protecting data that does not need to leave our own legal environment, would already be an improvement in security.

Security Made in Germany could develop into a quality brand.

The very first discussions on no-spy agreements, cooperation in cybersecurity policy or in cross-border data protection have shown how difficult it presently is to arrive at solutions that are internationally acceptable. The aims of allegedly absolute protection through surveillance on the one hand and the right to privacy and informational self-determination on the other hand seem to be too diverse and irreconcilable.

REVOKE SAFE HARBOR

Europe has a different understanding when it comes to balancing the freedom and security of its citizens. At the same time, Europe already has the world's highest level of data protection. Many of these regulations originated in Germany. If they are to protect its citizens effectively, these regulations must be implemented consistently. Several studies by the EU Commission have shown that the Safe Harbor Agreement with the United States provides European citizens with no effective protection. The logical consequence: Safe Harbor should therefore be revoked immediately.

This may temporarily lead to tensions, but it is the only way to create a new transatlantic order for cyber security and data protection. It is the only way in which Europe can succeed in negotiating on par and thereby protecting its citizens' interests.

ABOUT THE AUTHOR

Wolfgang Kopf, LL.M., leads Deutsche Telekom's Public and Regulatory Affairs department since 2006. He is responsible for the political representation, competition law, frequency and media policy and regulatory issues. Wolfgang Kopf studied law and the humanities at the University of Mainz, the Administrative University Speyer and the University of London.

DATA PROTECTION BASED ON THE NEED-TO-KNOW PRINCIPLE

At Deutsche Telekom data protection tops the agenda. That is why the Group is one of the few Dax-listed German companies to have set up a separate Management Board responsibility for Data Privacy, Legal Affairs and Compliance. How does Telekom handle customer data? An overview of the most important aspects.

Which customer data are stored and processed by Deutsche Telekom and for which purpose?
With voice telephony, contract and traffic data are stored and processed. The purpose of the contract data is to form a basis for contractual relationships and maintain the customer relationship. These include, e.g., data such as the name, address and information about used products, services and customer rates. Using traffic data, telecommunication connections are established and controlled. They are processed to generate invoices and stored as a performance record. Upon request, an itemized bill can be generated for the customer from this. Details about the collection and processing of customer data by Deutsche Telekom can be found in the relevant data protection regulations for the products that you have selected.

Who must be able to access the stored data?
For customer care Customer Service and technical staff need to access the stored data when necessary for processing. Customer Services must access customer data in order to process customer enquiries about invoices, for example. Technical staff needs access to the traffic data to rectify faults, for example. For other access the customer's explicit consent or specific legal permission is required.

Can the customer obtain information about his/her stored data?
Each affected party can request information pursuant to Paragraph 34 of the Federal Data Protection Act, regarding which data about him/her are stored by Deutsche Telekom. However, only the affected party personally has this right to request information, not his/her spouse, for example.

Does Deutsche Telekom retain connection data?
Since the decision by the Federal Constitutional Court dated March 2, 2010 Deutsche Telekom no longer retains connection data. We immediately deleted all connection data retained until that time and deemed as void on the basis of the legal regulations declared by the Federal Constitutional Court.

What does Deutsche Telekom do in order to protect customer data in the best way possible?
Deutsche Telekom has put in place comprehensive internal regulations and measures in order to protect customer data in the best way possible. Detailed concepts are being prepared for the systems that process data, which document the data protection, rights and data security. A requirement for starting up a system is the confirmation of compliance with data protection and data security regulations. Only when the required concepts are available and approved, can customer data be dealt with within the context of the relevant defined specifications. In general, a strict "need-to-know" principle applies to dealing with customer data.

Which protective mechanisms exist for the legally prescribed contact points for investigating authorities?
At Deutsche Telekom so-called "regional offices for special government regulations" are available as contacts for the investigating authorities. Employees work here who are specifically qualified and well-trained in data protection matters. Their actions are recorded and documented and monitored by the Federal Network Agency regarding compliance with legal regulations and fulfillment of the legal requirements.

Who checks the security of customer data and compliance with the regulations?
Clear requirements are defined by the legislator for the use and processing of customer data, through the telecommunication and data protection acts. The responsible regulatory agencies, i.e. the Federal Commissioner for Data Security and Freedom of Information, the responsible local government agencies and the Federal Network Agency, regularly review compliance with the data protection requirements. Specific systems, such as prevention of misuse, have been presented to the data protection authorities. Furthermore, the IT security precautions are regularly certified with internal audits as well as by external auditors. In addition to that, Deutsche Telekom carries out a Group-wide uniform data protection audit for its employees each year. It contains questions on the implementation of human resource, technical and organizational data protection.

110 AND 112 – RADIO CELL TRANSMISSION FOR MOBILE EMERGENCY CALLS

Since December 2012 the German police and fire services have been supplied with radio cell data of cell phones used for emergency calls. This information is relayed automatically. The required technical procedure was developed under the aegis of Deutsche Telekom and implement-ed successfully on all German mobile networks.

The fire service or police will come and help me - on this I can rely. In practice, however, the control centers must know where to send the rescue services, and not every emergency caller knows exactly where he is or, indeed, is still able to speak.

To ensure that there is no delay in clarifying the location, all mobile network operators in Germany are required to provide the emergency services automatically with emergency callers' radio cell data.

When emergency calls are made by cell phone, Deutsche Telekom is required to supply the location data of the radio cell.

This statutory requirement is based on Section 108 of the Telecommunications Act as specified in the Emergency Call Regulations.

To implement the Regulations in practice, the Federal Network Agency issued technical guidelines in June 2011. All mobile network operators active in Germany took part in drafting them. In close coordination with Deutsche Telekom, E-Plus, Telefónica and Vodafone, the Federal Network Agency laid down in detail how an emergency call was to be relayed from a mobile network to the fixed line connections of the fire service and the police. As each network operator designates its radio cells in a specific way, they had to find a solution that converted the four formats into one uniform emergency services format. Deutsche Telekom provides this service.

In practice, emergency calls received by the mobile networks are relayed to Telekom, which processes their radio cell ID for the control center, then converts them for the landline network and finally relays them via its fixed-line network to the police and the emergency services. Emergency calls from its own mobile network automatically include data that enable the radio cell's coverage area to be identified. In all other cases the control centers use the radio cell IDs provided to identify the coverage areas in the online databases of E-Plus, Telefónica and Vodafone.

OBLIGATION TOWARD FOREIGN SECURITY SERVICES

Should foreign security services require data from Germany, clear rules govern the procedure. They must request legal assistance from a German authority that will first check whether an administrative order is permissible under German law with particular reference to the existence of a legal basis. The German authority will then submit the request to Deutsche Telekom. If the legal requirements have been met, Telekom will provide the German authority with the data requested in accordance with its legal obligation.

DATA RETRIEVAL AND TELECOMMUNICATIONS SURVEILLANCE: OBLIGATION TOWARD DOMESTIC SECURITY AUTHORITIES

As there is currently no legal provision for data retention in Germany, Deutsche Telekom does not store traffic data for data requests by the authorities. In principle, however, German security agencies may request access to traffic data that the company needs and retains for its business processes. A court order is required to gain this access. In an emergency the public prosecutor may authorize access, but a court must subsequently confirm it. Information about customer inventory data is supplied to authorized agencies, where the legal requirements have been fulfilled, either automatically by the Federal Network Agency or on request by the telecommunications company in question.

Telecommunications surveillance measures, meaning the release of telecommunication content to an authorized agency, may be undertaken in connection with criminal prosecution or to avert danger subject, as a rule, to a court order. Telecommunications surveillance by German intelligence agencies is subject to special legal restrictions. By the terms of the Article 10 Act they are authorized, subject to strictly limited conditions, to apply for permit to undertake surveillance measures. By law the Bundesnachrichtendienst can monitor up to 20 percent of the data, but this entitlement only applies to international traffic. Specific "strategic telecommunications surveillance" measures are ordered and monitored by the so-called G 10 Commission. There is also a parliamentary control committee that supervises the intelligence services.

CORPORATE PRIVACY RULES: UNIFORM & WORLDWIDE

Telekom has drawn up new binding data protection guidelines for all of the Group's subsidiaries around the world. With its Binding Corporate Rules Privacy (BCRP) Telekom offers its customers and employees worldwide the same high level of data protection, worldwide.

Telekom's Binding Corporate Rules Privacy ensure an equally high level of data protection around the world.

The BCRP is a further development of the Privacy Code of Conduct (PCoC), which is already in force for many Telekom affiliate companies. It replaces the PCoC, taking the latest legislative changes into account, and applies to all Deutsche Telekom Group subsidiaries throughout the world. Telekom developed these guidelines to conform to the Federal Data Protection Act as well as European and international data protection guidelines. In some respects Telekom even goes beyond the statutory minimum standards.

Every affiliate signs up to the guidelines, which in Germany are known as Group Privacy Guidelines and, otherwise identical in content, are known elsewhere as Binding Corporate Rules Privacy (BCRP). By signing up to them each company undertakes, irrespective of the data protection regulations in force in its respective country, to observe the same high standards in collecting, storing and processing personal data. Where stricter data protection regulations exist than the BCRP, the statutory requirement takes precedence. Conversely, in countries such as in Brazil, which has no Data Protection Act, the BCRP applies in full.

Telekom has discussed and agreed its Group guidelines with the Federal Commissioner for Data Protection and Freedom of Information. It then sent them to international regulatory authorities. As soon as Austria and Poland approve the draft, the Telekom Management Board will adopt it and decide on its international rollout, to be completed by the end of 2014.

NEW GOVERNANCE MODEL FOR ALL COUNTRIES

Telekom's international governance model defines the areas of responsibility of data privacy officers and management boards of Telekom companies around the world.

Telekom's data protection specialists have developed an international governance model that is based on the Group's Privacy guidelines.

The model provides a binding definition of the profile that a country's data privacy officer must have and the tasks that he or she must perform. The governance model is also aimed directly at country companies' management boards and specifies their responsibilities.

With this model, Telekom ensures that every data privacy officer of a Telekom company enjoys the support required to enable him or her to fulfill the demanding requirements in handling personal data – even if statutory data protection in the country in question is less stringent than in Germany.

The Group undertakes an annual review of data protection guidelines as a part of its International Basic Privacy Audit. The country company's data privacy officer first fills out a questionnaire to provide the auditors at Telekom's headquarters with an overview of the situation at his or her company.

Telekom's international governance model is based on its Binding Corporate Rules Privacy.

At the same time some 30 percent of employees participate in an online survey. The results serve as the basis for further on-site audits. Experts from Telekom's headquarters review both physical precautions and the local data privacy officer's situation.

A COMMON APPROACH

Telekom's international sites and locations provide a high level of data protection, as regular on-site audits by the Group's Privacy division demonstrate.

Deutsche Telekom is present in around 50 countries. In these countries the Group's Privacy division comes across an abundance of views on what must be observed when dealing with personal data. These differences are both legal and cultural in nature. To achieve a uniform global standard of data protection Telekom implemented group-wide guidelines back in 2004 and has developed them continuously ever since. This regulatory framework, known as the Privacy Code of Conduct (PCoC), is geared primarily to the requirements of European law. Group Privacy carries out continuous on-site audits to check the extent to which overseas subsidiaries and associated companies comply with Telekom's PCoC provisions.

In 2013 the audits focused on South Africa, Malaysia, Russia, Spain, Hungary, Greece and Switzerland, reviewing administration facilities, production sites and data centers, amongst others. The audits' main focus is on the extent to which data protection requirements have been implemented in work processes. Along with numerous technical and organizational measures the auditors check the role of the local data privacy officer. Is he – or she – suitably qualified? Can he prevail with his data protection concerns against management resistance? Does he have sufficient manpower and financial resources at his disposal? If the auditors identify deficits they define measures jointly with the responsible local officers and check them in subsequent audits. In 2013, the auditors conducted 13 international audits and found that group-wide data protection has stabilized at a high level.

CHARTED RISKS

Deutsche Telekom's data protection experts have designed a map, on which they have charted the Group's data protection risks. The risk map helps the experts to identify the sites and systems that display a high auditing demand.

How do the Group's Privacy experts decide which IT systems and subsidiaries to audit in order to check how they handle personal data? In mid-2013, Telekom designed a planning tool that provides more transparency throughout the Group. The aim of this risk map is to formalize the choice of audit locations and to make them comprehensible for all concerned.

The map processes 26 risk factors. Essentially, it indicates how sensitive the processed data is. Sensitivity is measured in terms of the protection class of the data, its relevance for the secrecy of telecommunications and the degree of detail of any personality profiles created. The total number of data records processed is also included in the chart. In addition, the chart considers whether data warehouse systems are in use and how many interfaces to other ICT systems exist.

Another factor is the processing risk arising from the Group's interests in other companies. The cartographers look into the criticality of the business model that these companies pursue and the general level of data protection in the country in question. Anomalies and unresolved issues from previous audits are also considered. The risk map also includes information from current incident reporting. An up-to-date overall data protection risk rating is calculated from all these factors. On the basis of this evaluation the Group's Privacy experts decide which kind of audit they will carry out where.

UPWARD TREND CONTINUES

The basic data protection audit provides detailed information on how much Telekom employees know about data protection and how well they implement this know-how in day-to-day business. In 2013 the performance indicators showed yet another significant improvement.

Do you know how to encrypt e-mail securely? Do you know how to report data protection incidents? The basic data protection audit uses practical questions such as these to determine the extent to which data protection has become part of employees' day-to-day business.

To assess the long-term progress of this knowledge the Group's Privacy experts carry out an annual survey. In 2013, a representative sample of 36,000 employees from 33 Group companies took part. The results show a further improvement of the data protection level across the board. The main performance indicator, into which the auditors compute the many individual audit results, reflects this improvement. While this main performance indicator improved from 9.1 to 9.7 in 2013, the improvement in Telekom's international affiliate was even more significant. The level is now at 7.6, up from 6.5 in 2012.

Employees open their classrooms by a mouse click.

VIRTUAL SCHOOL

Starting this year Telekom employees have access to a web-based data protection training center. The new training tool is accessible around the clock on the Intranet. Users can learn more about all aspects of corporate data protection.

The training center gives employees an overview of the Group's Privacy training portfolio. On three floors they can access the training modules. They begin their course with a simple mouse click. On the first floor, there is the basic training that all Telekom employees are required to take. The second floor houses advanced training that expands on the basic training. The third floor is where specialized training courses on selected data protection issues are held, designed to cater to particular requirements, for example courses for Marketing, Human Resources or Accounts employees. The data protection experts measure the popularity of the courses with statistical tools based on click rates (of course, in an anonymised way).

GREATER PRACTICAL RELEVANCE

Deutsche Telekom relies on web-based basic trainings to make its employees fit for handling personal data. In 2013, the training was updated with an even greater focus on practical relevance.

Across the Group all Telekom employees are required to take a basic course in data and information protection. To ensure that this commitment is more than just a compulsory exercise, the Group's Privacy division has developed an interactive training that keeps the focus on employees' daily work routines and familiarizes them in a practical way with the requirements of data protection. To make its relevance to their work routine even clearer, the online courses were given a makeover in April 2013. Its content has since been designed to solely reflect the employees' perspective. Be it general knowledge about data protection, handling employee and customer data, or reporting incidents, the course designers always consider how the subject affects their colleagues' work. And in order to reach absolutely everybody, attention was paid to improving accessibility.

DATA PROTECTION ON TOUR

In 2013, Group Data Privacy Officer Dr. Claus-Dieter Ulmer visited several Telekom affiliate companies and discussed data protection with their management.

The overall level of data protection at Deutsche Telekom may be high, but the annual audits reveal differences in how data privacy is dealt with. That is why the Group Data Privacy department, as agreed with the Data Privacy Advisory Council, has gone on a tour to brief local managements on unresolved issues jointly with the local data privacy officer and to close the gaps. The aim of the tour is to generate greater attention for data privacy and to establish a uniform understanding on the subject.

For a uniform level of data protection across the Group it is important, Dr. Ulmer says, for the local management to understand that it is responsible for ensuring data privacy in the respective company. In some countries, for example, the budget allocated for data protection was found to be unsufficient. "Local data privacy officers must always have sufficient resources at their disposal to establish and maintain an appropriate level of data protection," he says.

How customer data is handled was also on his agenda. The Group's Privacy guidelines make it clear that only customers who have given their approval may be contacted with advertising. Customers should be able to decide for themselves what is done with their data. In some countries this is seen less critical, which may in part be due to a different understanding of data privacy in that particular culture. To this day there is no word in Chinese for privacy.

