Life is for sharing.

CONTENTS

"This is about preserving our high level of privacy in Germany," says **Professor Hansjörg Geiger**, member of the Data Privacy Advisory Council, in an interview.

21

Rapid response unit – Deutsche Telekom's CERT coordinates management of security incidents for all of the Group's information and network technologies.

26

Mobile devices are being targeted increasingly by cyber criminals. Companies should learn from the attackers.

42

Allianz für Cyber-Sicherheit

Cyber security alliance – More effective protection through cooperation, demands **Michael Hange**, President of the German Federal Office for Information Security (BSI).

46

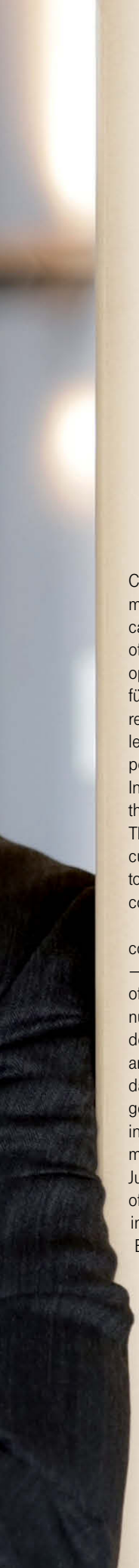
Customer service on the cyber front. Telekom's Abuse Team is the contact point for anyone who wants to report abuse of Internet services. The security experts followed up on more than one million reports in 2012.

44

“We have to tear down walls.”

At peak times, Deutsche Telekom’s IT systems register 400,000 digital attacks a day. Telekom is consistently enhancing its data privacy and data security level to ensure the attackers do not succeed.

Dr. Thomas Kremer, Board member for Data Privacy, Legal Affairs and Compliance



Customers seem to recognize this commitment to data privacy and data security. This can be seen from the representative results of the 2012 security report by the German opinion and market research institute Institut für Demoskopie Allensbach. According to this report, Telekom enjoys a significantly higher level of trust in relation to the handling of personal data in the telecommunications and Internet industry. As many as 45 percent of the population consider Telekom trustworthy. This result is outstanding in an industry where customers' personal data has to be dealt with to such a large extent — even more so as competitors are lagging well behind.

Telekom plans to continuously reinforce its commitment to data privacy and data security — something that is crucial not only in terms of the increasing threat from cyberspace. The number of Internet attacks has practically doubled within just one year. There are now around 100,000 new types of malware each day. As digital weapons become more intelligent, professional hackers are attempting to infiltrate the IT systems of companies, government organizations and private individuals. Just how far this can go was proven at the end of November 2012 when hackers successfully infiltrated the server of the International Atomic Energy Agency (IAEA), stealing and publishing confidential e-mail addresses.

Although security experts at Deutsche Telekom are constantly developing methods that have allowed them to detect and successfully prevent such attacks sofar, we cannot rest on our laurels. However the battle against cyber attacks cannot be won by acting alone — and there is consensus on the Management Board about this. Therefore we are not hiding behind a wall of silence and relying on the principle of hope. We are at the forefront of a movement that, together with other companies and national security agencies, will do everything possible to confront the dangers of a networked society. We make attacks on our systems transparent, unlike practically every other company. In this way we aim to share our knowledge and

> "Trust is the basis for successful business!"

thereby enable others to introduce suitable counter-measures more expediently. After all, 90 percent of attacks are avoidable if systems are kept up to date.

Yet many companies still shroud themselves in silence for fear of losing face. What advantages do they gain by concealing information about cyber attacks on their own systems? None! We all know that any of us could be a victim of a cyber attack. We therefore have to tear down the walls of silence! In the long term Germany can only protect itself effectively against digital threats by collaborating. This starts with very practical measures. We plan to set up a joint and independent test center with other companies in the IT and telecommunications industry — even our competitors. All companies involved could use it to test the security of critical network components against digital attacks. If the German Federal Office for Information Security (BSI) were to participate in such a test center, then this could even translate to an official security seal for technical products.

Technology for greater data security is just one side of the coin, however. Data privacy still requires a lot more attention. While the data privacy level in Germany and some European countries is very high, we urgently need consistent global rules on data privacy. This relates to more than just equal competitive opportunities. It is the only way we can win the trust of customers and help digital business models to succeed in the long term. Deutsche Telekom is leading the way in data security and data privacy. That said however, we will not cease to reinforce our customers' trust. New business areas such as cloud services and intelligent networks for power supply or the healthcare industry will only succeed, if customers can rely on secure solutions.

Dr. Thomas Kremer
Board member for Data Privacy,
Legal Affairs and Compliance

About the author

Dr. Thomas Kremer has been the Board of Management member responsible for Data Privacy, Legal Affairs and Compliance at Deutsche Telekom AG since June 2012. He was previously employed as General Counsel for ThyssenKrupp AG, where he took over as head of the Legal & Compliance Corporate Center in 2003 and was made Chief Compliance Officer of the ThyssenKrupp Group in 2007.

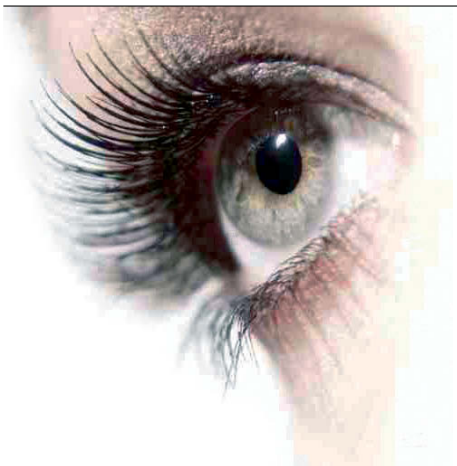
Customer data privacy in Sales

DEKRA accolade for Telekom Shops third year in succession.

High levels of awareness and expertise in handling customer data are paying off. As in previous years, the technical inspection agency DEKRA conducted a succesfull audit of the Telekom Shops in 2012. All Telekom Shops have earned the right to use the DEKRA seal of data privacy and data security according to the German Federal Data Protection Act for another year. For the first time, DEKRA experts visited around 150 shops without prior notification. The audits essentially covered two areas: On the one hand, the auditors examined security in retail shops.

For example, they checked whether customer data is adequately protected against theft or loss. On the other hand, DEKRA examined the handling of customer data in accordance with data protection regulations. The Telekom Shops plan to increase the data privacy level achieved even further.

As in previous years, the technical inspection agency DEKRA gave the Telekom Shops a successful audit in 2012.



Data privacy is put to the test with extensive internal audits.

With our own eyes

Internal audits show sustained improvement in data privacy worldwide.

Deutsche Telekom inspects the data privacy level across the Group by means of extensive self-auditing. Group Privacy performed a total of 60 internal audits in 2012. As in previous years, audits focused on mission-critical applications and processes as well as on data privacy in individual national companies and subsidiaries. The audits aim to identify vulnerabilities and resolve them using suitable technical and organizational measures. Furthermore, Telekom gains robust knowledge of how the data privacy level is developing throughout the Group.

The basic data privacy audit supplies the largest range of indicators. This is an annual survey in which more than 36,000 employees from 35 national companies took part in 2012. The audit clarifies how employees assess the level of data privacy in their working environment, whether they are familiar with data privacy processes relevant for their work, and to what extent they use the specified tools. The indicators established in 2012 show that awareness and expertise in handling personal data in the Group have continued to increase on an international level. In the case of Germany, the audit confirms very high awareness of data privacy.

Proven quality

TÜV NORD certifies Deutsche Telekom's billing processes.

Telekom produces around 65 million invoices per month in the fixed network and mobile communications segments. Hundreds, often even thousands of data traffic items at different rates have to be billed to the exact time for every customer. This is a highly complex task that extends from initial collection and preprocessing of data to actual billing through to writing, delivery and archiving of invoices. Many different IT systems work together for this purpose in fixed and mobile communications. TÜV NORD audited the entire process chain and its integrated systems in 2012. The auditors assessed both data privacy and the IT security of the billing process. While the fixed network area succeeded in renewing its 2010 certificate, the mobile communications area was awarded the TÜV seal for the first time.

TÜV Rheinland certifies external call centers

All Telekom partners successfully pass audits.