"I was met everywhere with open doors, ears and hearts," Dr. Ulmer says. "I was able to convey to my hosts why some international regulations that we specify in Bonn are indispensable for dealing trustingly with the data of our customers and employees and thus also for the good of the Group."

Countries visited in the course of the data protection tour included the Netherlands, China, Poland, Slovakia, the Czech Republic and Denmark.

EXECUTIVE INFORMATION SYSTEM FROZEN

During the migration of an IT system for personnel management it turned out that the system contained employees' personal data instead of anonymized data. The system was stopped immediately and the Works Council was informed.

SAP's Business Warehouse EIS (Executive Information System) generates statistical performance indicators for annual reports and deployment planning using data such as employee numbers, age structure and possible bottlenecks in personnel planning. All that it requires is anonymized data that cannot be traced back to individual employees. During a data protection inspection it transpired, however, that the system had since 2002 nonetheless included personal data of employees in Germany. After the incident came to light, all reports were blocked and the EIS was isolated from all other systems.

In principle, a company may process personal data of its employees as long as it complies with data protection requirements and uses the data for a legitimate purpose, such as payroll accounting. As this data protection clarification had obviously not been undertaken for the EIS, the personal data should have been anonymized – even though only a limited number of employees had access to the personal data in the system.

The Management Board apologized to the company's employees and notified the supervisory authorities, the Data Protection Advisory Council and the Supervisory Board's Audit Committee. Immediately after the error came to light, the Management Board also launched three projects to deal with the incident. An independent, third-party auditing firm is investigating why that personal data was being processed at all.

The auditors are also analyzing which data the software evaluated for which purpose and whether, during the time that EIS had been in use, there had been any anomalies to indicate that non-anonymized data had been processed. The system is also being remodeled in compliance with data protection and codetermination law requirements so that the legitimately required reports can be prepared again. In the third project, a team is investigating all HR systems for compliance with statutory framework requirements.

DATA PROTECTION AT SCHOOL

How children and young people can surf the Net safely and what they should bear in mind when doing so.

Malicious comments about teachers and fellow-students on Facebook. Photos of last weekend's drinking session on Instagram. Hefty bills for downloading expensive apps. Pitfalls of the most varied kinds lie in wait for users in the digital world, and the Internet forgets nothing.

If schools want to warn students about the risks they may encounter on the Internet they can book the services of a Telekom data privacy officer, completely free of charge. Dr. Claus-Dieter Ulmer, Deutsche Telekom's Group Data Privacy Officer, is one of the experts who explain to students what not to do when surfing the Internet and how they can surf safely. This service is available for schools of all kinds. For further information and inquiries please e-mail privacy@telekom.de.

HFGWLU INSTEAD OF MÜLLER

Telekom has developed its own anonymization tool that creates untraceable but clearly assigned pseudonyms from real data.

Deutsche Telekom processes millions of personal data in customer databases. Not to mention telephony and Internet usage connection data. If it introduces new software for, say, customer management or billing, the Group's IT experts must first test its functions using data that is as similar to reality as possible. Data protection law rules out using real data from legacy systems. That is why they originally used fictitious records, which, however, failed to reflect reality adequately.

One alternative is to anonymize real data by replacing real names or addresses. Müller becomes Meier and his address is now Holzgasse 11 and not Burgstrasse 17. But this procedure is very time-consuming. Also, it is not transparent how the security mechanisms of the third party software used for this exercise work. The new anonymization tool changes names into cryptic combinations of letters such as "Hsjxut" or "Pdhiwuhf" and converts telephone numbers into random numerical sequences. Using pseudonymized and then anonymized real data improves the quality of testing – to the benefit of customers and of Telekom – and it complies with statutory data protection provisions. This is because the transition from pseudonym to anonym does not take place until the key that is required for pseu-donymization has been deleted in full. Accessing the original data is then no longer possible.

DATA PRIVACY AND DATA SECURITY IN THE COALITION AGREEMENT

The coalition agreement contains clear statements on the new German federal government's targets of greater data privacy and data security. Telekom endorses these objectives and advocates strengthening the informational self-determination of digital network users.

It is particularly positive that the new government aims to implement the EU's General Data Protection Regulation quickly. On this point the coalition agreement states that "negotiations on the EU's General Data Protection Regulation must proceed swiftly and the Regulation must be approved fast in order to ensure a uniform level of data protection across Europe. We want to maintain the strict German data protection standards, especially in data interchange between citizens and the authorities. Europe needs uniform data protection legislation for business so that all providers who offer their services in Europe are subject to European data protection law."

Deutsche Telekom also welcomes the new federal government's aim of enacting legislation to

regulate the protection of employees' data. Clear provisions in this sector are long overdue. In this regard Telekom already aims to negotiate with its social partner a Group works agreement on the protection of employees' data.

"We will implement the EU directive on access to and use of telecommunications connection data," the coalition agreement between the CDU, the CSU and the SPD also states. "Storage of German telecommunications connection data that can be accessed and used must be undertaken by telcos on servers in Germany. At the EU level we will press for the retention period to be reduced to three months."

If the government passes legislation on data retention during the 18th legislative period, taking into account the pending decision by the European Court of Justice, Telekom will be bound by these statutory requirements. What matters are clear and comprehensible requirements leaving no room for legal uncertainties for telecommunications providers. An issue of particular importance for Telekom is a strict implementation of the court authorization requirement for all data, and especially for IP addresses, as envisioned in the coalition agreement: "Access to stored data may only be permitted for serious criminal offenses, to ward off acute threats to life or limb," and subject to a court authorization.

USER-FRIENDLY DATA PROTECTION NOTICES

Simplicity is one of the aims Telekom has set itself as a Group. It applies to products and solutions – and to data protection notices.

They are too long, too confusing or virtually incomprehensible for anyone other than lawyers. For many consumers, data protection notices often remain a closed book. Yet, in Section 93 the Telecommunications Act specifies that "service providers must inform their participants when the contract is signed about the nature, extent, place, and purpose of the capture and use of personal data in such a way that participants are informed in a generally understandable way about the fundamental processing facts relating to the data".

Telekom's data protection department has devised an icon so that customers can see at a glance when the purchase of a product or the signing of an agreement is of data protection relevance.

That is why Telekom began in 2013 to simplify its data protection notices to make them less confusing and more comprehensible. For one, it rewrote the material in a Q&A format so that readers can now find the required information quickly and without complications. For another, Telekom has simplified the wording considerably, making it much easier to understand. For the order confirmation when ordering a telephone connection the data privacy department has also drawn up an abbreviated version of the data protection notice.

Internal processes have likewise been improved. In the past, different data protection notices have at times been used for the same offers. A new procedure ensures that the data protection notice is always available in a uniform and up-to-date version. Also, the same version is used for private and business customers, and none is used when it is not required, such as when buying an end user device over the counter.

A CURSE OR A BLESSING?

Discussion and speculation about PRISM and Tempora have clouded our view of new Big Data technologies. Does the individual citizen really benefit from the capture and evaluation of enormous amounts of data? Or does business alone benefit at the expense of data protection? **Dr. Claus-Dieter Ulmer**, Group Data Privacy Officer, Deutsche Telekom, and Telekom Board member **Reinhard Clemens**, who as CEO of T-Systems sells Big Data solutions to his business customers, discuss the subject in this interview.

If you carry out Big Data analyses you should let your customers decide whether they want to make their personal data available.

Dr. Ulmer, the opportunities that Big Data offer must fill you with fear and dread. Will you prevent Telekom from dealing in Big Data?
Dr. Claus-Dieter Ulmer: I am not opposed to Big Data entirely. There are many positive application scenarios that deliver benefits not only to companies but also to people. They include, for example, real-time evaluation of traffic data to reduce congestion. But we at Data Privacy are maintaining a close watch on Big Data activities in the Group. We keep an eye on what we do with our customers' data and also on what T-Systems offers business customers by way of Big Data solutions.

Where, from the data protection perspective, are the fundamental problems of Big Data?
Dr. Claus-Dieter Ulmer: If we disregard machine-to-machine communication data, Big Data models in principle consist of processing information that is either personal or can be linked to individuals. That means there must be a legal basis for processing it. It can be either a statutory basis or the consent of the person affected. Stored data can also be anonymized. It is then no longer subject to data protection law, and a legal basis for processing it is no longer required.

Mr Clemens, this interpretation of data protection restricts the scope of Big Data solutions significantly. How often have you been annoyed with the data protection people?
Reinhard Clemens: Never! Our assessment of Big Data is very similar. Without public acceptance, the new technology will not prevail, and for that we need strict data protection. Last year we carried a study on Big Data with the Handelsblatt Institute. The results show that after the secret service affairs people are profoundly sceptical and feel uncertain about what happens to their data. We take that very seriously and check very closely with the data protection people which solutions we put on the market.

But has the damage not long been done with the NSA affair?
Reinhard Clemens: There is a very great loss of confidence among the general public. It is entirely understandable, but we must not forget that the issue is one of illegal access to personal data. That is not Big Data. Big Data is the processing, linkage and evaluation of non-personal data of all kinds, such as evaluating regional weather conditions in relation to shopping behavior. But evaluating the data of and on a specific person from a variety of sources is not even permitted in Germany. However, public opinion has yet to distinguish between the two. That is why our task as a company is to restore confidence in our business, especially in everything that has to do with personal data. Accordingly, Telekom has drawn up its own guidelines for Big Data, the most important point of which is transparency: Consumers must know what happens with their personal data.

Telekom offers Big Data solutions to its customers. What about your own customer data? Anyone who is in charge of marketing must be tempted to evaluate this data.

Dr. Claus-Dieter Ulmer: We are subject to a large degree to the provisions of the Telecommunications Act which are very strict – and rightly so. We may only use location data, in other words traffic data, for contract fulfillment, billing or reasons specified in the Telecommunications Act. The Act makes no specific statutory provision for data evaluation in Big Data models. The legal basis is insufficient for direct marketing or advertising, so it cannot serve as a basis for solutions such as Big Data evaluation. And we adhere to that.

But companies can bypass that by securing their customers' consent.

Dr. Claus-Dieter Ulmer: It is true that Big Data evaluation is permissible with the consent of those affected, but effective consent strictly presupposes that the affected person is informed in a way that he can evaluate the purpose of the data processing and the findings that might be deduced from it. He must be able to weigh up the risks that processing the data might have for him and his personal situation. He should also be aware of what is to be evaluated and how.

Reinhard Clemens: Our study confirms that if customers see a clear benefit they are positive about evaluation. A clear majority is opposed to online shopping providers requiring address, bank account and other personal details merely to make shopping faster. Over half the population accepts, in contrast, the idea of drug companies evaluating submissions to discussion forums in order to identify previously unknown side effects of a drug.

Yet three out of four consumers say companies do not inform their customers adequately whether they store data and what they use it for.

Dr. Claus-Dieter Ulmer: A number of companies are sure to hide away data protection-relevant aspects somewhere in the small print of their contracts and their general terms and conditions. That should not be allowed and that is why we place great importance on informing our customers as plainly and clearly as possible. Having said this, it is also our customers' responsibility to inform themselves about data protection aspects. It is worrying that the vast majority of consumers never or only occasionally reads the terms and conditions when they download an app to their Smartphone – because that is precisely where they can identify the black sheep of data protection and protect themselves from abuse.

Reinhard Clemens: I want to make it quite clear that consumers must know what advantages they can reap from companies using anonymized data to improve products and services. We must also make it clear that a large proportion of Big Data analyses is based not on personal data to which data protection law applies but on anonymized data. Our Big Data guidelines are also intended to provide clear and transparent assistance. We really need informed and responsi-ble handling of data – a culture of consent.

DEUTSCHE TELEKOM'S PRINCIPLES ON BIG DATA

1. Deutsche Telekom is aware of its social responsibility and will adopt the sensitive approach required in the development of big data solutions.
2. Deutsche Telekom is transparent with regard to its plans for biga data and big data solutions, and seeks exchange with supervisory authorities, politics, state and non-state institutions as well as customers and citizens.
3. Deutsche Telekom generally anonymizes all data it uses in big data solutions, making it impossible to draw any conclusions about individual persons. Anonymization takes place at source or as near to the source as possible.
4. Deutsche Telekom is committed to a culture of consent and will only integrate personal information in its big data solutions if this is necessary and if expressly authorized to do so by its owners.
5. Deutsche Telekom will only match anonymized data from various sources in such way that it can never be traced back directly to individual persons.
6. Deutsche Telekom will only evaluate information about groups of people if it can be sure that this step will not lead to results exposing a group to the risk of discrimination.
7. Deutsche Telekom does not disclose customer data to third parties, only the results of its down internal analysis.
8. Deutsche Telekom will provide transparent information on any changes that may be made to these principles.

ABOUT THE AUTHORS

Reinhard Clemens
has been a member of the Deutsche Telekom AG Board of Management and CEO of T-Systems since 2007. As an electrical engineering graduate, he was previously CEO of EDS in Germany and responsible for Sales, Business Operations and Strategy in Central Europe.

Dr. Claus-Dieter Ulmer
has been Group Data Privacy Officer at Deutsche Telekom AG since 2002.
As a law graduate, he was previously in charge of data protection at T-Systems International and practiced law with a focus on employment law.

CLOUD COMPUTING IS A MATTER OF TRUST

IT expert **Peter Franck** is a member of Deutsche Telekom's Advisory Council on Data Privacy. In Cloud computing he sees specific risks for architecture, applications and the groups who use the different offerings.

ABOUT THE AUTHOR

Peter Franck
has been a member of the Chaos Computer Club for around 30 years. His professional focus is on developing electronics, software and processes. He also worked for several years as a technical consultant. For the past ten years he has mainly worked in data rescue.

The portfolio of Cloud services ranges from the infrastructure to the application level. The processing and data storage goes on in the background, invisible to the user. The user sees only the presentation layer, mostly in the form of a web user interface or an app. As a rule, data is processed unencrypted in the Cloud. So there is always a possibility for the operator or provider to gain access: access the user cannot prevent. To assess who exactly might be involved, the location of the data centers and the jurisdiction the operator is subject to matters. This is all the more important when it is a matter of storing or processing personal data. In the end, the choice of a Cloud provider is a matter of trust in the operator and the technology used.

RISKS ON THE OPERATOR'S SIDE

The possibility of unauthorized access at the Cloud's administrative level is a total loss for every Cloud, because all processes and data are compromised in the worst case: This is not just a theoretical risk. There have been successful attacks on vulnerabilities in practically all hypervisors (i.e. the virtualization systems, that serve to administer and isolate virtual systems from each other). Quality Cloud operators, however, make sure to prepare for vulnerabilities of all kinds, in a more sophisticated than most small and midrange enterprises. This is also why outsourcing applications to the Cloud can well lead to an improvement in security.

An interesting development is so-called homomorphic encryption, meaning encryption processes that permit processing of encrypted data without knowing their content. The plain text is never in the Cloud and the keys remain in the user's possession. It will probably be a while before this process is available commercially, however.

The risk of a data loss is limited, but nevertheless real because many Cloud services do not provide mechanisms for a backup or restore of user data outside the Cloud, and every Cloud service relies in principle on the availability of the network and the infrastructure. We experienced a real life example of these risks when the Amazon EC2 went out in April 2011.

TENDENCY TO EXPROPRIATE THE USER

In the private sphere where the Smartphone boom drives Cloud applications, there seems to me to be a trend toward expropriation of the content generated by the user, in addition to what is usually faulty handling of personal data. Apps collect users' data and at times not only use it for purposes for which it was not intended but also fail to return it to the user whose data has been collected, making him dependent on the provider in question. Switching providers – or if the service ceases to operate – can lead to an inevitable total loss of content.

EXPROPRIATION OF DEVICES

Another fashion trend would seem to be the coupling of devices to a Cloud application. In this case you do not only lose the information laboriously collected; the device is suddenly useless, too, although technically it still functions perfectly. So expropriation now already extends to the devices used. That is why open source projects, such as Owncloud, have emerged, making it possible to host Cloud services on your own hardware and under your own control, thereby eliminating reliance on providers.

A sensible application is to save important data to the Cloud because it is protected from natural hazards. That, however, presupposes prior encryption by the user and verifiably good encryption procedures and secret keys that only the user holds. Most Cloud storage services do not fulfill this precondition. You can, however, make do with separate encryption before uploading.

MAXIMUM TRANSPARENCY

Telekom's Business Marketplace bundles different providers' Cloud applications on one portal. Geared in particular to SMBs, software can be used without the need to install it and run it on your own computers. But what about data protection on the Cloud computing portal? Dr. Claus-Dieter Ulmer, Group Data Privacy Officer, Deutsche Telekom, explains how data protection is ensured on the Cloud computing portal.

The Business Marketplace offers quality-tested software from the Cloud.

Small and midrange businesses (SMBs) have been uneasy about the risks of Cloud computing since before Snowden, Prism and Tempora. According to a spring 2013 study undertaken several weeks before the NSA affair, three out of four IT managers who have yet to use Cloud solutions are sceptical and have security misgivings about the Cloud. Yet according to another survey by the Information Technology Observatory (EITO) more than one company in two considers the introduction or further development of Cloud computing to be important or very important. For Germany's high-tech Federal Association for Information Technology, Telecommunications and New Media (BITKOM) Cloud computing even offers benefits in terms of security aspects because very few companies can secure their data anywhere near as well as a specialized Cloud provider.

BOOST CONFIDENCE IN CLOUD COMPUTING

So Cloud providers face the important task of informing users transparently and in detail about data security and data protection. It is striking, however, that in the debate on Cloud computing there is a tendency to roll data security and data protection into one. Even if the two sides of the risk medal interrelate, there is more than meets the eye in data protection for Cloud computing. While data security is very strongly based on security technology, data protection is based on how data is handled and on data protection provisions in the countries of origin of Cloud providers and providers of software as a service. Even within the European Union legislation on this subject varies in its levels of stringency.

An important objective for providers of Cloud computing solutions is to build confidence among users – both corporate and consumers. Yet the terms and conditions of contracts and their statutory basis are often hard to understand for people without legal training. Especially for smaller firms without a legal department, evaluating the data protection aspects of a Cloud offering involves a great deal of effort and expense.

In its Business Marketplace Telekom offers a large number of enterprise applications from the Cloud that are especially designed for SMBs. To offer prospective users of Telekom partners' individual applications maximum transparency on data protection matters, information about data protection is provided alongside the brief outline of the solution. Data protection aspects are described simply and comprehensibly, and marked by special symbols.

GERMAN DATA PROTECTION STANDARDS WHEREVER POSSIBLE

For each application precise details are provided of the country where the provider stores the data and who runs the software. On data storage, for example, Telekom distinguishes between Germany, the European Union and Switzerland as storage locations and sites outside of the European Union and Switzerland. Depending on the offering the software is run at a Telekom data center in Germany and complies with Telekom's strict security standards. Or the provider runs the software itself but uses Telekom's infrastructure to which Telekom standards apply. Finally, the provider may run the software at its own data center. Telekom will then check the security standards applied regularly on the basis of the agreed requirements. In addition, there are different data protection contracts with partners that depend mainly on their corporate location. Providers based in Germany are contractually required to guarantee contract data processing in accordance with Section 11 of the German Data Protection Act (BDSG). If a partner's solution does not process personal data, there is no specific contract on data processing. For some providers standard contract clauses approved by the European Commission apply.

MONITORING RIGHTS FOR CLOUD USERS

Users of individual Cloud software packages in the Business Marketplace also have monitoring rights. In principle, they are entitled to check themselves whether terms and conditions are fulfilled or to entrust third parties with doing so. Only where no personal data is processed, monitoring is not required. With its extensive Business Marketplace data protection and data security information expressed in language that is as plain as possible Telekom demonstrates how to build confidence in Cloud computing by means of transparency. This transparency is a part of its proactive approach to all data protection aspects of the Group's product and service offering.

NEW EDITION OF DATA PROTECTION GUIDE

The Telekom data protection experts have updated their guide to surfing safely on the Internet and issued it in a new edition.

Dangers lurk everywhere in the digital world. Users often fall into traps without knowing. Yet many risks can be managed by means of a few security precautions. The precautions to take are described in the data protection guide "Surfing in the Digital World" that can be downloaded as a pdf file free of charge from www.telekom.com/dataprotection.

The guide explains how to set passwords right so that they cannot be cracked. Unprotected WLAN routers are often gateways for fraudsters. While driving by on the road they scan WLANs to see which ones are not properly protected and then download illegal files from the Net via the wireless connection. That can lead to legal problems, because in Germany owners of WLAN connections are required to password-protect them.

Criminals resort to phishing to try and gain access to passwords or to PIN and TAN data. To do so they send fake e-mail to thousands of recipients or manipulate websites. If online banking users input their account details and password on these websites, the fraudsters may be able to transfer money to unknown account holders or to reroute bank transfers unnoticed. The guide gives advice on how to protect yourself from phishing attacks of this kind.

Smartphones are another security risk. If you want to surf the Net safely on the move, you should update your software regularly and password-protect your Smartphone. Permanently activated Bluetooth and WLAN connections pose a further threat. They provide criminals with an opportunity to hack into the system. If you use your Smartphone for work, you should never store sensitive data on your device.

STATUS REPORT ON DATA PRIVACY

In 2013, Deutsche Telekom implemented a further series of measures to improve data security and data privacy-relevant procedures.

TECHNICAL ERROR

A technical error in a link on the Internet sales portal for business customers came to light when a customer pointed it out. Due to this technical error, customers who signed a new contract, could accidently see the customer details of other business customers. They included companies' bank account details and personal data of the proprietors such as date of birth and identity card number.

This error only occurred in certain circumstances and was limited to customers who downloaded their order confirmation by link and did not use the correct confirmation method that was sent to them simultaneously by e-mail. So there is no way of knowing how many customers were actually affected. As a precaution Deutsche Telekom wrote to all 2,107 customers who might have been affected and also notified the supervisory authorities.

WRONG ACCESS DATA

In connection with a system change Telekom inadvertently e-mailed around 120 business customers the wrong activation link for an administration portal. The platform, which is used to manage Internet domains, was removed briefly from the Internet as a precaution until the error was rectified. Telekom informed the affected customers.

28 users of the new administration portal actually used the wrong activation link. In other cases no use was made of it. The error was noticed in a matter of hours and Telekom temporarily shut down the platform in order to prevent abuse. No damage was done. The error was identified and rectified immediately.

It was triggered by wrongly allocated e-mails, due to a system error. Before the system change Telekom had asked portal users to send in or verify their e-mail address in order to ensure that only authorized users would receive the activation mail. When the e-mail addresses were transferred, a system error led to data being mixed up.

ERROR IN IT MIGRATION

During preparations for the migration of an IT system it appeared that instead of only anonymized data it also included personal data of Telekom employees. The system was called to a halt, the Works Council was notified and the employees were informed on 26 August, 2013.

ORDERS ON PACKAGES

In June 2013, customer order forms were attached to hardware packaging in a Telekom Partner Shop to reserve the packages for customers. This data processing error was rectified without delay and the partners were given renewed training in data privacy.

For more information:
http://www.telekom.com/corporate-responsibility/data-protection/24582

CONTROL IS DESIRED

Supervisory Board member **Dr. Bernhard Walter** the audit committees at Deutsche Telekom and Daimler-Benz. The former Dresdner Bank Management Board Speaker outlines the tasks that the Audit Committee performs and explains why data protection and data security play an especially important role.

Telekom's Audit Committee monitors the effectiveness of in-house control, risk management and audit systems.

Many people associate the work of an Audit Committee with accounting. Why are data protection and data security also on your agenda?
Dr. Bernhard Walter: Monitoring of accounting processes and keeping an eye on the auditing of annual financial statements is without doubt a core area of our work, and because these are high visibility tasks, it is understandable that some people equate the work of the Audit Committee with them. In fact, however, the tasks we perform are much more extensive. In particular, we monitor the effectiveness of in-house control, risk management and audit systems. We check whether Telekom complies with all the relevant regulations and in-house guidelines. And the provisions of data protection and data security play a fundamental role in these compliance checks.

Why is that?
Dr. Bernhard Walter: Data protection and data security are directly associated with Deutsche Telekom's business model. Millions of customers around the world trust us with their data. In many cases we handle highly sensitive content – both for private customers and in the business sector. There is also the data – no less worthy of protection – of our 230,000 employees. To justify the trust that customers and employees place in us, we treat data protection and data security as a part of compliance and of risk management.

What can the Audit Committee do to perform these tasks?
Dr. Bernhard Walter: Data protection and data security are the subject of regular reports to the Audit Committee. We hold quarterly meetings and at an additional meeting we pay special attention to the Group's risk control system and look into whether it pays due regard to the requirements of data protection and data security.

You have been a member of the Supervisory Board since 1999 and in charge of the work of the Audit Committee for five years. So you surely remember the data protection scandal well. What, in your view, has changed since then?
Dr. Bernhard Walter: As the Audit Committee dealt with the subject intensively, I am indeed still very much aware of the incidents. Compared with the situation back then, the status of data protection at the company has improved significantly. Since 2008 there has been a Management Board director in charge of data protection, legal affairs, and compliance, and to implement his strategies and policies, he is equipped with comprehensive information and control rights.

Furthermore, a comprehensive package of measures has been implemented to improve data privacy and en-hance data security. We have also established an external body of experts from research, politics, businesses and society, the Data Privacy Advisory Board, to advise Telekom. It has proven highly effective. We ensure additional transparency by cooperating with the authorities and, not least, by issuing an annual report on data protection and data security.

ABOUT THE AUTHOR

Dr. h. c. Bernhard Walter,
born in 1942, was a Management Board member at Dresdner Bank from 1987, and from 1998 until May 2000 Speaker of the Board. He is a member of the Supervisory Board of several well-known German companies, including Deutsche Telekom AG, and Chairman of the Stiftung Frauenkirche Dresden's Foundation Board.

CRITICAL MONITORS

Deutsche Telekom's Data Privacy Advisory Board advises the Management Board, and promotes the exchange of news and views with leading experts and personalities from politics, teaching, business and NGOs on the latest challenges to data privacy and data security. The scope of the Data Privacy Advisory Board's remit is extensive. It deals with business models and processes on the handling of customers' and employees' data, and with IT security and the appropriateness of measures undertaken. Further issues are the international aspects of data privacy and the implications of new statutory provisions.

Its tasks also include assessing general data privacy and data security measures at Telekom, and drawing up proposals and recommendations on relevant issues for the Management Board and Supervisory Board. The Management Board may also request the Data Privacy Advisory Board to assess processes within the Group that are of data privacy relevance. The Advisory Board can also take up data privacy and data security measures itself, and draw up proposals or recommendations for the Management Board.

In 2013, the Advisory Board on Data Privacy held five meetings. Important issues included the assessment of data privacy and data security aspects of new Cloud applications, and the development of new security products by the Group. The Advisory Board also dealt with mobile payment systems and electronic logbook systems. The Advisory Board further discussed Big Data, and was informed about the findings of the basic data protection audit and the level of data protection achieved in the Group.

CURRENT MEMBERS OF THE ADVISORY BOARD ON DATA PRIVACY ARE:

Wolfgang Bosbach
CDU, member of the Bundestag and Chairman of its Home Affairs Committee

Peter Franck
Management Board member, Chaos Computer Club (CCC)

Professor Dr. Hansjörg Geiger
Honorary Professor of Constitution Law at the University of Frankfurt am Main, State Secretary at the Federal Ministry of Justice from 1998 to 2005, and President of the Federal Office for the Protection of the Constitution and the Federal Intelligence Service (retired)

Professor Peter Gola
Honorary President of the Society for Data Protection and Data Security (GDD), and author/co-author of numerous publications on German data protection law

Bernd H. Harder
Attorney, Management Board member, Federal Association for Information Technology, Telecommunications and New Media (BITKOM e. V.) and lecturer at the University of the Media, Stuttgart and the Technische Universität München (TUM)

Dr. Konstantin von Notz
Bündnis 90/Die Grünen, member of the Bundestag, Deputy Chairman of the parliamentary party, its spokesman on Internet policy, and a member of the Bundestag's Home Affairs Committee

Gisela Piltz
Member of the FDP's Federal Executive Committee and Deputy Chair of the North Rhine-Westphalian Free Democratic Party

Gerold Reichenbach
SPD, member of the Bundestag and its Home Affairs Committee (reporting on data protection, civil protection and disaster relief)

Dr. Gerhard Schäfer
Presiding Judge, Federal Supreme Court (retired)

Lothar Schröder
Chairman of the Data Protection Advisory Board, member of the Federal Executive Committee of the labor union ver.di, Deputy Chairman of the Supervisory Board, Deutsche Telekom AG, and a member of the Commission of Inquiry on the Internet and Digital Society

Halina Wawzyniak
Die Linke, member of the Bundestag, Chair of the Bundestag's Legal Affairs and Consumer Protection Committee

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

EXPERTS DISCUSS DATA PROTECTION AND DATA SECURITY

It was the idea of Klaus Dieter Hommel, Chairman of the Data Protection Advisory Board at Deutsche Bahn, and Lothar Schröder, Chairman of the Data Privacy Advisory Board and Deputy Chairman of the Supervisory Board at Deutsche Telekom. Data privacy and data security representatives of the two companies spent an entire day briefing each other on their work. During the day's discussions in Berlin Gerd Becht, Director Compliance, Data Protection, Legal Affairs and Group Security, Deutsche Bahn AG, and Dr. Thomas Kremer, Director Compliance, Data Privacy and Legal Affairs, Deutsche Telekom, stressed the importance of Data Privacy Advisory Boards. As independent bodies they advise the Management Board on issues of relevance for data privacy. They also make recommendations on sustainable development of data privacy. In the process they provide important impulses for data privacy work at the two companies. Deutsche Bahn presented inter alia management self-auditing solution and discussed video surveillance at railroad stations. Deutsche Telekom provided information about the development of international Cloud computing solutions in conformity with data privacy and data security, and about its annual Transparency Report on data privacy and data security.

WE MUST CARRY ON BUILDING CONFIDENCE

The behavior of the intelligence services has shaken the foundations of democratic society, says Lothar Schröder, Deputy Chairman of Deutsche Telekom's Supervisory Board. It has also put the integrity of telecommunications and the digital media into question.

2013 was a burdensome year for data privacy. The scandal involving interception practices by the American NSA and the British GCHQ raised fundamental questions about the foundations of our democratic society, and, not least, put the integrity of telecommunications and the digital media into question. Big Brother behavior by a number of intelligence agencies runs counter to every endeavor by telecommunication companies to treat the personal data to which they have access as confidential. Credibility will take a massive hit if we have reason to fear that someone is always listening to and spying on what we say and write.

SENDING OUT CLEAR SIGNALS AND FIGHT AGAINST A CLIMATE OF MISTRUST

Are intelligence agencies frustrating our work? The twelve members of Telekom's Data Privacy Advisory Board have for years successfully worked on protecting customers' and employees' data. For them interception of communication data of all kinds that is legitimized by other countries, up to and including surveillance of cell phone calls by political allies, is unacceptable, and on that the Data Privacy Advisory Board and the Management Board of Telekom are agreed.

Interception creates a climate of mistrust against which we must fight with all our means. That is why we must send out clear signals that this is something we are not willing to put up with. That is why the work of the Data Privacy Advisory Board continues to be important – as a powerful indication of how seriously Deutsche Telekom takes personal rights.

René Obermann publicly pointed out the game changing effects of the comprehensive interception of telecommunication data in a remarkable way. This critic was fully in accordance with the position of the Data Privacy Advisory Board.

This merits continued support. We must not treat personal rights like we sometimes treat our own health: Only when it's gone we notice that we miss it.

OWNING UP TO MISTAKES AND ACT CONSISTENTLY ON DATA PRIVACY

Just how important consistent action on data privacy can be for a company was shown in 2013 by a breach of regulations in the processing of employees' data. The Group's independent Group Privacy department identified an error in the central personnel data processing system. The Management Board responded swiftly and decisively. In the past, the company tended to sweep breaches of this kind under the carpet. On this occasion, however, the Management Board made the matter public and apologized to Telekom's employees.

On the initiative of the Management Board and the employees' representatives, and with the support of the Data Privacy Advisory Board a third-party investigation of the incident was commissioned. Its aim is to find out who processed which system data illegally and how to establish how the incident was able to occur and who was responsible for it. Only by means of relentless investigation such incidents can be avoided in the future. The nature of the infringement shows that the importance of data privacy has yet to be fully appreciated across the company although the processes of self-healing seem to be functioning.

Nevertheless, we still need specific legislation in Germany to protect employees' data. This is cause many of the general terms and conditions of data protection do not apply to the protection of employees' data. Simply updating the general data protection legislation to include provisions for the protection of employees' data would be over-complicate the law.