Telekom's call center service providers confirmed their high level of data privacy again in 2012 according to TÜV Rheinland. All audits had positive outcomes. While the 14 hotline providers received a new TÜV seal, the 17 call center companies deployed in sales renewed the seals they had been awarded in 2010. The two-year cycle is part of an auditing concept that TÜV Rheinland has developed together with Telekom. The seal, which was developed in 2009, is the only one of its kind in the German call center industry. In addition to TÜV Rheinland's audits Telekom performs its own internal audits if data privacy related changes are identified with the partners. In particular, risk management will initiate audits in sales and service when new providers commence work. The same applies for call center partners that establish additional locations or take over additional services. Telekom performed 22 such audits in 2012.

Federal Network Agency audits Münster data center

Customer data privacy in mobile communications.

Is Telekom doing everything in its power to protect the data of its mobile communications customers? The answer to this question is by no means to be found only in call centers and Telekom Shops. The data centers that operate software for customer relationship management (CRM) also have a major stake in ensuring optimal data privacy. In September 2012 the German Federal Network Agency audited the Münster data center in which Telekom hosts CRM software for its mobile communications arm.

To ensure data privacy, the audit focused on two major topics. In terms of daily business, the Federal Network Agency monitored whether Telekom processes, stores and deletes billing-related call data records in compliance with the law. In addition, the auditors examined how the administrative area is protected against abuse. The Federal Network Agency indicated its approval for the approach of the Münster-based data center in all respects.

Better quality of life for older people through use of intelligent equipment and systems.

Independent living in old age

Telekom develops data-privacy compliant communications systems as part of the SmartSenior research project.

To create technologies that enable older people to live independently in their own homes for as long as possible, 28 partners from industry and science joined forces in the SmartSenior project, which was supported by the Federal Ministry of Education and Research (BMBF). The result of the joint undertaking is the SmartSenior system. SmartSenior creates intelligent living environments for the elderly with its easy-to-use healthcare, security, service and communications solutions. The communications centerpiece is the TV set with add-ons such as touchpad, smartphone, room sensors, camera, medical measuring equipment and an intelligent wrist-watch. Telekom Innovation Laboratories coordinated the overall project and developed a number of subsystems. For example, a communications solution that alerts employees in a connected assistance center when sensors detect a risk situation in a home and there is no response from the resident. Solutions of this kind will only find acceptance when data privacy is also taken into consideration. Within its own sphere of responsibility, Deutsche Telekom produced process descriptions that were used as a basis for a data privacy concept developed together with its partners. The concept ensures compliance with all currently applicable data privacy provisions of the states of Berlin and Brandenburg and the German federal government as well as the regulatory requirements for clinical studies. Telekom's data protection advisors will also monitor future projects arising in connection with SmartSenior.

Deleting data for advanced learners

Telekom develops audit-proof solution for deleting employee data in SAP software.

Deletion of personal data is subject to particularly strict requirements in the area of human resources. To act in a compliant manner, a corporation such as Deutsche Telekom has to observe numerous legal regulations as well as a range of operational provisions. This is no trivial task, especially as retention and deletion periods can vary greatly depending on the word-ing of the law. Telekom analyzed the relevant requirements in 2012 and developed an audit-proof concept for deletion of personal data in SAP HR, the central software system that is used by Telekom's HR department to manage its tasks. The HR management software processes the monthly salaries of more than 120,000 employees with the principle client alone. The deletion module offered by SAP reached its limits when it came to implementing the deletion concept. Telekom therefore decided to additionally develop its own solutions. At corporate level, the new deletion concept is the first of its kind. An exchange of experience already took place with the German Federal Ministry of Transport and a number of DAX-30 companies where human resources departments face similar challenges. In addition, Telekom is in talks with German federal and regional authorities that are responsible for employee data privacy.

Go-ahead for De-Mail

Secure e-mail infrastructure for citizens, businesses and authorities.

Deutsche Telekom launched the secure mail service De-Mail in August 2012. Consumers and businesses use the new service to send digital documents confidentially. The basis for this is the German De-Mail Act. Secure login procedures, encrypted transmission and send and receive confirmations enable secure and verifiable electronic communication. Third parties can neither see nor manipulate messages. As the De-Mail Act places stringent demands on security and data privacy, providers have to go through a strict accreditation process. Only then are companies approved as De-Mail service providers by the Federal Office for Information Security (BSI). Deutsche Telekom has successfully completed the accreditation. Since March 2012, Telekom Deutschland and T-Systems International have been officially approved De-Mail providers.

Rapid response

Telekom branch office destroys illegally collected health data.

Managers at a Deutsche Telekom Technik branch office in the German city of Bayreuth were requested internally in January 2012 to record health and performance data on employees. This request was in breach of legal provisions and internal requirements with respect to the handling of employee data. As soon as this became known, existing lists were destroyed completely. The rapid intervention was initiated on behalf of the local works council. Disciplinary action was taken by Telekom against the employee who initiated the list.

TV just got smarter

Telekom introduces statistical evaluation of Entertain usage data.

With Web-TV, media libraries or TV archives, viewers can freely decide when and on what device to use their chosen format. The more this environment changes, the more important it is for suppliers to get to grips with changing consumer habits. This also applies to Telekom's web-based Entertain solution. Telekom has been collecting usage statistics since July 2012 in order to further enhance the product quality of Entertain. Interest here focuses on which programs are viewed by preference and which contents are being retrieved from the video library. Deutsche Telekom presented the process for evaluating usage data to the Federal and State Commissioners for Data Protection and Freedom of Information and addressed the alleged criticalities. Technical and organizational role concepts ensure that no conclusions can be drawn regarding individual customers. In addition, every customer is free to prevent evaluation of his or her data at any time. Deutsche Telekom informed its customers back in June by e-mail and a screen message in Entertain of its plans to collect the data and their option to opt out. This ensured that customers could object before statistical evaluation of usage data began.

Analyses of Entertain usage patterns do not allow conclusions to be drawn about individual customers.

“It’s high time.”

The European Commission presented its new draft Data Protection Regulation for the European Union (EU) at the end of January 2012. This regulation is planned to come into force at the start of 2014 and will then be directly binding after a transition period.

Dr. Claus Ulmer has been Group Data Protection Officer of the Deutsche Telekom Group since July 2002.

Some opposition can always be expected when legislators introduce new regulations, and this is no different in the case of the EU Data Protection Regulation. Especially in countries where governments have less stringent data protection laws, criticism of the draft with its 91 articles continues unabated. How does Dr. Claus Ulmer, Group Privacy Officer for Deutsche Telekom, rate the initiative from Brussels?

Dr. Ulmer, can you sympathize with criticism of the draft of the EU Data Protection Regulation?
Dr. Ulmer: First of all, the initiative by the European Union is very welcome and also urgently needed. We need uniform data protection legislation throughout the EU. Multinational corporations like Deutsche Telekom in particular need the legal certainty provided by uniform and reliable rules. By and large, the present draft is a success because it takes account both of current technical developments in the area of data processing on the Internet and also the aspect of international networking. We believe there is still scope for discussion however with regard to some aspects. For example, regulating the responsibility of supervisory authorities in terms of a one-stop shop as envisaged in the draft makes sense. However, the text of the regulation still has to be adapted to the extent that multinational corporations with numerous legal units are also clearly covered by the regulation and can therefore profit from it. Within the overall perspective of the current draft regulation, however, the advantages of a uniform European data protection standard predominate by far. I am convinced that the EU is setting standards with the EU Data Protection Regulation and all other countries will likewise gradually pursue a higher level for their data

privacy. We have recently seen examples of this in Malaysia and Singapore.

Some companies are of the opinion that self-regulation should suffice?
Dr. Ulmer: Self-regulation would not be very helpful, for who is to monitor it. Also, different self-regulation initiatives would not allow the same level of uniformity to be achieved with the standards as is possible with the planned regulation. We ourselves have been able to live quite easily with the strict data protection requirements of the German Telecommunications Act (TKG) as well as the German Federal Data Protection Act (BDSG) for many years now – in fact at Telekom we even go further than the legally prescribed requirements in some respects. Moreover, past experience shows that self-regulation processes can be too lengthy. A discussion process generally kicks in first of all before binding contents can be discussed at all. However, this impedes fast and flexible business transactions with other companies, such as in the case of cloud offerings. In addition, the self-regulation approach often leads to confusion among consumers as to what is actually desired or intended. I therefore view clear and generally binding conditions as especially important as the basis for optimum flexibility for companies. This opportunity has been opened up by the EU Data Protection Regulation.