LEGISLATION TO PROTECT EMPLOYEES' DATA IS A MUST

We need clear legislation on protection of employees' data that takes into account the special dependence of employees on employers and offers sanction mechanisms. Companies that fail to handle their employees' data sensitively must be sanctionable. We also need greater co-determination rights for data privacy officers and works council members, and immunity protection for office holders in data privacy and co-determination.

Enabling the communication of confidential personal information is a part of Telekom's core business. If this core element is violated (either by its own actions or by those of others), the company has a problem. Telekom has learnt from past mistakes and earned an advantage over its competitors in terms of credibility. This advantage must be expanded in the years ahead.

ABOUT THE AUTHOR

Lothar Schröder
is Deputy Chairman of Deutsche Telekom AG and Telekom Deutschland GmbH Supervisory Board. Since April 2006 he has headed the Telecommunications, Information Technology and Data Processing division on the Federal Executive Committee of German labor union ver.di. He is also responsible for "Innovation and Good Work" and for the union's Masters', Technicians' and Engineers' division (mti).

“WE NEED HIGH AND UNIFORM GLOBAL DATA PROTECTION STANDARDS”

State-imposed data espionage among partners is unacceptable. On that point **Wolfgang Ischinger**, Chairman of the Munich Security Conference, and **Timotheus Höttges**, Management Board Chairman of Deutsche Telekom, agree. But professional cybercrime poses a greater threat to digital society.

How, in your view as Chairman of the Munich Security Conference, has the subject of cyber security developed in 2013?
Wolfgang Ischinger: We first included the subject on our agenda in Munich in 2011. The first Cyber Security Summit followed in 2012 in Bonn because the subject had rapidly gained momentum. Cyber security is now one of the most important issues in the international security policy debate.

With the NSA affair making a major contribution …
Wolfgang Ischinger: I think everyone now understands how central the issue of cyber and data security is for all of us. The threats increased exponentially even before the NSA affair, but many companies and governments did not yet take them very seriously. In that respect, PRISM and Tempora have even done us a favour. Our awareness of and interest in the risks and opportunities of the digital world have increased significantly, and that is very important.

Timotheus Höttges: … Although I should like to add that we must not mix up two different threat scenarios. After the revelations, there were too many things that were lumped together, in my opinion. What we have learnt about secret service practices cannot be directly compared with the activities of professional cybercriminals. The secret services with their surveillance have made it clear how important data protection is for all of us: be it as private individuals, in business, or in politics. The US agencies’ primary concern is to achieve greater security. Whether the right balance has been struck in relation to the right to privacy, is the subject of the current debate. The cybercriminals are not interested in balance. They want to cause direct damage – with great success, as we know now.

What, then, are the consequences of the over-zealous work of the secret services?
Wolfgang Ischinger: A substantial loss of confidence, serious mistrust of the state and of many companies.

Wolfgang Ischinger, Chairman of the Munich Security Conference.

ABOUT THE AUTHORS

Wolfgang Ischinger
is Allianz SE’s Chief Representative, and took over as chairman of the Munich Conference on Security Policy in May 2008. As a lawyer specialized in international law, he was previously employed by the Foreign Office of the Federal Republic of Germany, serving inter alia as German ambassador in Washington, D.C., and London and, previously, State Secretary at the Foreign Office. He headed the German delegations at the Bosnian peace talks in Dayton and was also representative of the European Union in the troika negotiations on the status of Kosovo.

> **“ THE CYBERCRIMINALS ARE NOT INTERESTED IN BALANCE. THEY WANT TO CAUSE DIRECT DAMAGE. ”**

Timotheus Höttges, Management Board Chairman of Deutsche Telekom.

People wonder who and in what they can still trust in the digital Wild West. The Internet, their own government, business? Everyone seems to be able to do whatever they want, and to be doing it across frontiers and without inhibitions. Regaining the confidence that has been lost is an enormously important task because the digital world also offers magnificent opportunities.

How can this work in a globally connected world when individual countries or companies pursue only their own interests?
Wolfgang Ischinger: There are examples of the international community being able to agree on common rules even on complicated issues. That is clearly not a straightforward process, but we urgently need global, international regulations and confidence-building measures. A transatlantic no-espionage agreement, for example, could have this effect, and a European no-espionage agreement would be an important first step in that direction. This EU standard could then serve as a start-ing point for dialog with Washington and other partners. We could be sure to number among our allies
large US corporations whose business model is based almost entirely on the Internet and whose success is at stake. Due to the NSA a rethinking has begun among consumers, and very well known US companies recently launched a campaign to this effect.

But ratification of the EU's General Data Protection Regulation has taken years already. That really doesn't sound very promising.
Wolfgang Ischinger: The NSA affair will give the General Data Protection Regulation its final impetus. A meaningful transatlantic or global dialog on something like a code of conduct is conceivable only on the basis of a clear stance of the EU.

If the politicians reach an agreement, would that not necessarily have repercussions for business?
Timotheus Höttges: Data protection is not just a topic for politics; it is one

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

for companies, too. Let everyone put their own house in order. Companies also collect data. That is often necessary, yet sometimes dubious. Overall, the business community is responsible for doing more for IT security and data protection, and for closing as many loopholes as possible to prevent abuse.

But repeated corporate data affairs do not exactly contribute to improving confidence in business.
Timotheus Höttges: Many of those so-called affairs are an expression of the new transparency in data security. This transparency is important for companies to be able to react faster and more efficiently to attacks. Telekom has always promoted openness and I am delighted that we have made significant progress here. We face increasingly professional cybercrime with a veritable tsunami heading toward us. Business in general has long been unaware of the dimension of this problem facing us. Another point is, of course, how companies themselves handle customer data. Therefore, there are clear rules in Germany that we must comply with.

What lessons has Deutsche Telekom learnt from this cyber-war conflict situation in 2013?
Timotheus Höttges: We came to clear conclusions after our own data protection issues of more than five years ago. Since then no stone has been left unturned. In this context, we were not only the first German company to appoint a management board member with responsibility for data protection but have also checked all departments, sites or applications for data protection aspects and made adjustments where necessary. Today we are a model for others where data protection is concerned. But we are not, of course, infallible and we, too, constantly have to adapt to new threats from cyberspace.

Do you believe that in the future customers will prefer products from trustworthy companies?
Timotheus Höttges: The risk-awareness of the people is constantly growing. So they will start to furn their back on offers and companies they do not trust. Just as people expect of a car that its brakes work and they can drive safely, they expect us to protect the data they entrust to us and expect to be able to surf the Internet safely. Telekom understood at an early stage the importance of security on the Net and responded with products such as the Cloud Made in Germany. I would like to expand on the competitive advantage that Telekom enjoys in this field.

So do you see the debates on cyber security and data protection as an opportunity for Telekom?
Timotheus Höttges: I see them as an opportunity not only for Telekom, but also for Germany as a business location and for the European economy. We are highly competent on cyber security matters and can establish ourselves as market leaders in cyber security technology. With our high security standards and our understanding of data protection we can position ourselves with high-end security products of our own in competition with US and Chinese hard- and software products. Since summer 2013 Telekom has certainly received an enormous number of inquiries from companies that want to know what we can do for them by way of cyber security. They benefit from the expertise we have built up consistently in recent years.

With all due respect for the outrage about the work of the intelligence services, did what Edward Snowden revealed come as a surprise to you?
Wolfgang Ischinger: I would have never thought that they would go this far and spy on the heads of governments of friends and allies in their own countries. But I did feel that some of the reactions in Germany were slightly naïve. It has always been the case that confidential or even secret information should not be discussed over open telephones or telephone lines. So we should not just blame the United States but consider how to protect ourselves. Why don't we make greater use

Munich Security Conference MSC
Münchner Sicherheitskonferenz

Over the past five decades the Munich Security Conference (MSC) has developed into a central annual gathering of the international strategic community. Since its foundation the MSC has served as an independent forum dedicated to promoting peaceful conflict resolution and international cooperation in dealing with present and future security policy challenges. Its special focus is on transatlantic partnership.

For further information visit
www.securityconference.de/en

of the technical possibilities? Why don't we encrypt our communication more consistently? Why do we still deal with the media so naïvely? There is evidently a great deal of ground to cover and information to take on board.

FOR MORE CYBER SECURITY

On 11 November 2013 the Munich Security Conference and Deutsche Telekom held the second Cyber Security Summit in Bonn, continuing the summit talks between senior business executives and politicians first held in the fall of 2012.

Along with keynote speeches by EU Commissioner Neelie Kroes and German Minister of Justice Sabine Leutheusser-Schnarrenberger, participants were able to follow a high-caliber platform debate on Cyber Security, Data Protection and International Relations. The speakers included former Israeli Prime Minister Ehud Barak, former cyber security advisor to US President Barack Obama, Howard A. Schmidt, Austrian Interior Minister Mag. Johanna Mikl-Leitner and Yves Leterme, Deputy Secretary-General of the OECD.

In 2013, the Cyber Security Summit concentrated on espionage and sabotage, on the regulatory framework at national and international levels, and on specific security solutions. In a final communiqué, the participants listed proposals to set the right course for more security in cyberspace. Public awareness of the threats that face cyberspace must be enhanced, and companies, public authorities and private end users must be made more aware of cyber security risks, their prevention, and the opportunities it offers. Cyber security policy is economic policy, too, given that a high level of data protection and data security is a locational advantage in the globalized world. Digital business models only work if customers can rely on the security of their data.

That is why business has a vital interest of its own in making IT systems as secure as possible by means of technical and procedural measures. Greater security is an important distinguishing feature, competitive advantage and sales argument at the same time. Further development of cyber security competences will pay off because it creates technological sovereignty and contributes toward building a profile as a trustworthy exporter of high-end cyber security products.

Cyberspace needs a binding framework that provides a balance between legitimate security requirements and elementary basic rights, a framework in which the basic concept of freedom on the Net is maintained. Only overarching cooperation promises success. To establish an awareness of the risks a comprehensive picture of the sources, the quality and the quantity of the attacks occuring every day is needed. The state, businesses, and society must constantly re-establish a situation picture of this kind by means of voluntary, international, and cross-industry exchange.

The Third Cyber Security Summit will be held on November 3, 2014 in Bonn.

www.cybersecuritysummit.de/current
Experts from business, politics, science and research discuss crime, economic espionage, and sabotage on the Internet.

THE HARE AND THE TORTOISE

Telekom invests a great deal of energy, input, and manpower in data privacy and data security, but it faces — and is fighting against – a growing number of attackers and malware.

70

employees at Telekom's Data Protection Department put IT systems, processes, and new products to the test on a daily basis.

3

billion virus attacks were registered by Kaspersky customers' computers in 2013.

80

percent of Internet users in Germany felt at the end of November 2013 that their personal data is generally insecure on the Internet.

35

targeted attacks per day are registered by the fully encrypted German government network.

7,222

inquiries sent by customers and employees to datenschutz@telekom.de were answered by Group Privacy in 2013.

250,000

online banking identities were stolen in a mere three months, according to the Federal Office for Information Security (BSI).

70

malware e-mails an hour are sent in the German government network on average, according to the Federal Office for Information Security (BSI).

170

national data protection coordinators ensure at Telekom Group sites in Germany that the same level of data protection is in place everywhere.

800,000

hacker attacks per day were recorded by Telekom honeypots at peak periods.

100

data privacy officers represent the interests of the central Group Data Privacy Officer at Telekom sites in Germany and around the world.

42.5 million

euros of damage were done by cybercriminals in Germany alone in 2012, according to the Bundeskriminalamt.

70

percent of companies plan to invest more in IT security in 2014 to improve their security status.

9

percent of Internet users in Germany used encryption software for their e-mail at the end of 2013, according to the industry association BITKOM.

580

members belonged to the Alliance for Cyber Security in mid-December 2013. Its membership had doubled within six months.

42

national and international audits were conducted by external and internal certified auditors within the Telekom Group.

180

Telekom honeypots attracted hackers in 2013 to enable Telekom experts to gain new insights into cyberattacks.

16,762

times the Abuse Team notified Telekom customers of malware on their computers in a single week in May.

1,446

internal security alerts and action recommendations were issued by Telekom CERT in 2013.

45

percent of companies have no emergency plans for IT security incidents.

301

Telekom employees work solely for the internal data security department.

300

days is how long half of all hacker attacks on companies go unnoticed.

200,000

new malware programs a day are distributed on the Internet by hackers, according to Kaspersky Lab.

A WAKE-UP CALL FOR COMPANIES

Michael Hange, President of the Federal Office for Information Security (BSI), sees the NSA affair as having a positive side effect. Spying and espionage used to be issues that were hard to get across to companies, but the activities of intelligence agencies have given rise to a rethink. Everyone is now aware that hacker attacks can pose a serious threat to business and the state.

Edward Snowden's revelations have taken IT security, previously an issue discussed more at the expert level, to the center of general public interest in just a few weeks. There is a growing readiness to invest more heavily in IT security. Cyber security and protection from digital industrial espionage are now regular topics on management agendas, and so it should be! Both the quantity and quality of cyberattacks increased significantly again in 2013. Around 40,000 new malware variations take shape daily. And those affected seem to know little about it. Half of successful hacker attacks on a privately used PCs go unnoticed for more than 300 days. So it really is high time to tackle the topic intensively and take suitable protective measures.

In spite of the many reports of attempted and sucessfull cyberattacks, we still have no clear idea of where we stand on cybercrime, but we must assume that it poses a massive threat to the economy. That is demonstrated by a simple analysis. A standard operating system or other comparably complex software consists of tens of millions of lines of program code. Experts reckon that about 0.2 per mill of them are either faulty or constitute security loopholes. That would mean that ten million lines of code include 20,000 loopholes for hackers.

LOW RISK OF DISCOVERY

Cybercrime has developed into an international market characterized by a high degree of division of labor where professional hackers offer their services. They build made to order tools that criminal sales organizations put on the market and buyers use illegally. One reason why these services are attractive is that the risk of discovery is very low. Only using the tools is punishable by law. Developers and marketers are permitted to offer their services openly under the eyes of the police on the Internet or at fairs. Furthermore, hacking is a lucrative business. Many targets can be at-tacked simultaneously for a manageable financial outlay. Used en masse, even a low success rate is enough to earn a good living.

In view of these developments it is, however, important not to resort to blind actionism. All that is needed to reduce the risk of a successful hacker attack are a few structured measures starting with prevention, which can be improved significantly beyond the mere use of a firewall and a virus scanner. What counts is not just to make IT security a management matter on a one-time basis but to implement it by means of sustainable processes.

IT security is a permanent management task starting with a concept that defines the firm's "crown jewels" and the methods by which to protect them. The BSI has a wide range of recommendations and offers of assistance, and certifies not only products but also trustworthy IT security service providers. Even more wide-scale use of cryptography could solve many security problems. For many years there have been encryption methods that provide a high level of protection if they are implemented correctly. What has hitherto been lacking is industry demand for them. With appropriate investment IT security by design is worthwhile, as is shown by the German government network to which all Ministries and most federal government agencies are connected. It was set up 20 years ago at great expense and has achieved a very high security standard that is in principle designed to withstand even attacks by intelligence agencies. To this day there have been no indications of successful hacker attacks on it even though up to 3,000 standard attacks a month and four or five targeted attacks on it per day are registered. If the government had decided back then that every Ministry and each government agency had to protect itself on its own, the security situation today would be different.

CROSS-BORDER DIALOG

In Germany, the state also feels obliged to protect the integrity and trustworthiness of using information technology for private users. That is also why we have improved the protection of electronic identities enormously by developing the new electronic identity card. Furthermore, the federal government has established a statutory framework to enable citizens, enter-prises and public authorities to communicate with each other securely online by means of the DE-Mail-Act.

We also want to reactivate the debate on the IT Security Act. A number of business associations expressed misgivings about the requirement to report cyberattacks. Yet what we currently have is a situation in which a high number of attacks take place but only a few get recognized. A successful defense against the growing risk of industrial espionage and hacker attacks can only be built up in the long term, if we have an overview of the current situation on the basis of which protective mechanisms can be developed. Improvement of cyber security is a joint task for the state, businesses, science and research. That is why we must arrive at a cross-border dialog, and that is why a common European data protection regulation is so important to regain the confidence lost.

ABOUT THE AUTHOR

Michael Hange
has been President of the Federal Office for Information Security (BSI) since October 2009. As a math graduate, he was previously employed at the BSI as, inter alia, head of the Consulting and Support Department. Compiling the Basic IT Protection Manual was a main focus of the department's work, helping to develop effective IT security management in administration and business.