What will be new in some countries is that companies with more than 250 employees have to nominate a data privacy officer. Is this not long overdue?
Dr. Ulmer: Absolutely, there should be a neutral and independent body in every company for assessing issues arising in relation to data privacy. This body has to specify the rules for complying with data protection requirements, check their compliance and intervene where necessary without fearing detrimental effects in the company. Deutsche Telekom takes the role and powers of the data privacy officer very seriously. The data privacy officer enjoys independent and paramount authority in this Group in his or her specialist area and in this respect exerts direct influence on entrepreneurial decisions. The rules set out in the draft regulation should be based on German statutory rules and should at least also attribute the position of an independent supervisory body to the internal data privacy officer so that the position can be meaningfully implemented. From the perspective of Deutsche Telekom, the appointment of a data privacy officer for companies should also be accompanied by privileges

> "Deutsche Telekom takes the role and powers of the data privacy officer very seriously."

at the level of the EU regulation. We therefore support the proposal to dispense with registration and notification requirements in the appointment of a data privacy officer or at least to identify the data privacy officer as the role responsible for this as opposed to the supervisory authority.

How can an internal data privacy officer be neutral? As an employee, is it not more a case of "He who pays the piper calls the tune"?
Dr. Ulmer: I reject this perception most emphatically. Germany has a unique data protection law that defines our duties and rights and to which we as data privacy officers are bound. Our actions are of course also guided by the interests of the company. But not only by these, rather also by the interests of those affected by data processing. A solution that is viable for those involved must be developed here. Our understanding of the role of a data privacy officer is reflected to an extent in the draft of the EU Data Protection Regulation. As already indicated, the draft requires further reworking in terms of the supervisory body implementation and the assurance of sufficient resources to perform the work required. The data privacy officer must report directly to corporate management and greater protection against dismissal must be provided also following termination of tenure so that the data privacy officer can act independently and fulfill his or her duties as an operative supervisory body.

Article 36 of the draft EU Data Protection Regulation states that the company shall ensure "that the data privacy officer is involved properly and in good time in all issues relating to the protection of personal data." How does Deutsche Telekom ensure this today?
Dr. Ulmer: The Privacy & Security Assessment Process introduced in the Group states that as data privacy officers we must be involved in decision and development processes together with IT Security. Thus, for example, when new products and services are scrutinized with respect to data privacy-related aspects. Only when we have received approval under data protection law will such projects be assigned additional budgets. Our department has a staff of over 60 at Headquarters in Bonn alone in order to manage the approval processes. In addition to this there are employees who monitor and assess implementation of data protection measures both locally and also at all other locations outside of Germany.

The draft EU Data Protection Regulation also stipulates that data privacy violations be reported. Is this ruling fit for purpose?
Dr. Ulmer: This is already applicable law in Germany and therefore mandatory for us. It is to be welcomed that this will now become uniform law in all member states. However, I expect that the EU will define precise thresholds above which a company will have to report an incident. Otherwise this point will remain too vague.

Why a threshold? Should every data privacy violation not be reported?
Dr. Ulmer: We already report and publish all occasions in compliance

with legal requirements on the Internet. However, the question arises as to whether less might be more here. Experience from the U.S. shows that tedium sets in when ev-ery incident is reported and published. Sooner or later the public stops paying attention to these incidents. We have to consciously tackle this risk of overkill caused by information overloading. Data privacy thrives on being noticed and its ability to contribute to a shift in thinking.

Do strict data privacy laws also lead to competitive disadvantages in some cases?
Dr. Ulmer: Deutsche Telekom is convinced that it will have long-term competitive advantages if it complies with the required data privacy and carries out trust-enhancing measures. In the spirit of our mission "Creating an environment of trust" we are firmly resolved to strengthening and steadily improving the trust our customers, the public and our employees have placed in Deutsche Telekom. According to the EU regulation, all products and services should be automatically made data privacy friendly at the time of delivery or when they are first used. This means then that only as much data is collected, processed and disseminated as is absolutely necessary for use.

"Deutsche Telekom is convinced that it will have long-term competitive advantages if it complies with the required data privacy and performs trust-enhancing measures."

How does Deutsche Telekom do this today?
Dr. Ulmer: We have fulfilled this requirement for some time, since the Telecommunications Act and the Telemedia Act provide clear instructions in Germany. We welcome the fact that customers are actively made aware of data privacy aspects and have to declare their willingness to use data. Only then can they make differentiated decisions. An example of this are apps. If you disable location services on the smartphone, the app that requires the positioning data will ask on next usage whether you want to activate the location service. This is just a small example of data privacy in practice.

A company has to respond in writing to consumer queries within one month free of charge.
Dr. Ulmer: ...and we are generally even faster than four weeks. However we also want to further improve the process of actively providing information. The Internet offers us additional opportunities here, for example by incorporating explanations of terms. In this context it will also be the case that we provide more specific data privacy information tailored to the respective product.

The right to delete data should be introduced. This also includes the obligation to inform third parties of the request for deletion. How would Deutsche Telekom feel about that?
Dr. Ulmer: We have no problem with this, since we have also been doing this for some time. When customers switch to a competitor, we delete their data. If someone wants to be deleted from the electronic phonebook then we also request Google, for example, to delete the entry from the cache. The difficulty would only then arise if the provider were to be required to ensure full deletion of all data. This cannot be demonstrated technically in many cases. Commercially justifiable efforts must then suffice. I see it differently however if people enter data themselves on the Internet. We can support them within our sphere of responsibility but I am basically of the opinion that the originator must seek deletion apart from that.

"We have fulfilled this requirement for some time as the Telecommunications Act and the Telemedia Act provide clear instructions in Germany."

Article 20 of the EU Data Protection Regulation states that companies may only produce behavioral profiles of their customers if expressly permitted to do so. Is this bad for Deutsche Telekom?
Dr. Ulmer: Not at all, we have long since had a permission clause for advertising and market research purposes. There are companies however that use cookies that consumers do not notice. This procedure is referred to somewhere in the data privacy statement but who reads general terms and conditions of business or data privacy statements. Cookies record the pages someone visits on the Internet. Providers therefore get to know a person's interests, correlate them and use this profile for targeted advertising. Greater transparency should be offered here for customers in my opinion. Deutsche Telekom also behaves transparently and in a customer-friendly manner in this context.

How do you propose to take your customers with you on the journey?
Dr. Ulmer: There are many possibilities, starting with this report on data privacy and data security. However I would like to address concrete planning. It is increasingly difficult for customers to orient themselves in the present online and smartphone world. Data privacy settings are often difficult if not impossible to find or it is very difficult to understand how they are implemented. We therefore want to develop our privacy button for different application areas. We have already done this for anonymizing IPv6 addresses. In the case of smartphones, this could be an app for example, which provides the user with knowledge and – more importantly – control of data flows.

Dr. Claus Ulmer is Group Data Protection Officer of the Deutsche Telekom Group since July 2002. Having studied law in Tübingen and Munich and being awarded a doctorate from the University of Tübingen, Ulmer was employed as a lawyer from 1993 to 1999 in a Stuttgart law firm where he focused on employment law. From 1999 to 2002 Dr. Ulmer was a legal adviser with international responsibilities at debis Systemhaus before taking over the function of Data Protection Officer from January 2001. From August 2001 to June 2002 he was head of Data Protection at T-Systems International.

Uniform data privacy for the EU

The EU Data Protection Regulation is to replace the Data Protection Directive that came into force in 1995 and should standardize data privacy law in the EU member states. The regulation will then become valid throughout the EU with immediate effect and cannot be amended by national law. Reaction to the draft presented in

January 2012 varies. BITKOM essentially welcomes the EU-wide consensus of data protection authorities as well as the planned self-regulation of the economy. However the high-tech association criticizes some of the requirements, arguing that they cannot be implemented at all in the companies or only with considerable effort. The Federal Government requires leeway for national implementation and opening clauses. The Ministry of the Interior lists a number of regulations that have not been mentioned to date in the EU regulation, including those for video surveillance or transferring data to credit agencies.

More stringent reporting requirements

Telekom has complied with new requirements of the Telecommunications Act (TKG) for several years.

Since March 2012, telecommunications providers have had to report data privacy violations even in cases where employees delete or modify data without permission. The supervisory authorities must be notified of all incidents of this type, while consumers have to be informed of cases that lead to serious impairments. With the additional notification requirement, the Telecommunications Act creates greater transparency in the telecoms industry. Prior to this, providers only had a duty of notification if data was made available without permission to third parties, such as through loss or theft. With the new regulation, the Telecommunications Act now goes beyond the requirements of the Federal Data Protection Act (BDSG). Telekom has been able to implement the new reporting requirement straight away since it has already been voluntarily reporting data incidents for several years.

Transparency for the telecoms industry.

Telecommunications Act amendment ends competitive disadvantages

Equal opportunities

Legal amendment allows worldwide processing of telecommunications data.

With the 2012 amendment to the Telecommunications Act the Federal Government has removed a provision that had caused telecommunications companies considerable competitive disadvantages. In recent years, transmission of personal data to non-EU states was only permitted in exceptional cases. The Telecommunications Act went far beyond the level of regulation of the Federal Data Protection Act in this respect. In March 2012, the industry-specific provision in the Telecommunications Act became obsolete. Since then, the provisions of the Federal Data Protection Act have also applied to telecommunications providers. This means that completely new operating models are now possible. As with other companies, Deutsche Telekom can now involve partner companies worldwide, for example, in the remote maintenance of its systems. With service technicians cooperating across a number of continents, 24-hour services can now be offered in line with the follow-the-sun principle. The data privacy level that has existed to date remains unaffected: Telekom obligates all non-European partners to the same high protection standards as exist within Europe. Lowering of the data privacy level for customers is thus precluded.

Greater legal security

Federal Network Agency publishes guidelines for storing traffic data.

How long may and should telecommunications companies store their customers' traffic data? Reliable answers are provided in guidelines issued in September 2012. Based on specific recommendations, the Federal Commissioner for Data Protection and the Federal Network Agency indicate which retention periods provide suppliers and consumers with legal certainty. Apart from traditional telecommunications data, the guidelines deal with traffic data that can be collected in e-mail and Internet traffic. Providers use this data primarily for accounting purposes with their customers and other network operators. In addition, however, traffic data can also be used in incident management.

Graded by data category and intended use, the guidelines make recommendations as to when it makes sense to delete traffic data earlier than required by the Telecommunications Act. Telekom already complies with most of the recommended deadlines or even comes in ahead of them (see chart). Only in two areas does Telekom come in above the guide values of the supervisory authorities, but still within the legally defined deadlines. In both cases, this involves data that Telekom maintains in anonymous form for external service providers where these providers grant their customers an objection period of 180 days. The retention periods can potentially be amended during renegotiation of service contracts.

Data retention – Open-ended

While the EU directive is being evaluated, re-regulation is not foreseeable in Germany.

The Federal Government did not reach a consensus in 2012 on the re-regulation of data retention. Activities were reported on the other hand at European level. Following examination of the EU Data Retention Directive, there seems to be a trend toward reducing the minimum retention period to three months. The current directive requires periods of between six and 24 months.

Deadlock in Berlin

Political disunity continues in Germany regarding how a new legal regulation should be implemented. In 2010, the German Federal Constitutional Court declared the federal law to be unconstitutional. Two different potential solutions are being discussed at present by the Federal Government. While the Ministry of the Interior favors a six-month data retention period, the Justice Ministry is calling for the so-called quick-freeze approach in combination with a short data retention period. In the quick-freeze approach, telecommunications companies prevent the intended deletion of traffic data in individual cases when an authorized authority indicates its desire to retrieve this data within a certain period. In addition, IP address data is to be stored for seven days in any case.

Deutsche Telekom fulfills requirements for storage of traffic data.

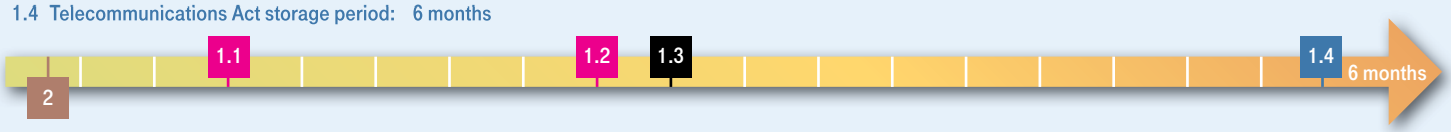
Deutsche Telekom already stores IP address data for seven days in order to be able to effectively combat malware (see chart). This is done in compliance with Federal Network Agency guidelines for the storage of traffic data. Should the Federal Government opt again for a six-month retention period, Deutsche Telekom can at any time return to the practice in place up to 2010.

Lawsuit because of non-implementation

The European Commission has taken Germany to the European Court of Justice for failure to implement the directive. Penalty payments of EUR 315,000 per day of non-compliance are under discussion. They will only fall due, however, from the effective date of a judgment. Exactly when the judgment is expected was not clear at the end of 2012.

Data protection-compliant storage of traffic data

1. Billing data other than for flat rates
1.1 Telekom storage period: **Up to 30 days** (if customer does not require itemized bills)
1.2 Telekom storage period: **80 days** (if customer requires itemized bills)
1.3 Guideline storage period: **3 months**
1.4 Telecommunications Act storage period: 6 months



2. Mobile network IP addresses and location data (except for location-dependent cellphone tariffs)
2.1 Telecommunications Act storage period: Not specified
2.2 Guideline storage period: 7 days
2.3 Telekom storage period: 7 days

Deutsche Telekom sometimes deletes traffic data sooner than the German Telecommunications Act requires.

Source: Deutsche Telekom

My house in cyberspace

New Internet portal explains work of geodata services for consumers.

Since September 2012, Internet users have had a central point of contact that is responsible for data privacy in connection with geodata services. This includes services such as Google Street View, for example. Consumers can go to the website **www.geodatendienstekodex.de** and find out how the services work, whether their house is captured and what rights they have. The new information service is based on the work of a registered society for self-regulation in the information economy, "Selbstregulierung in der Informationswirtschaft e.V." (SRIW). Founded in 2011, SRIW is an alliance of eight leading service providers, among them Deutsche Telekom, which provides about one third of the society's funding.

The Privacy Code of Conduct for geodata services is at the top of SRIW's agenda. Under this code, providers of geodata services are obliged to ensure transparency for consumers and provide information and an opportunity to object. In essence, providers commit voluntarily to make any image material used digitally unrecognizable in case of objections. Telekom is committed to the code of conduct because it links its own websites with external geodata services. While the Das Örtliche telephone directory service links to maps and images from Microsoft Bing Maps, the ImmobilienScout24 portal uses the Google Street View panorama service.

Privacy Code of Conduct for geodata services commits to transparency and information.

Urgently needed

Employee data privacy needs clear legal basis.

Reform of employee data privacy is seen by Telekom as a matter of urgency. The legal situation companies are finding themselves in regarding employee data privacy has been unclear for too long. Telekom committed itself to strict self-regulation in the wake of the spying affair. Now, following a lengthy period of inactivity in the legislative process, a new draft bill was introduced in January 2013, which might be passed during the course of the year.

The proposed new legislation addresses some of Telekom's requirements. For example, the draft for the first time contains a regulation on data transfer within corporate groups and also takes account of the corporate need to conclude commissioned data processing agreements with companies in third countries with a recognized high level of data protection. This saves resources and provides legal certainty. The proposed new legislation prohibits secret video surveillance. Open video surveillance remains possible under certain conditions. Use of covert video surveillance techniques has been banned at Telekom for years under a Group works agreement. Likewise, use of video surveillance for quality assurance purposes is also prohibited at Telekom. All in all, video surveillance at Telekom is only used to protect buildings and property.

Unfortunately, the new proposed legislation contains no provisions regarding modern and innovative forms of communication such as "bring your own device" or use of private devices for business purposes. It remains to be seen whether the legislator will still address proposals in this regard put forward by Telekom.

Informational self-determination in practice

Deutsche Telekom introduces data privacy standard for anonymous surfing under IPv6.

In tandem with the rollout of the new IPv6 Internet protocol, Telekom has launched a data privacy solution on the market that allows IP addresses to be reliably obscured. Users can themselves decide the extent to which they want to make the identities of their terminals anonymous. The new solution has been available since September 2012 and is the first of its kind in the telecommunications industry.