CUSTOMERS' DATA IS OUR HIGHEST PRIORITY

For vehicle specialist Carglass security and data protection are of upmost importance. When it outsources data it only does so to a provider in Germany.

When stones damage a car windshield many car owners contact Carglass. The car glass expert seals damage to windshields with a patented special transparent resin. As Carglass operates as a partner for most leading car insurers, customers can assign their entitlement to settlement to Carglass. The glass specialist then settles bills directly with the insurer. "To enable us to deal with the repair," says Frank Müller, Carglass' IT manager, "car insurers entrust their customers' data to us. For us it is thus enormously important to fulfill high security standards and to ensure data privacy. The security of customers' data is our highest priority."

Carglass employs a full-time data privacy officer who checks the contracts with insurers and ensures that customer data is processed in-house in compliance with data protection requirements (either a statutory basis or an opt-in process). IT security is the responsibility of a team of over 20 employees headed by Frank Müller. In order to fulfill his task he regularly keeps himself informed about new technologies and tools. In his opinion that is essential to keep pace with developments in the cyber sector. "Cyberattacks," he says, "change so fast that we must always use the latest security concepts to protect our IT operations."

A THREE-STAGE SECURITY CONCEPT

For IT security Müller relies on a three-stage concept consisting of a next generation firewall, a demilitarized zone (DMZ), and regular penetration tests by professional providers. "Our firewall," the IT manager says, "inspects data traffic to ensure that malware cannot masquerade as another application and find its way into the network. It is a next generation firewall concept that is based on application control rather than on conventional port control." The penetration tests serve to reveal and rectify any security vulnerabilities before a hacker can exploit them. "We do our best to protect ourselves and our customers' data," Müller says. The many attacks on the company's infrastructure that are registered prove that their work is not in vain. Müller says that botnet attacks have especially increased in number. "Attacks," he says, "are increasingly launched by hijacked computers whose owners have no idea of what is happening."

On the physical side two Telekom data centers with a loop connection ensure high system availability. "The loop connection carries our data traffic via separate lines to two different Telekom exchanges," Müller explains. In the unlikely event of an exchange failure the vehicle specialist's systems remain intact. In addition to running its own data centers Carglass uses the private Cloud. It will only consider a German hosting partner that guarantees data will only be stored and processed at German data centers with a redundant backup that is also located in Germany. "Telekom," Müller says, "provides us with a network hosted here in Germany and guarantees that our data will not leave the country."

LEARNING FROM ONE ANOTHER

To keep abreast of the latest developments IT manager Müller attends user meetings and gatherings of IT department spokesmen. "As a Telekom dialog customer," he says, "we are regularly invited by Telekom to attend meetings at which we discuss in committees and working groups how problems can best be solved in the future." He doesn't keep new findings to himself. Carglass is a subsidiary of the global Belron Group which is represented in 36 countries. International Group guidelines define IT security and data protection requirements. The heads of IT at Group companies around the world regularly share best practices in order to support each other and learn from one another. "Once a month," Müller says, "one of us prepares a lecture as a webinar." The other IT managers log in and ask questions about the solution their colleague presents. "It is an extremely important exchange for us because we all face the same challenges."

Carglass heads of IT meet regularly to share news and views on security issues.

RACE AGAINST THE SPAMMERS

99.9 percent of T-Online.de and Telekom e-mail traffic consist of spam. Platform protection and spam filters reject this mail right away. Yet spammers constantly try to circumvent these protective barriers.

Despite effective protection, spam mailers occasionally succeed. Attack and defense is basically a hare and tortoise game. The easiest way to avoid spam is if the recipient's address is unknown. Yet spammers are constantly testing combinations of first names and surnames and pseudonyms, and even addresses that cannot be guessed can find their way into the clutches of a spam mailer if, for example, a virus infects an acquaintance's computer or hackers steal customer data from a company's servers.

FRAUDSTERS EARN COMMISSION

Fraudsters use stolen e-mail addresses to register for competitions and newsletters of blameless and respectable companies, for example. As "affiliates" the fraudsters earn commission for each address. Affiliate marketing is an Internet-based sales solution that involves a provider (usually a commercial provider or merchant) paying its sales partners, or affiliates, by results.

Sadly, a spam filter is unable to distinguish between newsletters that are requested and newsletters that were not requested and are spam. In this way unsolicited advertising at times finds its way into the box of a user who is well protected from spam.

Spam is even more difficult to classify if the features of unsolicited e-mail vary. For an e-mail's "fingerprint" to be classified as spam it must first be known to be spam. The recipient of spam improves his filter by reporting it to his e-mail center as spam, but some spammers vary their mail so skillfully that each variation must first be put through the fingerprint process. The user can then easily gain the impression that he is constantly reporting the same spam mail.

USERS MUST BE HEALTHILY SCEPTICAL

Spam filters also have difficulties with mail when the sender uses a few random characters for the e-mail subject and the body of the mail. The filter classifies the mail as clean because it contains too little content. Spammers send e-mail of this kind to validate addresses. If a seemingly defective e-mail is delivered, the sender receives the information that the recipient's e-mail address exists.

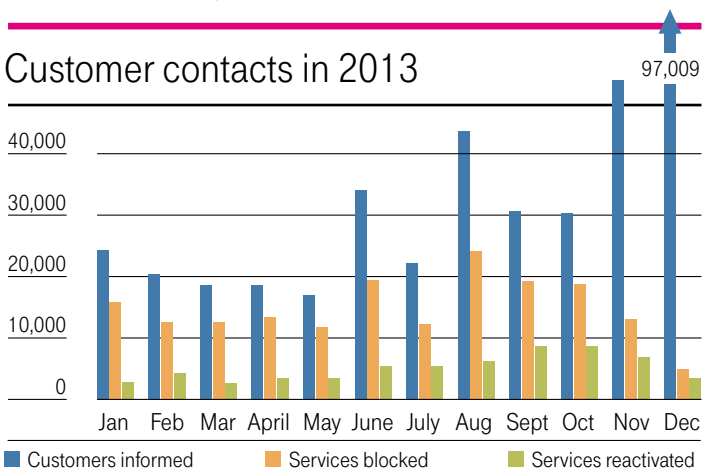
Spammers sell these addresses in what might be termed the criminal underground. The buyers want to be sure that they are paying for genuine and not fantasy e-mail addresses. As today's users switch e-mail addresses more frequently than in the past, criminal buyers would like to be sure they are purchasing current addresses to which they can send spam, phishing, scam, and virus mail.

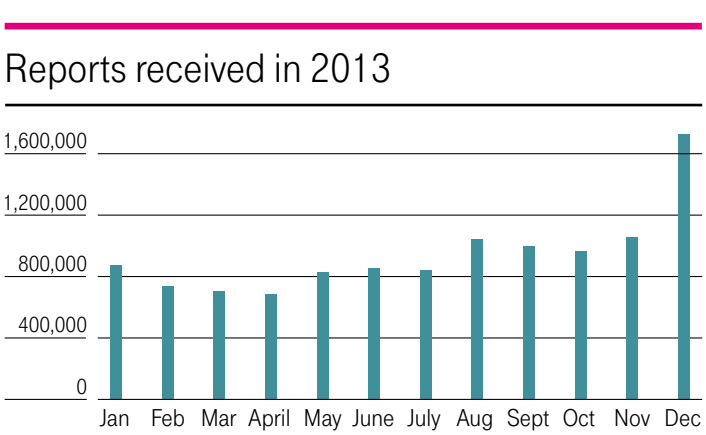
STRUGGLE FOR ATTENTION

Especially brazen criminals aim to infect their victims' computers with viruses and Trojans. They hope that users who unsuspectingly click on a link or an attachment will not be particularly careful when checking their bank statements.

That is why improving spam protection is a constant race against the spammers – and also a struggle for attention and a healthy scepticism on the users' part. You may never have received unsolicited e-mail and your spam filter may keep most spam at bay, but you could fall foul of a spammer at any time. So it is important to be informed and not to be too careless.

THE ABUSE TEAM ARE THE PEOPLE TO CONTACT IF YOU WANT TO REPORT ABUSE OF DEUTSCHE TELEKOM INTERNET SERVICES. IN 2013, THE SECURITY EXPERTS LOOKED INTO MORE THAN ONE MILLION REPORTS.





IT SECURITY IS A MANAGEMENT ISSUE

Companies still tend to regard IT security as a costly obligatory expense, says **Thomas Tschersich**, Senior Vice President Group Cyber & Data Security at Telekom. Yet an IT failure would pose a threat to their very survival.

Companies are constantly cutting costs to cope with fierce competition. IT security can surely be no exception.
Thomas Tschersich: Cost reduction and savings measures rank first to fourth on CIOs' agendas. That obviously makes it hard to puch for additional expenditure on IT security. Yet companies are running a serious risk. If their IT were to fail due to cyberattacks, many companies would face a threat to their survival within a matter of days, and that is conveniently forgotten.

Is that not a slight exaggeration?
Thomas Tschersich: Years ago it was said that a bank without IT would be bankrupt within a few days. Today, even smaller firms rely on their IT and the Internet. For a company that does most of its business online the availability of its online shop is crucially important. A successful denial-of-service attack that puts its website out of action is enough to bring business to a standstill. DoS attacks with a bandwidth up to 60 times that of past attacks mark a new trend.

So spending on IT security will need to increase significantly?
Thomas Tschersich: Not necessarily, but IT security must be regarded as a strategic issue. Only then will it receive the management attention it deserves and be a part of entrepreneurial responsibility. To this day corporate risk assessments deal for the most part only with classical risks like credit defaults or production losses. Nobody has cyberattacks on the radar. This is an area in which many companies seem to rest on their laurels, comforting themselves with the thought that they have always gotten by in the past.

How serious are the risks?
Thomas Tschersich: According to the 2013 Cyber Security Report only 13 percent of companies have never been hit by an Internet attack. 62 percent of decision makers in politics and business see data fraud on the Internet and 57 percent computer viruses as a very serious risk for the general public in Germany. So while the threats are recognized, too little is done – especially by small and midrange enterprises.

How must one deal with the subject as an entrepreneur?
Thomas Tschersich: Security must be a management issue, especially at small and midrange companies that do not have security experts of their own. They face no less serious a threat than the big guys. Yet IT, and with it IT security, is handled as a sideline by the neighbor's son or by an interested employee who can put his hobby to use at work. As a result, security is often not handled in a comprehensive way. A firewall and antivirus protection alone are not enough. To take a simple example, if I save my data to tape or DVDs every evening yet leave them alongside the server, a break-in or a fire is all that is needed for to lose everything. That may not have much to do with a cyber risk, but it is still widespread.

What can a small or midrange enterprise achieve technically in the short term?
Thomas Tschersich: To protect yourself, you really must install the latest versions of antivirus programs and software on all your computers. That should close around 90 percent of security loopholes. Software updates should then always be installed without delay. Updates often deal with security vulnerabilities that have come to light. And if you want to protect yourself from espionage and data interception, you must definitely encrypt your e-mail traffic. These three measures, for example, do not cost much, but they are a great help.

ABOUT THE AUTHOR

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

THE TELEKOM HACKER TEAM

New Telekom products or websites are subject to stringent security requirements already in the development and production phase. To ensure that there really are no security vulnerabilities ahead of their launch, an in-house team of hackers looks for hidden loopholes.

Around 30 Telekom employees try with all the means that hackers have at their disposal to identify vulnerabilities, thereby forestalling attacks that criminal hackers would otherwise launch. Around 200 products and websites underwent tests in 2013. They usually yield results. Although development is subject to detailed data security requirements from the outset, the hacker team identifies on average ten vulnerabilities per test. The difference between them and the criminals is that the "good" hackers go no further once they have cracked the safe and thus do no damage.

The methods used by the in-house hacker team correspond to the ones that criminal hackers use. The security experts keep a constant watch on the "hacker market" and learn the methods that the hackers use. The good hackers have an advantage over the criminals in that they know in advance and from the inside the systems' critical points, and are thereby able to launch their attacks in a more targeted manner. They even discover vulnerabilities that many of the external hacker would be unable to find.

A security evaluation determines which new solutions are to be hacked by the Group's in-house security experts. The team investigates uncritical solutions only on special request. The systems tested include network solutions, Cloud applications, in-house systems and DSL routers. Suppliers' products must also undergo a Telekom hack – and benefit from it. Fundamental vulnerabilities are often identified in connection with, for example, outdated software. Criminal hackers frequently make use of vulnerabilities of this kind. An once that door is open, they would have no problems to do serious damage with simple technical means.

Once a year the Telekom hacker team evaluates all the vulnerabilities that it has discovered. The most important sources of error are then transferred into stringent security requirements for development and production.

GUIDE FOR PROCESS STEPS

A new workflow tool takes teams that develop new products and systems for Telekom through the Privacy and Security Assessment process in a structured approach.

When employees of the Group develop new products, systems, or platforms, Telekom's Privacy and Security Assessment (PSA) process ensures an adequate level of security and data privacy. The PSA Portal maps the entire workflow, from the definition of security and data privacy requirements – i.e. the selection of relevant requirements –, and documentation of implemented solutions and measures to the release.

To do so, the tool maps the roles of project manager, system manager, security expert and data privacy advisor. It takes all of the employees involved through the relevant process steps online and documents the latest status of the project at the same time. They click a button to release the project for colleagues in other departments. That creates security in implementation of the relevant requirements, and enables security and data privacy to be implemented efficiently in new developments.

A further advantage of the web-based project tool is that cooperation is not dependent on the media used. Switching between Excel, PowerPoint and other applications is no longer necessary. The entire project is managed and documented via an online user interface and can be exported if required. If the newly developed system is expanded at a later date, applying the requirements selected in the previous version to the new system will still be possible.

PSA FOR ALL SUBSIDIARIES

To collaborate internationally at the same ambitious level, all projects must fulfill the same security requirements. That is why Telekom rolled out its Privacy and Security Assessment process at all European companies in 2011. Data Privacy, Legal Affairs and Compliance (DRC) defined 19 core PSA requirements. All companies mirrored these requirements against their existing processes and established whether adjustments were necessary. DRC is now reviewing the progress that companies have made in implementing the process. Specialists from the Group's headquarters will then visit the companies to assist them with further process adjustments as required.

UNAUTHORIZED ACCESS IMPOSSIBLE

Deutsche Telekom uses encryption and authentication mechanisms to protect Group bodies' confidential documents from unauthorized access.

When the Management Board, Supervisory Board, Data Privacy Advisory Board or other Deutsche Telekom executive bodies meet, many important decisions have to be made. Drafts and resolutions must be kept under lock and key, and accessible only for authorized persons. That is why Telekom since 2013 has used an online safe where all documents for each body, such as minutes or confidential information, are protected from unauthorized access.

The solution registers every access to the stored documents, so that it can always be traced who used or downloaded which file and how. Changes to the content are also always recorded, so even authorized persons cannot manipulate documents unnoticed.

To log on, a similar procedure to online banking is employed. After inputting their user names and passwords, members of the bodies are sent a text message with a single-use PIN number that has to be entered to access the data safe. If they are Telekom employees, they can also use their electronic company ID in the form of a smart card.

Additional protection for especially confidential phone calls is provided by encrypted Voice over IP phones that are available within the company, so that calls cannot be intercepted either in-house or by third parties.

HOW TO IDENTIFY CYBERATTACKS AT AN EARLY STAGE

Vulnerability of globally networked companies is on the rise, with industrial espionage and cyber sabotage increasingly targeting business expertise and processes that are indispensable for corporate value creation.

Fail to adjust your cyberattack detection and response capabilities to this threat, and you will only ever lag behind these complex and focussed attacks. To overcome this role of being pursued, a role that is as risky as it is frustrating, you need evidence-based security management that connects information in a targeted way, so that it can be evaluated in real time. The aim of this proactive approach is not only to protect yourself from known attacks but also to identify attacks that are yet unknown, and to initiate immediate countermeasures.

T-Systems and RSA have joined forces to implement their Advanced Cyber Defense (ACD) services. RSA's "intelligence-driven security" approach is based on all security-relevant information from networks, systems and applications being centrally recorded, conflated and analyzed. Security is becoming a Big Data challenge. The combination of modern IT security technology, expertise, and access to data resources and in-house early-warning systems makes it possible to set up these new security systems.