The new IPv6 Internet protocol provides 340 sextillion IP addresses – enough to supply all conceivable terminals with their own ID. This would make it technically feasible to create detailed profiles of users and their movements. Telekom's data protection standard mitigates against these consequences. The solution model includes three mechanisms that impact the traceability of IP addresses to a varying degree. For example, Internet users are to be able to request a new prefix for their router's device address at any time by simply clicking a button.

The new data protection solution is already fully available on the network side. Every time customers disconnect, they are assigned a modified IPv6 prefix and a new IPv4 address when they reconnect. The new routers in the Speedport W 724V series enable Telekom customers to set up anonymous surfing in line with their individual requirements. Telekom plans to continuously develop the new data protection standard.

Do-Not-Track standard postponed to 2013

Solution for enabling technical implementation of EU Cookie Directive not yet available.

The objective of concluding work on the Do-Not-Track (DNT) standard by mid 2012 proved too ambitious. Discussions on a global web tracking standard were simply too complex. The responsible working group of the World Wide Web Consortium (W3C) has largely agreed on the technical design of the standard, whereby Web users can determine at the click of a mouse whether or not they want to allow themselves be tracked on the Internet. The real challenge, however, remained on the regulatory side. Since its inception in spring of 2011, the Do-Not-Track working group has been struggling over a common approach that would provide sufficient validity for the standards of all jurisdictions.

The core of the issue here is to harmonize U.S. and European consumer protection requirements. The Do-Not-Track initiative established a new task force at the end of 2012 with the aim of clearly establishing the upper limit of what is permissible for the European Union. Telekom is the only German company to be involved directly in the working of the W3C working group. As with the EU Commission, the Telekom data privacy experts regard Do Not Track as a suitable means to effectively implement the EU Cookie Directive adopted in 2009.

Fast-tracking implementation of the EU Cookie Directive.

Support for smart metering

While Germany is intensifying its commitment to data privacy, the European Union is actively involved in promoting enhanced data security.

Smart metering is one of the milestones on the path toward intelligent energy management. When remotely readable electricity meters supply consumption data around the clock, electricity suppliers and consumers benefit equally. Suppliers are provided with valuable information for managing their capacities and reliably maintaining network operation. Customers can keep track of their energy costs and use electricity primarily when it is most favorable to do so.

Data privacy for consumers

Since smart metering gives rise to the collection of personal consumption data, the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) applies. In order to further strengthen data privacy, the Federal Government instructed the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) to create a protective profile and a technical guideline. While the privacy profile has been available since November 2011, the guideline is expected at the beginning of 2013. The German Federal Office for Information

Smart metering needs a protective profile.

Security is focusing its attention on the control module attached to the meters. As a central communications platform between the meter and smart metering provider, the control module should act as a secure data container. The profile outlines requirements for a device architecture that ensures a high degree of data privacy. For example, the control module has to be able to encrypt and sign the consumption data in order to prevent unauthorized access. The requirements extend to the design of the transmitting device to also be equipped to deal with physical attacks or manipulation from outside.

Data security in network operation

While Germany concentrates on data privacy in the control module, the European Union has launched an initiative to strengthen data security in power grid operation. The European Network and Information Security Agency (ENISA) put together a working group in 2012 as part of which it drew up recommendations for adequate data security together with industry representatives including Deutsche Telekom. The recommendations point out the impact of data security on the stability of electricity production and indicate which minimum standards have to be maintained by future smart grid providers. For example, it is important to effectively exclude the possibility of attackers reporting incorrect consumption data to the grids so that operators misjudge the current grid load. An initial draft of the data security recommendations became available at the end of 2012. ENISA will have concluded its foundation work in 2013.

Trust edge among population

Telekom enjoys great credibility in handling personal data.

"Which companies do you regard as trustworthy when it comes to handling personal data?" On this question in a representative Allensbach survey, Telekom came out on top by a long margin among IT and telecommunications companies. 45 percent of those surveyed regard Telekom as trustworthy. The company in second place scored just 27 percent. Telekom takes the top spot in all age groups, but at 57 percent it enjoys an especially large trust bonus among the over-60s. The Institut für Demoskopie Allensbach carried out the representative survey as part of its security report in June 2012.

External advice welcome

Deutsche Telekom's Data Privacy Advisory Council advises the Board of Management and promotes exchanges with leading experts and personalities from the worlds of politics, academia, business and independent organizations on current data privacy and data security-related challenges.

The Data Privacy Advisory Council deals with a wide range of topics. It discusses business models and processes for handling customer and employee data as well as IT security and the adequacy of measures taken. It also examines international aspects of data privacy and the implications of new legal regulations.

Its duties include evaluating data privacy and data security measures at Telekom as well as developing proposals and recommendations for the Board of Management and Supervisory Board on relevant issues. The Board of Management can request the Data Privacy Advisory Council to assess data privacy-related processes in the Group. The Advisory Council also takes up data privacy and data security topics independently and elaborates suggestions or recommendations for Deutsche Telekom's Board of Management.

The Data Privacy Advisory Council met five times in 2012. Important topics included assessing data privacy and security aspects of new cloud applications as well as developments in the growth areas of energy and the connected car. The Advisory Council also dealt with the draft of the EU General Data Protection Regulation and the expected impact on Deutsche Telekom. It also advised on the evaluation of Entertain usage data and informed itself about the results of the basic data privacy audit and the data privacy level achieved in the Group.

The current members of the Data Privacy Advisory Council include:

Wolfgang Bosbach, CDU, member of the German Bundestag and Chairman of its Committee on Internal Affairs

Peter Franck, Member of the board of Chaos Computer Club (CCC)

Professor Dr. Hansjörg Geiger, Adjunct professor of Constitutional Law at Goethe University in Frankfurt/Main, State Secretary of the Federal Ministry of Justice from 1998 to 2005, former President of the German Federal Office for Protection of the Constitution and the German Federal Intelligence Service

Professor Peter Gola, President of the German Association for Data Protection and Data Security (GDD)

Bernd H. Harder, Lawyer and member of the Executive Board of BITKOM e.V., lecturer at Stuttgart Media University and Technische Universität München (TMU)

Dr. Konstantin von Notz, Bündnis 90/Die Grünen, member of the German Bundestag, member of the Committee on Internal Affairs and deputy member of the Committee on Legal Affairs and the Subcommittee on New Media, member of the Enquete Commission on Internet and Digital Society

Gisela Piltz, Member of the German Bundestag, Deputy Parliamentary Group Leader of the FDP parliamentary group

Gerold Reichenbach, SPD, member of the German Bundestag, member of the Committee on Internal Affairs (rapporteur for Privacy and Civil Protection and Disaster Assistance) and member of the Subcommittee on Civic Engagement, deputy chair of the Enquete Commission on Internet and Digital Society

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

Lothar Schröder, Chairman of the Data Privacy Advisory Council, member of the ver.di National Executive Board and Deputy Chairman of the Supervisory Board of Deutsche Telekom AG, member of the Enquete Commission on Internet and Digital Society

Halina Wawzyniak, Die Linke, member of the German Bundestag, Deputy Party Chair, member of the Enquete Commission on Internet and Digital Society

Professor Dr. Peter Wedde, Professor of Labor Law and Law in the Information Society at the Frankfurt University of Applied Sciences, Director of the Europäische Akademie der Arbeit (EADA) at the University of Frankfurt am Main

Trust gain

More than in scarcely any other industry, data privacy must play a major role in companies in the information, telecommunications and media sector. This applies primarily when processing of customer data is a key component of a company's business model. For example, Deutsche Telekom has data regarding who customers are phoning and for how long, which movies they are downloading from the online videoshop Videoload, or how they are using the music streaming service Spotify. Cloud computing is also giving rise to new areas in which Telekom as a cloud provider receives and processes its customers' data. This applies, for example, to the data that T-Systems stores in its data centers as a data processor for other companies. Added to this is personal information on around 230,000 employees in the Group.

The task of safeguarding data from contractual relationships for over 150 million lines is enormous in its own right. The scale and sensitivity of this data require that protection of personal rights be treated more importantly than anything else. Telekom has to protect this personal data from external access and against abuse by all technical means possible, using the know-how of its employees and the advice of external specialists. In an increasingly networked economy, this is an essential requirement for business success.

Facing the judgment of a critical expert community is an important step and shows that data privacy at Telekom is more than mere lip service. The Data Privacy Advisory Council plays a special role here in particular as an external observer and advisor. In addition, Telekom is one of the first international groups to have elevated the Data Privacy and Compliance area to Board level. All measures are used to build trust with regard to customers and employees as well as private and public shareholders in the Group.

The composition of the Data Privacy Advisory Council represents the political plurality of views in Germany, but also specialist know-how on various aspects of data privacy and data security. It subjects business models regularly to a neutral and critical view — sometimes even to the level of individual products and services. All current data privacy-related developments in the company are discussed openly. Telekom benefits in this way from the experiences of the members of the Data Privacy Advisory Council.

Following up privacy scandals has long since ceased to play a role in the sessions of the Data Privacy Advisory Council. Rather, its work is forward-looking and focuses much more on how to protect personal rights in the future. Internal Group processes are increasingly becoming a focal point for the Data Privacy Advisory Council. Special attention is also paid to new business areas such as healthcare, energy and the connected car. Personal data will accumulate in these areas on an as yet unknown scale and will have to be protected. Telekom's Data Privacy Advisory Council provides support for these endeavors.

All of the data privacy measures that Telekom has initiated and implemented in the past four years have changed the Group in a remarkably positive way. Telekom today is leading the way in data privacy and data security, and this is also reflected in terms of actual figures. According to a representative survey by German opinion pollsters Allensbach, 45 percent of the population regard Telekom as trustworthy when it comes to handling personal data. This is an astonishingly high figure if one considers the volume of personal data handled in the information, telecommunications and media industry. A look at the competition clearly supports this. The next competitor in line in the Allensbach survey was some 20 percentage points behind. Deutsche Telekom has worked hard to regain this trust and intends to not just maintain it in the future but also build on it. For this reason we remain closely involved in developments as Data Privacy Advisory Council and would rather be safe than sorry in ascertaining the consequences that certain actions or services have for protecting personal rights. Neither the high level of awareness nor the sense of shame about abuse should be allowed to diminish. This also applies when it comes to protecting employee data.

A Data Privacy Advisory Council is also suitable for other companies, however, especial when processing customer data is a key component of the business model. For these companies a Data Privacy Advisory Council should be an established best practice. It erects no barriers, but rather opens our eyes before customers themselves have their eyes opened at a later time with possibly negative consequences. So I can only recommend other companies to consider introducing a Data Privacy Advisory Council too.

About the author

Lothar Schröder is Deputy Chairman of the Supervisory Board of Deutsche Telekom AG and Telekom Deutschland GmbH. He has been a member of the ver.di National Executive Board since April 2006, with responsibility for "Innovation and good work" and for the "Master craftspersons, technicians, technologists and engineers (mti)" employee group. He also heads the Telecommunications, IT and Data Processing unit.

Think twice!

Anyone who wants to tackle data privacy and data security in an integrated manner has to ensure that their employees are also properly informed and trained. Telekom launched a number of information campaigns again in 2012.

It generally happens unwittingly and only rarely with criminal intent. Employees may open the digital door to external attackers or fail to observe security regulations. They should therefore be included actively in the practice of an effective security culture. This is the only way to ensure information security. This starts with awareness of any potential data privacy and data security risks. Alongside the usual online portals and training, Telekom decided in 2012 to launch an "advertising campaign" as well as lighthearted and practical information measures in a bid to ensure the material was not too dry.

Information protection in an instant

Many Telekom employees have to deal with business or personal information every day. It can therefore be difficult at times for employees to decide how confidential data should be treated or which data is subject to data privacy legislation. Telekom classifies personal data according to five data protection classes and business information into four confidentiality classes from open to strictly confidential.

For better understanding, employees can now use a well-structured data privacy disk, similar to a parking disc. It helps them to classify information and data correctly and quickly without having to know exact concept definitions. They can immediately identify the level of protection required and the protective measures they have to apply accordingly. In addition to a paper version, there is also an electronic version that can be accessed by employees on their PC desktops. The next step in 2013 is to produce a smartphone app.

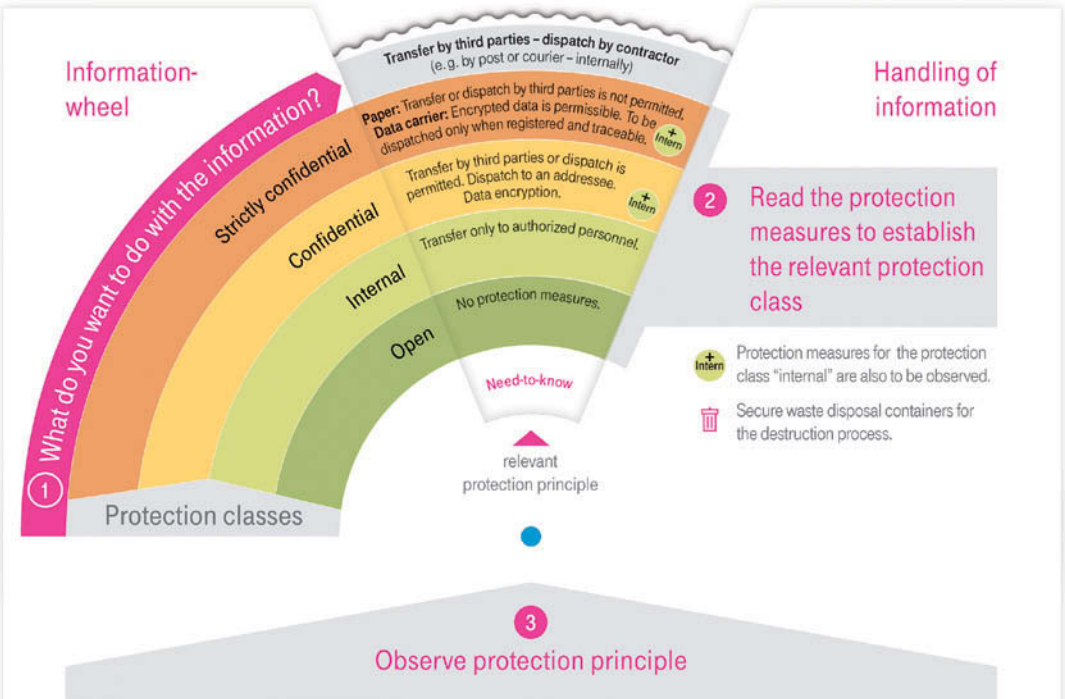
In addition, Telekom has developed a series of information sheets, which explain individual security rules concisely and comprehensibly. For example, there are overviews for secure use of data with smartphones or at external meetings. The topics and content are tailored to the different target groups, for example, members of a team, executives or organizational unit heads. However, this will not work without clear rules, which is why all Telekom employees have to commit to compliance with data and information protection regulations every two years.

Campaign against social engineering

Social engineering is a particularly clever way to acquire confidential information about a company. The attacker deceives the employee by using a false identity. Fake phone calls by an alleged technician requesting confidential access data would be an example of social engineering. Meanwhile, phishing is an electronic variant of social engineering. A typical example of this is spying on PINs and TANs in online banking.

Social engineering represents a major potential threat for Telekom since all employees can be affected by it. Creating awareness among employees is therefore one of the most important steps toward preserving information security and data privacy. To protect themselves, however, employees have to understand the attack mechanisms theoretically and to practice defensive behavior. Social engineering, after all, relies on basic innate mechanisms of human information processing and on emotionally controlled, non-reflective behavior. Who wants to prevent the friendly technician coming into their office when all he or she wants to do is fix a problem? Employees have to learn in such situations to take their time, deliberate and respond correctly.

Telekom launch the internal company campaign entitled Think Twice! in 2012. The objective was to convey to employees the correct gut feeling for threatening situations. And the message "I won't allow myself to be put under pressure, misled or taken in." The campaign, which is to be continued in 2013, is based on a media mix that includes an audio clip, an interactive film, a type test, a team and board game or a competition.



Protecting basic rights

Interview with **Professor Hansjörg Geiger**, member of Deutsche Telekom's Data Privacy Advisory Council.

Professor Geiger, what lies ahead for data privacy officers in 2013?
Prof. Geiger: The key topic will be the European Data Protection Regulation. The current proposal by the EU Commission is moving in the right direction in general, but Germany in particular should engage intensively in further discussion.