ACD is centered on the Next Generation Security Operations Center (NG SOC) where the experts collect information about all of the relevant attack scenarios. With an in-house focus the security experts at the NG SOC investigate where corporate values or supporting IT and telecommunication systems are vulnerable or have already been attacked. Externally, they clarify potential attackers' motives, methods and tools, and recognize the relevant scenarios before the damage has been done.

CYBER SECURITY REPORT 2013

One out of five firms polled by the Allensbach Institute for Demoscopy for the 2013 Cyber Security Report faces attacks by hackers, daily or several times a week.

The risk evidently rises with the size of the company. One out of three companies with over 1,000 employees said they registered several attacks per week. Among smaller companies with up to 100 employees, 16 percent report frequent attacks. The issue of IT security was nevertheless considered to be very important by nearly all companies (92 percent). This is reflected in their investment, with 35 percent of respondents reporting significantly and 41 percent slightly higher expenditure in this area.

Business executives have also become more risk-aware. A year ago around 42 percent of large companies rated the risk of damage by a hacker attack as high or very high; the latest figure is 53 percent. Yet the majority of companies (56 percent) feel they are prepared as well as possible to face this threat. Around 40 percent even have a comprehensive strategy for dealing with cyberthreats and a further 13 percent are working on one. Well over 40 percent, however, rely only on individual measures to protect their IT systems and company data.

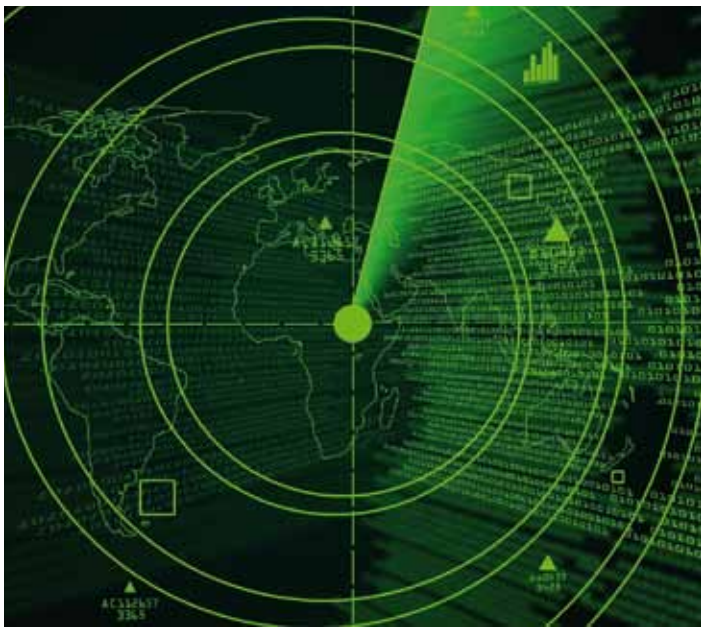
For the study, which was commissioned by T-Systems, the Allensbach market researchers interviewed 221 executives from large companies and 293 decision makers from midrange businesses.

FROM REACTION TO PROPHYLAXIS

Deutsche Telekom's CERT rapid reaction force will ward off attacks before they become dangerous.

Cybercriminals constantly vary their attacks. Firewalls, proxy servers, intrusion prevention, and other classical security measures are no longer sufficient to keep pace with modern attackers. That is why Deutsche Telekom's Cyber Emergency Response Team (CERT) is taking on additional preventive tasks. The CERT experts are to ward off cybercriminals before they can do any damage.

"Protective measures like a firewall," says Bernd Eßer, Head of Deutsche Telekom CERT, "are based on defined rules and are only effective when attacks correspond to certain criteria." But professional hackers vary their methods sooner or later in order to achieve success. "To ward off these unpredictable attacks at an early stage," he says, "we will in future need to merge and evaluate data from five different sources."



In order to ward off unforeseeable attacks, Telekom CERT evaluates data from five different sources.

TARGETED SEARCH FOR MALWARE

These sources are the Group's firewalls, its intrusion prevention systems (IPS), proxy servers, Exchange servers and Telekom's antivirus solution. The firewalls, for example, record when an attacker tries to find open ports through which to intrude into Telekom systems. The intrusion prevention systems are lined up behind the firewalls and recognize when malware such as a bot client has infected an employee's system.

Hackers use a bot to control hacked systems remotely, to read out data and to attack other systems either to sabotage them or to infect them, too. Telekom's IPS solutions learn or know which IP addresses the hostile servers use.

Telekom's proxy servers record the IP address from which the Intranet communicates with which website on the Internet. This simple protocol data is a valuable source of information if the Group's forensic team has identified the malware in an infected e-mail attachment. Telekom employees who receive e-mail with a suspicious attachment send it to the IT forensic department. If it is found to be malware, the security specialists find out which URL it would use if it were to install itself on a system. The proxy server's protocol data can then be searched for this URL to identify systems on which the malware has implanted itself.

The security experts use a similar procedure with the log data of the Exchange servers that are in charge of transporting e-mail within the Group. If a malicious e-mail attachment is identified, the CERT specialists set up a targeted search for further e-mail with this attachment and deal with it directly on the servers.

QUARANTINE FOR VIRUSES

Telekom's antivirus solution recognizes malware by itself and puts it into quarantine. From the log data CERT specialists can see whether infections are becoming more frequent in a certain area because an attack is taking place there.

Furthermore, Telekom forensic specialists analyze the malware that the antivirus program has identified. They find out how it behaves on an infected computer and can then embark on a targeted search for systems that fulfill the appropriate criteria, and modify the antivirus software so that it clean up infected computers automatically. In future, Telekom's CERT will compare the log data of the firewall and the proxy server with the data of reputation feeds. In this way they can identify IP addresses that in all probability host the malware without an employee having to report suspicious e-mail attachments.

CERT AS MANAGED SERVICES

US companies often use a Big Data approach to evaluate stored data on a large scale, from all manner of log sources in the event of a presumed or actual attack. In Europe, that is only possible to a limited extent due to data protection requirements. That is why CERT employees rely on their experience of how cybercriminals go about their attacks and of the phases that make up a cyber attack. They can evaluate log sources in a targeted manner to identify indications of these attacks.

As CERT only models the approach of external cyber criminals, the procedure poses no data protection problems because the use cases are such that they constitute an initial suspicion of criminal behavior and thereby permit CERT to go ahead with further evaluation. Telekom will also be offering the new CERT services as a managed service for industrial enterprises.

TELEKOM'S SECURITY MANAGEMENT: THE CORE OF CORPORATE SECURITY

The ancient Greek philosopher Aristotle said that the whole is more than the sum of its parts, and that is one reason for Telekom's different security areas to collaborate even more closely.

Since 2010, Telekom's Security Management has been certificated to ISO 27001 by DQS, one of the leading management system certification companies in Germany. It certified the functioning of the Information Security Management System (ISM) of the Group's central security areas and reaffirmed the high quality, continuous development and integrated risk-oriented security perspective of Telekom's Security Management. The current consolidation of central security functions in the Management Board area responsible for data privacy, legal affairs and compliance is thus the next logical step to consistently development and continue with the convergence concept beyond virtual collaboration into even more strongly integrated security organization. This is to the advantage of the Group because it strengthens further the integrated security perspective in considering and responding to the growing complexity of the risk situation. This, of course, continues to be done in close collaboration with the data protection department.

SECURITY POLICIES 2.0

"What you need is clear and concise content, a clear definition of roles and responsibilities, a defined purpose and obvious consequences for non-compliance by staff." For Gartner analyst Les Stevens these are the key aspects of successful security policies.

They are precisely the reason why Deutsche Telekom in 2013 continued to fine-tune its Security Policies, centrally drafted for the Group and implemented in June 2010. Since the policies were implemented uniformly and step by step across the Group, suggestions from German and international Telekom units and subsidiaries have found their way into them.

With Security Policies 2.0 the Telekom security managers have further simplified the language of the requirements and have developed a checklist of the individual test points that had previously been framed in more generic and general terms. Group units can now see even faster what they need to tackle in order to implement the policies. It used, for example, to be said that security risk management consisted of the four steps risk identification, evaluation, treatment and acceptance. The policies now describe more precisely how these four steps can be implemented and how this implementation may be checked.

Security Policies 2.0 cover a broader scope. They include issues like workplace violence (such as mobbing) and cyber security. Regarding the latter, the security managers had to deal with the new risks incurred by "bringing your own device" or by malware unintentionally smuggled in on USB sticks.

INTERNATIONAL COLLABORATION

The International IT/NT Security Leadership Team ensures that the technical security of all European affiliate companies with their own telecommunication networks fulfills the same appropriate requirements.

The Telekom Group shall continue to grow together and all affiliate companies are to collaborate on the same level of ambition. To achieve this objective, the Data Privacy, Legal Affairs and Compliance division has set up the International IT/NT Security Leadership Team. The team consists of the heads of technical security at Telekom headquarters and at the affiliate companies. It meets every six weeks and holds an annual strategy workshop. Participants jointly decide on topics they will discuss in detail over the course of a year, often smaller groups, like a task force and using a project structure. These working groups develop solutions and guidelines that both the country companies and headquarters utilize to continuously increase their security level.

In 2013, participants chose as their core issues DDoS protection, patch management and know-how transfer in secure LTE development. The working groups dealt with tools and processes to provide protection from distributed denial-of-service attacks, developed concepts to efficiently and sustainably eliminate security vulnerabilities by installing patches during continuous operation, and devised measures to prevent attacks on LTE networks.

Information is shared between headquarters and affiliate companies at several levels in order to promote collaboration and networking between them. Specialized cooperation between companies is at the expert level. The high level of participation underscores how important this work is for all concerned.

IDENTIFYING AND PREVENTING COMMUNICATIONS FRAUD

Consumer associations issue regular warnings of frauds that use expensive telephone service numbers. Value-added service numbers are especially popular with criminal fraudsters. Calls often cost several euros per minute. Telekom tries to identify fraud by all means legally available – and thereby to protect both its customers and the company itself, explains Volker Wagner, in charge of Group Business Security (GBS) at Telekom.

Fraudsters manipulate telephone connections and send telephone bills sky rocketing.

It is a race against virtual opponents and against time. Fraudsters are using one new method and one new subterfuge after another to exploit the providers' telecommunication services to generate fraudulent returns. The damage caused by this abuse is amazingly enormous. According to a 2013 study by the Communications Fraud Control Association, fraud costs the global telecommunications industry around US$ 46 billion a year.

A few fraud scenarios account for the majority of cases. Offenders hack into telecommunications facilities or voice over IP connections and take over control of the connections. They steal or take over identities and take control over customers' accounts. Costs mount up especially fast for customers if they inadvertently make a return call using one of the provider's expensive service numbers. Their providers then bill them without knowing that they never really used the service. That often leads to a dispute between the provider and the customer who, understandably, does not want to pay these charges. If Telekom is unable to prove fraud, it is eventually left with the costs.

OBSERVATION OF TRAFFIC AND USER DATA

Telekom uses special systems to recognize and prevent cases of abuse of this kind. To do so, it is necessary to observe traffic, usage and inventory data, and, if required, filter and evaluate it. This is done according to Section 100 of the Telecommunications Act, which states that the service provider may "use such inventory and traffic data as is necessary to secure its entitlement to payment in order to identify and prevent illegal use of the telecommunications network or service."

There is little point in tracking and evaluating the data traffic of around 40 million customers in full. That is why the experts use fraud recognition systems that enable them to filter data traffic in accordance with specified criteria, including certain threshold levels. If, for example, the system identifies an unusually high level of expensive voice and data communication on a telephone line, it will send out an automatic alert. The network experts can then look into the cause and maybe stop to the abuse.

There are also time-limited, project-based fraud recognition measures. The network experts check data for pre-defined fraud scenarios. In the course of this process they draw up a concept that inter alia describes precisely the data records and IT tools that are to be investigated.

DRAWING UP WHITE AND BLACK LISTS

As fraud recognition may involve customers' personal data, measures may only be undertaken in close coordination with Group Privacy. A catalog of scenarios describes all procedures that comply with data protection law, and can be used legally to process traffic, usage and inventory data for fraud recognition and investigation.

Scenarios that comply with data protection law are "whitelisted" and can then be used repeatedly. In case of doubt, Group Privacy must be involved as a matter of principle. Scenarios that Group Privacy rejects are "blacklisted." There are, however, certain procedures for which the fraud recognition team must in each case secure approval from Group Privacy and the legal department in advance.

THE FRAUD RECOGNITION TEAM'S TASKS

Fraud recognition falls mainly within the remit of Group Business Security (GBS). It involves the following tasks:

- definition of business requirements for IT-assisted fraud recognition systems
- identification of possible cases of fraud from ongoing observation of traffic and networks, and from project-based assignments
- communication of suspected cases of fraud to other departments in order to combat fraud.

ABOUT THE AUTHOR

Volker Wagner
has been in charge of Group Business Security (GBS) at Telekom since 2008. Previously he held leadership positions in the areas of audits, finance and sales. In addition he is the chairman of the German Association for Security in Industry and Commerce, and a board member of two German security associations, and engaged in ASIS International association.

ACCELERATED EXPANSION

Deutsche Telekom operates a globally distributed early-warning system for cyber-attacks. Honeypots play a key role in the system. The network currently registers up to 800,000 attacks per day.

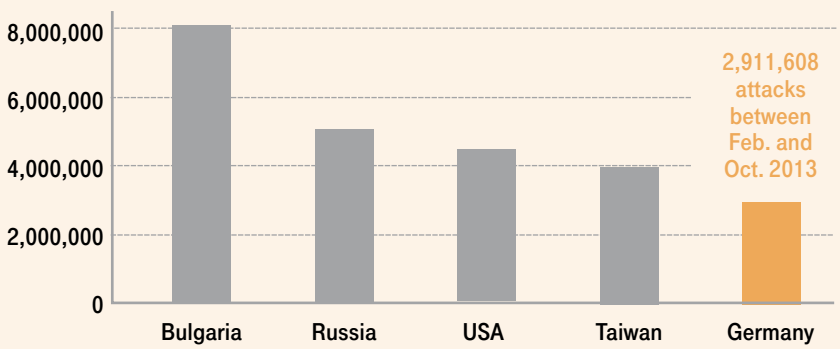
Honeypots simulate vulnerabilities in order to attract attacks so that they can be analyzed. In 2013, Telekom again enlarged the network significantly. In the course of the year nearly 100 new honeypots were set up, making their total number now around 180.

In order to make information from the early-warning system as widely available as possible, Telekom established a freely accessible Internet portal for CeBIT 2013. The Security Dashboard (**www.securitydashboard.eu**) provides real-time data on the latest threat situation. Attacks on individual countries can be shown by means of honeypot installations. Portal visitors can also see the countries from which attacks originate. Most come from China, Russia and the United States, but generally Germany, too, is among the top five countries from which cyber attacks originate.

Honeypot network data is no guide to whether the attackers are based in these countries, however. The overwhelming majority of IP addresses involved are those of hijacked computers remote-controlled over the Internet. The honeypots' sensors cannot see where the command servers are that work in the background.

THE TOP FIVE COUNTRIES OF ORIGIN

Between February and October 2013 most of the cyberattacks on Telekom honeypots came from Bulgaria, Russia and the United States, with hackers using different number of hijacked computers per attack. Most computers hijacked and misused for cyberattacks were located in China, the United States and Germany.



SECURE SIM CARDS

In mid-2013 around 900 million SIM cards for cellphones and Smartphones were reported to be not secure. SIM cards used by Telekom Deutschland customers were not affected because Telekom uses a stronger algorithm, even for older SIM cards, than the one that was being discussed at the time.

Specifically we are talking about the older DES data encryption standard. SIM cards with this outmoded encryption technology can be hacked remotely by text message. The text contains a self-installing malware. The user can only identify possible misuse in retrospect. Hackers could then make phone calls with the hijacked card, redirect calls or listen to them. Experts estimated at the time that around one SIM card in eight around the world might be infected by the malicious code.

MOBILE HONEYPOTS

In addition to around 180 stationary honeypots, Telekom currently uses mobile honeypots that simulate different Smartphones. Together they register up to 30,000 attacks per month.
These honeypots, operating from a data center, behave like a jailbroken iPhone or a rooted Android Smartphone. While Smartphones on sale with a Telekom SIM card are very well protected from cyberattacks on the network side, Telekom honeypot experts purposefully have prepared the decoy devices to make hacking them easy. The honeypots have a public IP address which makes them an attractive target for hacker attacks. On average, the mobile honeypots register up to 30,000 attacks per month. Attacks can be identified when someone logs onto a device and tries, for example, to copy the address book or images, or to install an application to make the phone part of a botnet. These attacks are largely similar to those on computers that are connected to the fixed-line network.