Why Germany?
Prof. Geiger: It's about preserving our high level of privacy. Data privacy is a basic right here. The relevant decisions of the German Federal Constitutional Court are also regarded as real achievements from an international perspective. By this I mean the basic right to informational self-determination and the basic right to assurance of confidentiality and integrity of information technology systems. The latter probably sounds quite unwieldy for the lay person, but essentially means that nobody is allowed to infiltrate a computer or telecommunications system without a warrant.

Are these basic rights now up for discussion again?
Prof. Geiger: If Germany is not careful, this development could imply this at least in part. Due to its legal form, the European Data Protection Regulation will become directly applicable law in all member-states. This would seriously limit the leeway for the German model with its many sector-specific regulations. German standards that go beyond the European regulation would no longer have a legal basis.

> "Nothing less is at stake than maintaining the high level of data protection in Germany."

Are German interests adequately represented today?
Prof. Geiger: Whether German involvement is sufficient will only become clear as the legislative process continues. The fact however is that the Federal Government, the Opposition and business interests are already extremely active. For example, the CDU/CSU and FDP parliamentary groups as well as SPD parliamentary group have presented detailed proposals in which they indicate quite clearly the issues that still require discussion. For example, applicants are requesting that the obligation for companies to appoint a data privacy officer should not be limited to large corporations but should also apply to midrange enterprises. A further requirement relates to the handling of sensitive data. This includes particularly sensitive data such as religious affiliation or membership of a labor union. Since we have to assume that our social protection objectives will continue to change in the future, the catalog of sensitive data should not be conclusively formulated.

Is it already clear whether the EU is moving to meet these demands?
Prof. Geiger: The current draft shows some improvements, though the German privacy level has still not been reached. We therefore still have a lot of work to do, particularly in the first half of the year. After all, the Commission and the European Parliament have the ambitious goal of concluding consultations by mid-2013.

Should the telecommunications industry participate with particular intensity in the discussion?
Prof. Geiger: It has been doing so for a long time. And for good reason. Data privacy made in Germany is regarded as a competitive advantage in many markets. If the new EU regulation were not to reproduce the German privacy level adequately, the only way out would be through an opening clause that would give Germany the opportunity to include more stringent standards. Such unilateral actions cannot be in the interest of our national economy, however, especially since one of the primary objectives of the new EU regulation is to compensate for regulatory imbalances in Europe. I expect a fascinating discussion to develop in 2013 against this backdrop.

Professor Hansjörg Geiger has been involved with the topic of data privacy since the beginning of the 1970s. His professional and academic career spans various roles in business, research, politics and the judiciary. Prof. Geiger was employed, among other things, as an independent researcher with Siemens, as a prosecutor and judge at the Munich District Court, as head of section with the Bavarian State Commissioner for Data Protection, as State Secretary in the German Federal Ministry of Justice, as President of the German Federal Office for Protection of the Constitution and as President of the German Federal Intelligence Service.

Risks are shifting

Excessive scaremongering or is it high time? This is not a question **Wolfgang Ischinger**, head of the Munich Security Conference, and **René Obermann**, CEO of Deutsche Telekom, are asking themselves in relation to cyber war. It's obvious to both of them that it's time to act.

Wolfgang Ischinger, head of the Munich Security Conference.

Wolfgang Ischinger took over the chair of the Munich Security Conference in May 2008. He studied law and international law and occupied various roles from 1975 to 2008 as a senior diplomat in the German Foreign Office. Among other roles, Ischinger has served in German embassies in Washington, D.C., Paris and London, as head of the Political Directorate-General and as State Secretary at the Foreign Office. Mr. Ischinger headed the German delegation on the Bosnia Peace Talks and was the EU representative in the troika negotiations on the future of Kosovo.

The former German ambassador to Great Britain and the U.S. put the topic of cyber security on the agenda of the Munich Security Conference two years ago. The interest of leaders from the realms of industry, politics and science was so great that Wolfgang Ischinger together with René Obermann issued an invitation in September 2012 to a separate Cyber Security Summit in Bonn. Fifty executives were to take part. In the end, some 80 senior managers joined the discussion on cyber war and IT security.

Mr. Ischinger, why does the topic of cyber security require its own conference?

Wolfgang Ischinger: Because industry and the state are coming under increasing attack from the Internet. A completely new type of threat is therefore emerging which follows its own rules and requires completely different security and defense measures. Not many seem to be aware of this yet, however. Although IT experts know a lot about the risks from the network, the real doubt lies in whether business leaders really perceive and correctly assess these risks. We therefore have to make this a strategic topic for boardrooms. And a dedicated high-level Cyber Security Summit will clearly contribute to this.

But the risks don't just stop at company or national boundaries?

Wolfgang Ischinger: We are increasingly facing genuine transnational global challenges that states and even groups of states can do little about. Natural disasters for example come under this heading. No phenomenon is more transnational than cyberspace. But it is precisely here that we are a long way off workable regulations and agreements at an international level. There is absolutely no capacity to act internationally. Progress is therefore urgently needed and necessary at national and international level. Especially since cyber security is becoming a location issue. There is no doubt that the well-prepared states will enjoy a better reputation globally than those that do nothing to combat cyber war.

Mr. Obermann, how serious would you say the situation is then?

René Obermann: Organized crime and industrial espionage aided by the net are no longer the stuff of science fiction films. Practically every area of public and private life is now dependent on functioning telecommunications and IT infrastructures. This means that not

to the network

René Obermann, CEO of Deutsche Telekom.

only a single company, but rather an entire location can be affected by cyber attacks. Controlled attacks from the Internet can have serious consequences, for example paralyzing power grids and financial markets. An example of this can be found in the U.S. at the end of 2011 when operators of natural gas pipelines came under attack from phishing for months. Simply clicking one of the malicious links was enough to allow the malware to install itself on the systems. This would have allowed the hackers, for example, to manipulate systems for controlling gas compressors.

What would be an appropriate response to the digital threat situation?
Wolfgang Ischinger: The time has passed when viruses, worms and Trojan horses could be battled alone. Cyber attacks are becoming increasingly professional. Hobby attackers can still be combated with technical resources. But a new branch of industry has developed in the meantime. Professional cyber criminals are developing cyber weapons on behalf of companies and states for attacking targets. They include Trojan horses such as Stuxnet, which was evidently commissioned by a government agency. It is therefore no longer about inflicting a little damage or annoying someone. The danger that states, for example, are entering into a cyber war with their secret services has increased significantly.

But wouldn't this then only happen locally, since only individual computers can be attacked?
René Obermann: No, for some time now, anything that has an IP address has been networked. The risk that critical infrastructures in a region or even a state might be disabled is therefore growing. There have already been attempted attacks on nuclear power plants and natural gas pipelines. Just imagine cyber criminals manipulating a nuclear power station's control systems, for example. The German government is also registering attacks more frequently on its government network. Anyone trying more than just switching off computers clearly could trigger disasters — even now! If bogus hardware and software components were installed in a particular aircraft type, for example, it would be possible to direct an entire range of such aircraft remotely.

René Obermann has been Chairman of the Board of Management of Deutsche Telekom AG since November 2006 and has been responsible for innovation in the Group since the beginning of 2012. Prior to this, Obermann was CEO of T-Mobile International AG & Co. KG and the Deutsche Telekom Board Member for Mobile Communications. His career began with a business traineeship at BMW AG in Munich. Following that, he set up his own business, ABC Telekom, in 1986, in which the Hong Kong-based conglomerate Hutchison Whampoa acquired an interest in 1991. René Obermann was Managing Partner of the resulting company Hutchison Mobilfunk GmbH and then Chairman of the company's managing board.

But to speak directly of cyber war seems somewhat exaggerated?
Wolfgang Ischinger: We see it differently. If cyber attacks were to cause disruption on such a scale that governments felt forced to respond through military intervention, that would be critical. This issue has preoccupied the U.S. and NATO in strategy papers for some time.

Then there's a case to be made for stopping networking?
Wolfgang Ischinger: Networking can no longer be stopped. We consciously take the risks since the advantages it offers for companies and states are fully undisputed. They guarantee access to markets and innovations and hence to economic growth. A global economy can now only be managed when we work, trade and live on a networked basis. Or do you seriously want to suggest that we dispense with smartphones or tablet PCs and turn back the wheel of time?

Mr. Obermann, companies like Deutsche Telekom are contributing to the increased networking of society. Are we on the right path?
René Obermann: Despite all undeniable security risks, networking has to continue. But we have to learn better how to deal properly with the new risks, gradually reducing them to a minimum — knowing full well that we can never be 100 percent secure.