Another mobile honeypot named Honeydroid and specially adapted to the Android operating system is currently running on a Samsung Galaxy S4 and an HTC Desire. Both Smartphones can be used to almost their full functional extent while the software installed on them detects attacks from the mobile Internet and relays them to Telekom's early-warning system. In recent months, fewer attacks on the mobile honeypots have been recorded. That could be because the IP address allocated to them has changed to an area that has not yet been a focus of hacker activity.

HIGHLY POPULAR

Since October 2013 Deutsche Telekom has invited hackers to test its German Internet portals for vulnerabilities. The first person to identify a bug receives a cash reward.

The so-called Bug Bounty program got off to a flying start. In October and November 2013 around 500 reports about security vulnerabilities were received. Thanks to the Internet community's enthusiastic support Deutsche Telekom is now able to improve the security of its Web applications significantly yet again.

The initiative is based on a so-called responsible disclosure policy. The informant agrees with Telekom neither to make use of the vulnerability nor to publish it anywhere else. At the same time, Deutsche Telekom undertakes to resolve the reported security issue as quickly as possible. The informants' commitment earns them a cash award. The amount depends on the criticality of the bug and of the portal affected. The Bug Bounty program is focused on all *telekom.de domain Web portals. Bounties are awarded for the first reports of vulnerabilities in program code developed by Deutsche Telekom. They are not made for bugs in any third-party products that Telekom may use. For terms and conditions visit www.telekom.com/bug-bounty

IMPROVED INTERCEPTION PROTECTION FOR CELLPHONE CALLS

Telekom is Germany's first network operator to use the A5/3 encryption standard for voice transmission on its mobile network. Calls on the GSM network now enjoy better protection from possible interception. The standard was implemented throughout Germany by the end of 2013.

Customers do not need to do anything about encryption of their cellphone calls. Encryption is applied automatically during transmission from phone to network. The A5/3 standard improves encryption on the GSM network. The new algorithm has so far been considered secure. Encryption standards of similar strength are used on the UMTS and LTE networks. For the new standard Telekom had to install new hard- and software around the country at around 30,000 base stations and central network points.

A particular challange to a sucessful changeover was posed by some 50,000 older handsets still in use, which are unable to work with the new encryption standard. To ensure that these customers are not suddenly cut off, Telekom had to develop and test a special software solution. All cellphone models will now continue to function, but calls from older models will continue to be encrypted using the A5/1 standard.

Telekom uses the A5/3 encryption standard not only in Germany but also in Macedonia, Montenegro, Poland and the Czech Republic. Other countries are to follow.

WLAN HOTSPOTS WITH BUILT-IN SECURITY

Deutsche Telekom aims to set up the world's largest hotspot network. To do so, it launched the WLAN TO GO initiative in June 2013. By 2016, 2.5 million new hotspots are to be established in Germany alone.

WLAN TO GO

By means of a special configuration of the Speedport W724V router DSL customers will be able to share unused bandwidth of their connection with other Telekom customers. Telekom has checked the new solution's security.

DSL customers receive entirely secure solution working on all Speedport W724V routers. If a broadband customer decides to take part in WLAN TO GO, the router sends two WLAN signals, thereby creating two totally separate WLAN networks. One is encrypted and remains private, the other is available for hotspot users to access via Telekom_FON.

A hotspot user who logs on via Telekom_FON cannot access the private WLAN. The same applies in the other direction. The hotspot user does not need to worry that the owner of the connection might access his mobile terminal device. Furthermore, with WLAN TO GO there is no risk of liability for illegal use by third parties. As only authenticated users have access to the hotspots, usage can be traced.

STRIKING THE BALANCE BETWEEN DATA PRIVACY AND SECURITY

As a telecommunications provider Telekom must protect its customers' data with all the means at its command and has every intention of doing so, but in certain circumstances the law requires it to divulge personal data.

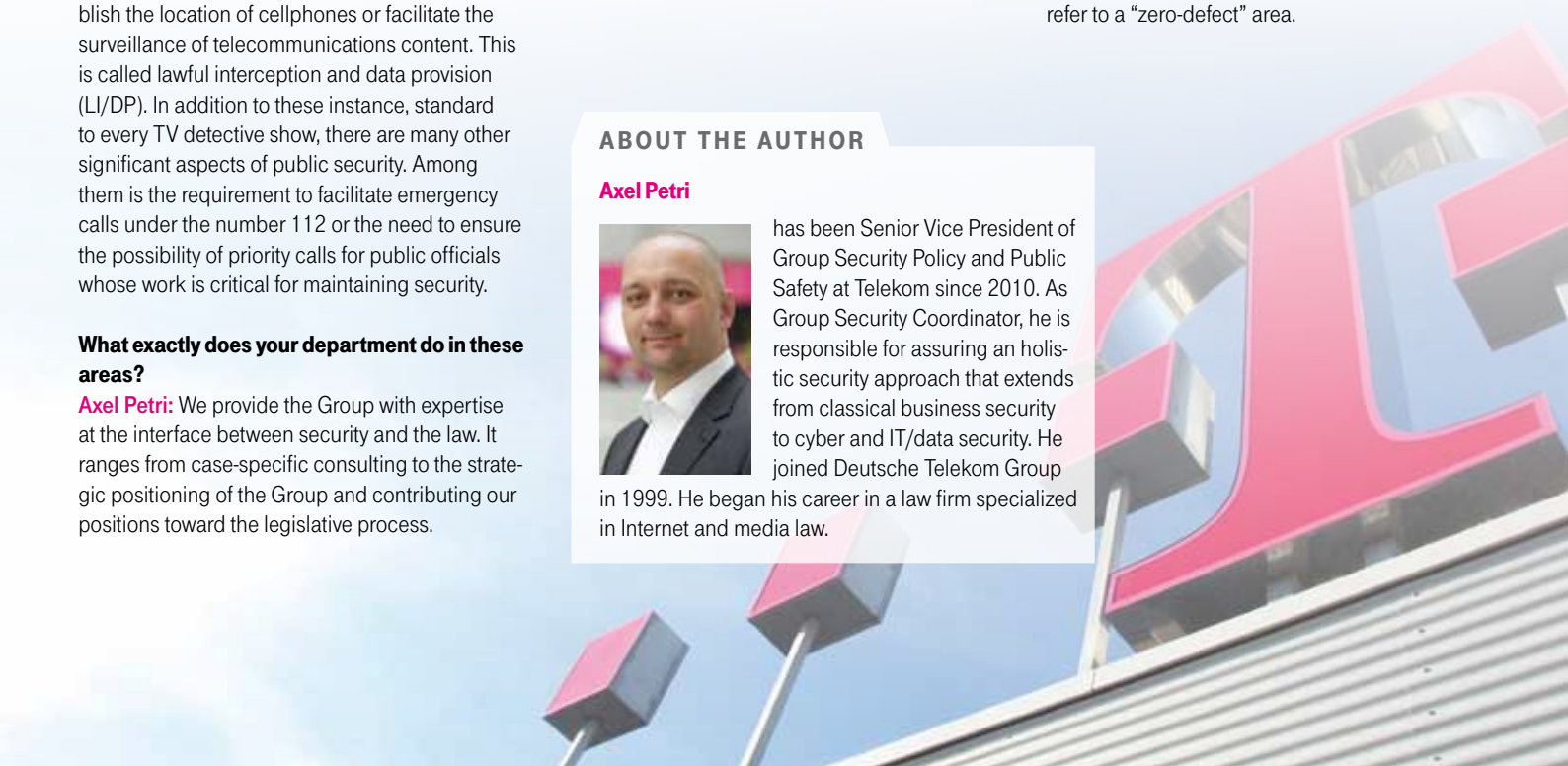
What lies behind the concept of public security?
Axel Petri: The concept is defined in the German Telecommunications Act (TKG), which deals with public security in Section 7.3. It refers to all the mandatory requirements that Telekom must fulfill as a provider of telecommunications services in order to help maintain security and order. What, for example, are its rights and duties when the security authorities request information, or in implementing surveillance measures or in supplying information to authorized bodies?

What specific obligations must Telekom fulfill?
Axel Petri: We must, for example, notify government authorities of certain telephone data, establish the location of cellphones or facilitate the surveillance of telecommunications content. This is called lawful interception and data provision (LI/DP). In addition to these instance, standard to every TV detective show, there are many other significant aspects of public security. Among them is the requirement to facilitate emergency calls under the number 112 or the need to ensure the possibility of priority calls for public officials whose work is critical for maintaining security.

What exactly does your department do in these areas?
Axel Petri: We provide the Group with expertise at the interface between security and the law. It ranges from case-specific consulting to the strategic positioning of the Group and contributing our positions toward the legislative process. For the LI/DP sector we also implement measures to provide, for example, access to databases or network elements.

In which circumstances does Telekom fulfill security authority requests?
Axel Petri: For Telekom the sole and supreme guiding principle is to comply with the law. Only when all statutory requirements are met, we implement the orders of the authorities – as a rule courts or public prosecutors. As you can see, the real world is totally different from the fictitious TV world where this seems to happen on demand. We must also provide this statutory service 24/7 and be on call around the clock.

Is public security not of the greatest interest for everybody?
Axel Petri: Along with public security there is always the obligation to respect our customers' telecommunications secrecy and to fulfill statutory data protection requirements. In practice, sad to say, these two legal rights often conflict with each other, as evidenced by the extremely contentious political debate on statutory provisions for data retention. We must also consider carefully what we do in order not to either obstruct the course of justice or infringe telecommunications secrecy. So we must always strike a very fine balance in this high-profile area. If mistakes were to occur, they would have an immediate negative effect on the Group's reputation. That is why we refer to a "zero-defect" area.



ABOUT THE AUTHOR

Axel Petri

has been Senior Vice President of Group Security Policy and Public Safety at Telekom since 2010. As Group Security Coordinator, he is responsible for assuring an holistic security approach that extends from classical business security to cyber and IT/data security. He joined Deutsche Telekom Group in 1999. He began his career in a law firm specialized in Internet and media law.

TELEKOM EMPLOYEE MAKES E-MAIL MORE SECURE

Time for innovation: Wolfgang Bollenbach develops an encryption solution for private e-mail addresses in an ideas program.

GIS employees are allowed one day per month to develop innovations.

"Delight customers and make things easier!" Wolfgang Bollenbach took this Telekom Group guideline to heart and developed an encryption solution for private e-mail addresses as part of an ideas program at Group Information Security (GIS) where he works. It is inexpensive, simple and geared to the need for greater security.

Using open source products, Bollenbach created a website that generates encryption certificates for e-mail addresses. It costs virtually nothing but the added value for the user is enormous. On the basis of the so-called S/MIME standard e-mail can be encrypted end to end in their entirety.

S/MIME stands for Secure/Multipurpose Internet Mail Extensions, and is an international standard for the encryption and signature of e-mail. A user can use the encryption certificates for all his terminal devices. He can use the certificates to encrypt his e-mail to anyone who also has S/MIME certificates. Telekom is currently looking into whether the service can be integrated into its products.

At Group Information Security (GIS) the One Day per Month program laid the foundations for innovative ideas like Bollenbach's. It offers GIS employees an opportunity to spend one day per month working on a project of their own that has nothing to do with their day-to-day work. The only requirement is that it relates to Telekom. Since the program was launched, employees have developed and implemented a whole range of ideas, including mobile honeypots for Telekom affiliate companies.

SECURITY LOOPHOLE CLOSED

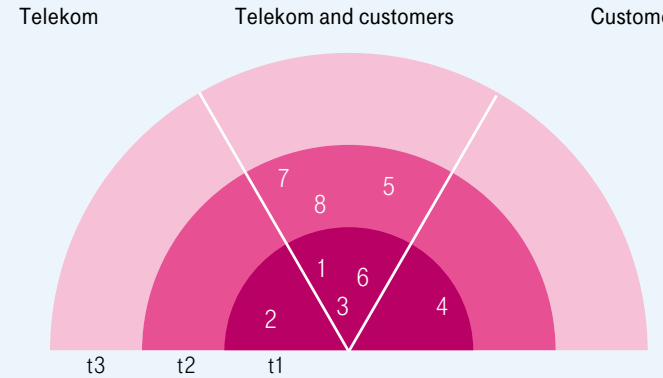
In mid-2013, a hacker discovered a security loophole at Telekom's Customer Center. Intruders could have hijacked e-mail addresses with the suffix @t-online without the user noticing anything. Telekom closed this loophole immediately.

Right until the loophole was closed, there were no indications that it had actually been exploited and e-mail accounts had been hijacked. A possible attack could have been launched by means of a script that hackers could hide on a website. This website would also have to originate from the telekom.de domain. If users clicked on the infected website, the script would have begun to work in the background.

The malware would first have changed the user's address from, say, Müller-90@t-online.de to Müller-80@t-online.de. The original e-mail address would then have lapsed and the hacker would re-apply for the e-mail address Müller-90@t-online.de himself. The former account holder would no longer receive any e-mail because it would all go to the address's new owner. After receiving the tip from the hacker, Telekom closed the loophole by means of an additional password request.

STRATEGIC THREAT RADAR

Telekom's CERT uses the threat radar to display current cyber threats. The radar offers the company a way to identify threats at an early stage and to plan for appropriate security measures.



THREATS

1 Advanced persistent threats (APT)
2 Spear phishing aimed at Telekom employees
3 Mobile malicious code
4 Attacks on mobile banking
5 Denial of Service attacks on DNS infrastructure
6 Attacks on DSL routers
7 Attacks on automotive CAN bus systems
8 Attacks on smart TVs

DEVELOPMENT STAGES

t1 Active exploitation of a known vulnerability
t2 Vulnerability exists, exploitability proven
t3 Vulnerability exists and can in theory be exploited

WHO IS THREATENED?

The radar shows who is affected by a threat: customers who use Telekom products and services (right), Telekom and its internal systems (left), or both (center).

E-MAIL MADE IN GERMANY

For large companies and small and midrange enterprises, for craft workshops and private homes, using e-mail is always associated with the risk of infection by Trojans or viruses. And e-mail is as open as a postcard anyone can read en route.

That is why ensuring e-mail security is a compulsory task for safe and secure IT. Yet, even the latest virus scanners and firewalls fall short of the mark. They may filter out most of the malware from e-mail traffic but they fail to ensure that third parties cannot read the contents of a mail. In principle, the Internet transmits e-mail unencrypted from sender to recipient. While on its way, the providers transporting route e-mail via many different computers. In the process reasonably competent hackers can read the e-mail by using simple means, and e-mail often contains information that is of interest for criminals, such as account numbers.

TRANSMITTING E-MAIL ENCRYPTED

Thus, the only effective protection is to send confidential e-mail encrypted. Telekom, together with United Internet, has launched an industry initiative for secure e-mail communication in Germany to which freenet also signed up later. With "E-mail Made in Germany" the e-mail of GMX, T-Online.de, Web.de and freenet will be encrypted automatically on all transmission routes between e-mail servers and data centers. All without having the users to do something or change his settings.

E-mail addresses will also be marked so that users can tell before sending mail whether the recipient's e-mail address corresponds to the E-mail Made in Germany standard. For encryption the partners use only keys made in Germany and open source solutions that do not, unlike commercial products, have security loopholes.

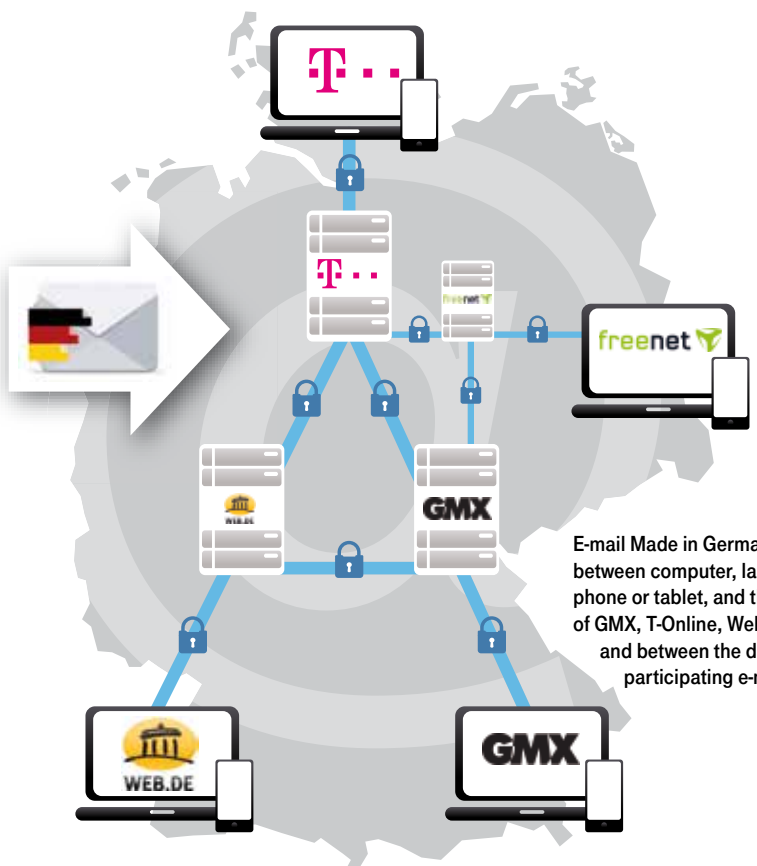
PROCESS ALL DATA ONLY IN GERMANY

"E-mail Made in Germany can be compared with a postcard that we not only put in an envelope but also pack all of the sealed envelopes into additional mailbags. That means, the sender and recipient are erased en route," says Telekom IT Security manager Thomas Tschersich. Mail can still be sent to other e-mail providers such as Google, Yahoo or Microsoft, but E-mail Made in Germany can't guarantee neither secure transmission nor that the data is processed in Germany. "The partners in the initiative," Tschersich adds, "also guarantee to process all data only in Germany. Data is thus subject to the strict German data protection provisions – without possible watering-down or regulation by authorities in other countries."

VERIFIABLE, SECURE AND RELIABLE

De-Mail goes even one step further in providing security. It corresponds to registered mail with a receipt for acknowledgment. The sender receives confirmation from the recipient that he has read the mail, and as with E-mail Made in Germany hackers can neither read nor manipulate the contents of a De-Mail on its transport across the Internet. De-Mail can only be provided after the service has been certificated by the Federal Office for Information Security (BSI). This ensures a uniform, tested level of security.

The legal basis for De-Mail is Germany's De-Mail Act, which lays down the minimum requirements for secure electronic data interchange. The Act also provides a regulated procedure by which these requirements and the De-Mail providers are monitored. These are important preconditions for the development of confidence in the security and quality of De-Mail services. The statutory provisions also ensure that all De-Mail users with different providers can contact each other.



E-mail Made in Germany relays data between computer, laptop, Smartphone or tablet, and the e-mail servers of GMX, T-Online, Web.de and freenet, and between the data centers of participating e-mail services.

USER-FRIENDLY IT SECURITY

More time and money must be invested in IT security, especially in the usability of security solutions. Only if security becomes more usable, we will no longer consider it to be a nuisance. Professor Matthew Smith, a computer scientist at the University of Bonn, is convinced that this is the case.

Regardless of what actually triggered the boom in apps, practical applications for Smartphones and tablets have revolutionized the usability of software. Users previously had to struggle through days of training courses. With apps it was suddenly all so much easier. Download and install them, and most apps can be used without having to plough through manuals.

Most IT security solutions lack this new lightness of software usability. Even sophisticated offerings gather dust as white elephants on the providers' shelves while one new security vulnerability after another makes life easy for cybercriminals. Until now, much of the development in IT security followed the principle that users must adjust to the technology. They must learn how to use systems correctly. It is high time this principle was reversed. In research on usable security and privacy we are therefore developing security solutions that adjust to the users, and are thus easy to understand and use.

It begins with small ideas. Take apps, for example. Although they are user-friendly, hardly anybody reads the long pages of security information about an app's permissions before they install it. Why bother when the practical app converts a Smartphone into a flashlight or scales? Yet the permissions – usually in small print – contain "hidden" information about what an app is authorized to do with the Smartphone in addition to its evident purpose. It may, for instance, access contact data or locations. We cannot be sure whether the provider will sell this data to companies for advertising purposes or for data analysis, but he probably will. In this way the app provider converts the user into a product.

Poor usability of security solutions costs time and nerves.

OFFER GREATER TRANSPARENCY

That is legitimate as long as the provider makes it clear what he intends to do with the users' data. Only then they are in a position to decide for themselves whether they want to divulge this data or not. For this purpose we have developed as an example of people-centered IT security an app for Android devices that makes it quite clear which data the app provider wants to make use of and how. If, for example, an app accesses the Smartphone's phone directory, our software selects a contact from the directory and notes, say, that "the app is accessing your mother's phone number". Or it shows your current location on a map and points out that "this app can see that you are here right now". And if it can even switch the camera on, our app then displays the live camera image.

This may not achieve perfect security, but it does create transparency. The user must understand what the app can do. With a study of ours we were able to demonstrate that visual references to an app's capabilities change the users' download behavior. They install fewer programs on their Smartphones that have permissions they cannot follow.

Usability begins with the development of software. A lot of security loopholes are due to errors in programming and configuration. In that respect, nothing much has changed, I believe. We have the technical capability to provide more security but we do not have the people who can set up and run the systems more securely. In several studies our team of researchers has interviewed hundreds of developers and administrators, and searched systems specifically for errors. We were able to establish that many developers and administrators do not know what security loopholes exist in their systems.

Developers often work under high time and cost pressure on increasingly complex systems. It is almost impossible for a developer to identify and eliminate all of the vulnerabilities in millions of lines of code. That is why we as users must deal in live operation with the many security gaps that ought to have been closed at the programming stage. The hacker needs only a single error to break into the system. It is also amazing what vulnerabilities professional hackers find and how specifically they exploit them.

Furthermore, security code is highly complex and very difficult to program. That is why we must also improve developer training. For too long IT security has been seen as an optional and sometimes even an unpopular informatics discipline that is not on offer in the curriculum of some conventional universities and universities of applied science. That is why I am very much in favor – and advocate – of making IT security a part of basic training and a compulsory subject in computer science, and of paying special attention to its usability by people.

ABOUT THE AUTHOR

Matthew Smith
is Professor of Usable Security and Privacy at the University of Bonn and a member of staff at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE). He studied computer engineering, graduating with distinction and has for many years been engaged in research on IT security, especially the usability of IT security systems.

THE CYBER SECURITY BUSINESS UNIT

T-Systems has bundled its IT security portfolio in the Cyber Security business unit. Senior Vice President Cyber Security, Dr. Jürgen Kohr, pursues a strategy that is geared to the guiding principles of transparency, competence, simplicity and cooperation.

News headlines about Whatsapp, the New York Times, Adobe or President Obama's online websites have all demonstrated that in 2013 professional hackers made use of every loophole in the digital systems of companies, private individuals or authorities to do damage for a variety of motives. Fighting cybercriminals is no easy task because they switch their digital weapons and change their tactics fast.
But how can CIOs best protect their companies? The focus is on experts and management sharing news and views on acute threats across companies and industries. Using the motto "Security is for Sharing", T-Systems is setting up a kind of digital neighborhood watch with the Cyber Security BU in the chair as its moderator. The aim is to establish a permanent exchange on security issues at the decision-making level. The insights gained are then used for new products and defense strategies. Transparency reduces the attackers' lead and improves defenses with the result that the cost of launching attacks is growing increasingly expensive for the cybercriminals.

CLEAN PIPE: SECURITY STRAIGHT FROM THE TELEKOM CLOUD

Underestimating the risk and a lack of awareness of how attractive you are as a target for cybercriminals are the greatest threats. Few companies have the resources and competences required to deal with targeted attacks. SMBs find it especially hard to keep up with technology and trained personnel, with the pace of one new attack after another and sophisticated methods of attack. In many cases they fail to notice attacks or only do so when it is too late. The time in which the attacker can go about his attack unnoticed must be reduced drastically. That is the only way in which counter-measures can get under way sooner and limit the damage.

In 2014, T-Systems will test new Clean Pipe security services from the Cloud and will start providing them to customers as from mid-year. Clean Pipe will automatically filter harmful content at data centers. Small and midrange businesses

will thereby benefit from protective mechanisms that are otherwise only available for large corporations. T-Systems is cooperating with LANCOM, a German company that has developed a router certificated by the Federal Office for Information Security. The infrastructure for Clean Pipe is expected to be available for the whole Group by the beginning of 2016 ready to clean the data traffic of up to one million SMBs in the Telekom Cloud.

SECURITY COOPERATION FOR LARGE CORPORATIONS

If you first need to measure security incidents before acting against them, you will constantly lag behind targeted attacks. To get ahead, an evidence-based security management is required that links information precisely and evaluate in real time. With "Advanced Cyber Defense by Telekom" the group aims at exactly this, to recognize attacks before they have taken full effect is the target. "ACD by Telekom" combines state-of-the-art IT security technology, expertise and access to data resources such as the Group's own early-warning systems – its honeypots – to deliver cyber security management that controls a company's IT security and reacts dynamically to attacks. To set up a Next Generation Service Operation Center, the Group has joined forces with RSA. The "intelligence-driven security" approach of IT security provider RSA records as much information as possible from networks and applications, conflates them and assesses them by means of Big Data analyses.

TELEKOM ENCRYPTION IN THE CLOUD

Another strategic key issue is to market security innovations faster by means of start-ups and risk capital. The Cyber Security business unit is currently taking encryption and the Cloud forward with CipherCloud, a Californian company in which T-Venture holds a stake. This collaboration aims at enabling users to work with the encrypted data that is stored in the Cloud. This new solution uses keys from Telekom's own trust center. The CipherCloud solution will enable secure use and total control of data in private, hybrid and public Cloud applications, thereby resolving data privacy and regulatory misgivings.

ABOUT THE AUTHOR

Dr. Jürgen Kohr
is Senior Vice President of the Cyber Security business unit at T-Systems. He was previously head of strategy in the IT large customer division and chief of staff for Telekom Management Board member Reinhard Clemens. As a business administration graduate, he drives the development of new security products. He is also a member of the Investment Committee of the Infrastructure Fund at T-Venture, Deutsche Telekom AG's venture capital company.

E-MAILS WITHOUT DETOURS

When indignation about mass surveillance by intelligence services soared in the fall of 2013, Deutsche Telekom launched the idea of national or Schengen area routing, firing up a debate on the alleged end of Internet freedom. This is a clarification.

The Internet of short distances: if data is transmitted within Germany, foreign intelligence services are not allowed to intercept it.

This is a campaign about alleged protection from US intelligence agency surveillance activities, German newspapers, including the Frankfurter Rundschau, wrote: "Internet traffic that originates in and is destined to recipients in Germany is now only to be sent via lines and servers in Germany. In theory that is possible. What good does it do? Virtually none." On that at least the columnist was right about what some commentators interpreted as the end of the free Internet. But that is not what it is about. There is no sealing-off or censorship of traffic to Germany from other countries as there is in China. Telekom customers will, of course, continue to be able to use all the services they want, regardless where in the world they are from.

NATIONAL ROUTING IS A STANDARD PROCEDURE IN THE US

Internet traffic will of course continue to flow to the UK, the USA and elsewhere in the world, but there is no reason why data from Frankfurt to Berlin should be routed via London or New York. The issue is that data should not leave the jurisdiction in which it is created and processed, not even en route to its domestic destination. In the United States, national routing is applied routinely for a long time already and forms part of contractual arrangements between network operators and the government. If data does not leave the country, foreign intelligence services have no access to it – no legal access, at least. Data routing cannot prevent them from spying in Germany, but it is then illegal and may create diplomatic problems for the spies.

TECHNICALLY FEASIBLE AND POLITICALLY RIGHT

In routing, all market players aim to strike a balance between security and expense. Today, nation-al traffic is partly routed via other countries because large carriers with surplus capacities attract traffic by means of predatory pricing. Telekom has no influence on the routing policies of other carriers, but as it has the largest network in Germany, national routing is technically feasible and makes sense security policy wise – at least for its own customers. E-mail from a Telekom connection can be sent to a German T-Online address without detours via other countries. If other providers follow suit, data traffic within Germany can also be kept within Germany across providers. To implement this, one could also think of mandatory laws.

STATUTORY ARRANGEMENTS REQUIRED WITHIN THE EU

Routing tables are constantly revised, subject to changes in networks, free capacities and pricing. It is possible to take security policy objectives into consideration without major extra expense, but it would need to be legitimized politically. Telekom is well aware that its national routing proposal covers only a part – and maybe only a small part – of overall data traffic, and if the EU Member States were to agree on common regulations, a larger share of total traffic could be protected in the secure Schengen area. Some might see this as a marketing gag. Others see it as at least a good start, taking us forward from a shock and dismay debate to actually implementing new security measures. And any move toward greater security is clearly better than continued idleness.

NATIONAL ROUTING IS LARGELY IMPLEMENTED ALREADY

For Telekom customers, national routing has largely been implemented already. Domestic traffic is transported in Germany only. In exceptional cases, such as when bottlenecks occur, alternative routes via neighboring European countries are used. Telekom also has direct network connections with nearly all major national providers. If all providers adopt the same approach in their networks, we will have de facto national routing. This does not require any prior coordination with other providers, and the proposal neither changes the competition nor impinges on network neutrality.

INFECTION PROTECTION

To minimize the risk of infections brought into the system, Deutsche Telekom tries out a new scan station that checks mobile data carriers for possible virus infection only in seconds. The station is located in the main lobby of its Group headquarters in Bonn.

IT security managers break out into a cold sweat at the thought of more and more employees bringing their own data carriers to work and inserting them unchecked into company computers. Potential attackers find this laisser-faire attitude on the users' part more than convenient. The better a corporate network is protected externally, the more important USB sticks, SD cards and DVDs become as means of gaining access. Stuxnet is probably the best-known example. An employee of the uranium enrichment facility at Natanz, Iran, was "given" an infected USB stick and, hey presto, the attackers succeeded in gaining access to the nuclear facility's control technology even though it was, technically speaking, totally sealed off from the outside world.

TEST RUN FOR SCAN STATION

Since the fall of 2013, Telekom has been trying out a user-friendly testing device for mobile data carriers. The scan station is in the lobby of Telekom's Bonn headquarters to which the public has access. Along with employees all visitors are invited to have their mobile data carriers checked. The scan station's wooden stand has a touchscreen that asks the user to insert his or her mobile data carriers. There are slots for USB sticks, SD cards and DVDs. The scan station then checks them automatically for all manner of malware. The search algorithms used are from four providers of antivirus software.

The scan station checks USB sticks, SD cards and DVDs for malware.

The scan station evaluates data stored on the data carriers locally. Users are notified of the results via the touchscreen. If the scan station identifies malware, it offers to remove it. If disinfection will require data to be deleted, the user is informed beforehand. The owner of the data carrier is in charge of the situation at all times and is free to decide the extent to which he wants assistance.

Two worlds, one Smartphone: with the SiMKo 3 you can make encrypted phone calls and still surf the Internet.

HIGH-SECURITY MOBILE COMMUNICATION

The Federal Office for Information Security (BSI) has sucessfully tested the SiMKo 3 security smartphone and has approved its VS-NfD (short for "Classified – For Official Use Only") security rating in September 2013.

Members of the federal government and Ministry, and federal agency employees now have at their disposal for the first time a mobile device for especially confidential messages that is based on the newly developed L4 high-security microcore as its operating system. In October 2013 the Smartphone version of the SiMKo 3 was followed by a tablet prototype based on the Samsung Galaxy Note 10.1.

SiMKo 3 is not just for data applications such as e-mail, calendars, contacts and tasks. It can already be used as an interception-proof crypto telephone for encrypted calls based on Voice over IP and high-security encryption methods. In addition, it will shortly be authorized for use by federal agencies for the official SNS (secure cross-network voice encryption) standard. If a device is lost, nobody can see what is stored on it. Its certgate crypto card ensures that users must authenticate themselves and encrypts all data on the device. Its contents can also be deleted remotely.

Both devices run securely on the same platform so that no extra outlay and no investment in a second infrastructure are required. For the SiMKo 3's core and its security technology Telekom relies wholly on German companies. The crypto card is from certgate and the encrypted connections are delivered by NCP. Both are companies based in Nuremberg. The L4 microcore system was developed by TU Dresden, the Dresden start-up Kernkonzept, Telekom's Innovation Laboratories and the Berlin start-up Trust2Core. Implementation of the core was made possible by especially close collaboration with world market leader Samsung.

PUBLISHING INFORMATION

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

Photos

Deutsche Bahn,
Deutsche Telekom,
Fotolia, iStockphoto

Date of publication: 1/2014

www.telekom.com/dataprotection

www.telekom.com/security