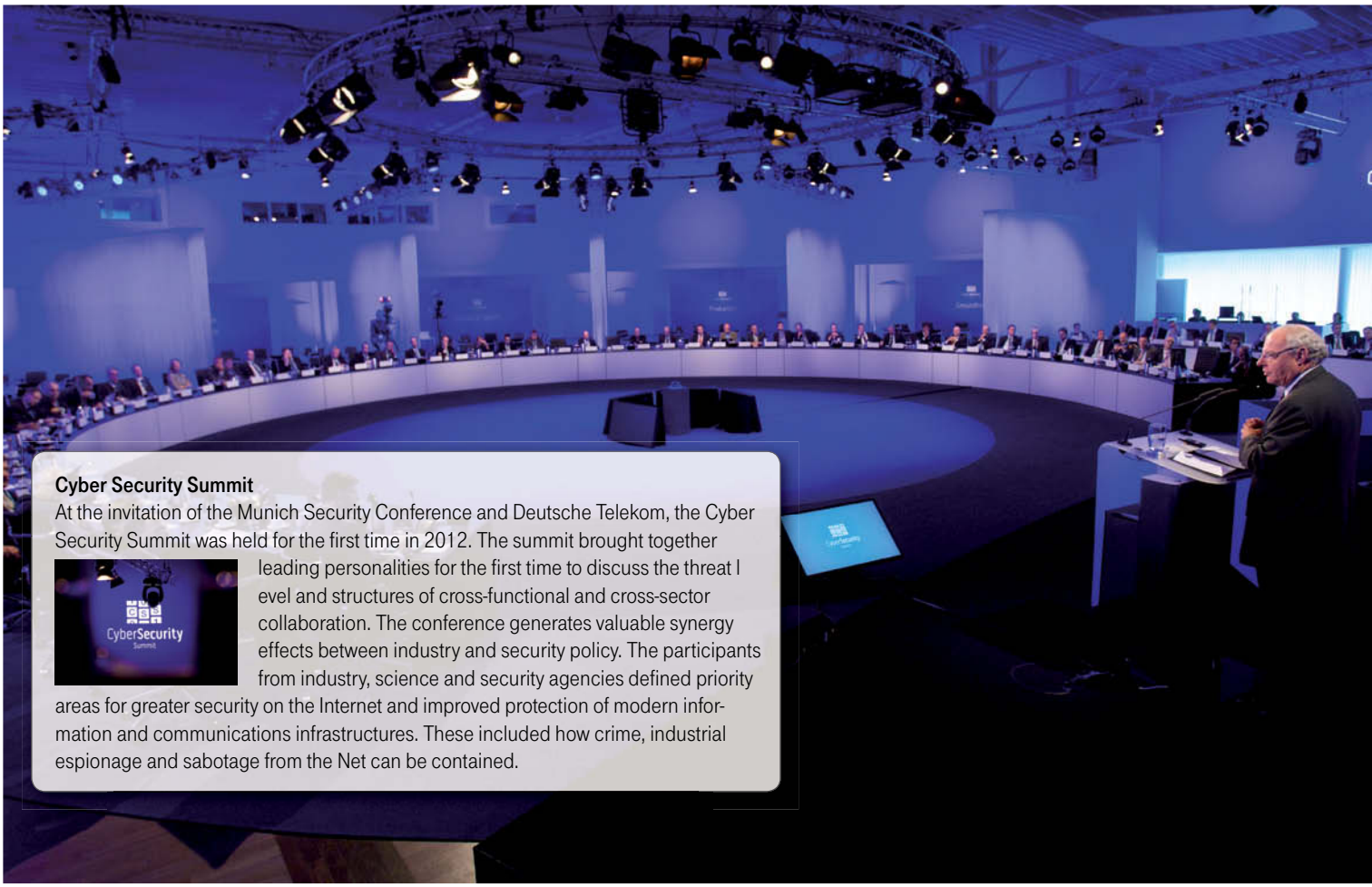
You have established three business areas that exclusively drive forward intelligent networking. What role do security and data privacy play in this?
René Obermann: I take it you mean the energy, healthcare and automotive areas. Security is right at the top of the agenda in these areas for a variety of reasons. The energy sector is in the middle of a transition phase, triggered among other things by the turnaround in energy policy. Power grids need to become smarter so that the power feed from thousands of photovoltaic systems and wind turbines can be managed. In addition to the transport network for electricity, a data network is being set up in which important information is exchanged between producers and consumers. We have to safeguard these new networks and data. At the end of the day, the energy networks are critical infrastructure.

And what is the situation in healthcare?
René Obermann: Data privacy is especially important here. It is frequently used as an argument against networking. The healthcare industry is therefore still finding it difficult to harness the advantages of networking. However, whether patient data is better collected in suspension files in medical practices and hospitals or in medical office information systems with often insufficient security is something I would question. As a telecommunications company we implement telecommunications, media and data privacy law on a daily basis, which means we have gained wide-ranging experience and therefore also know how this can be solved in healthcare.

So, how can the topic of cyber security be dealt with adequately?
Wolfgang Ischinger: The battle against cyber threats can only be won by working together. I therefore see it as very important from a security standpoint to set up a center for gathering information. Many companies are still concealing hacker attacks. They fear it will damage their image if the whole world knows that they were victims of cyber attacks. If they share their findings however, they will help others to protect themselves better. Conversely, it will also help them.

Munich Security Conference msc
Münchner Sicherheitskonferenz

Munich Security Conference
The Munich Security Conference is the most important independent forum for the exchange of views by international security policy decision-makers. Each year it brings together senior figures from all around the world to engage in an intensive debate on current and future security challenges. The Munich Security Conference discusses and analyzes current security challenges and tackles future topics. This includes issues such as security in a digitally networked world.



Cyber Security Summit
At the invitation of the Munich Security Conference and Deutsche Telekom, the Cyber Security Summit was held for the first time in 2012. The summit brought together leading personalities for the first time to discuss the threat l evel and structures of cross-functional and cross-sector collaboration. The conference generates valuable synergy effects between industry and security policy. The participants from industry, science and security agencies defined priority areas for greater security on the Internet and improved protection of modern information and communications infrastructures. These included how crime, industrial espionage and sabotage from the Net can be contained.

And what's the situation with the state? Should it stay out of problem solving?
Wolfgang Ischinger: Trust is absolutely essential to make progress at national level. There is an interesting area of tension, however, between the state and industry. Industry would prefer it if the state did not interfere in business. When it comes to issues of public security, however, the state should assume responsibility. Nowhere do these two positions overlap as much as on the topic of cyberspace. I can well understand that companies may find it difficult to disclose cyber attacks. However, what we know and learn then is not enough. Without information, innovation in the battle against cyber attacks will become more difficult than it is already. We therefore have to urgently adopt common approaches.

How does Deutsche Telekom feel about providing information openly?
René Obermann: We handle the information very transparently and report attacks on our systems. There were massive hacker attacks on our systems between September 3 and September 6, 2012. We had the situation under control at all times and were also able to identify the data center where the cyber attack originated. We also pass on such information to the Federal Office for Information Security (BSI) or providers of security software as this helps prevent the worst from happening in other companies. We therefore need a cyber security alliance with participation from all sectors. More than 70 percent of critical infrastructure is privately owned. We have to work together in the private sector, be open and honest in our dealings with one another and learn from each other. The cyber security alliance initiative (Allianz für Cyber-Sicherheit), which was launched by the Federal Office for Information Security and the German industry association BITKOM in 2012, is a move in the right direction. We are actively involved in this.

What form should such an alliance take?
Wolfgang Ischinger: We approved a policy paper at the end of the Cyber Security Summit in which the participants established that what was being done previously needs to be more closely dovetailed in the future and that stakeholders from industry, politics and society need to be networked more efficiently across sectors. An urgent task for such an alliance—ideally under the guidance of the Federal Government and as a joint initiative of industry associations—is to set up a platform in which all branches of industry and companies of all sizes can get involved.
Such a forum will allow findings on attack scenarios to be transferred openly and quickly between the members.

Rapid response team

Deutsche Telekom's CERT coordinates the management of security incidents for all of the Group's information and network technologies.

Every day the Cyber Emergency Response Team (CERT) receives ten messages detailing new vulnerabilities that have to be checked.

"The exciting thing about our work is that on any given morning we can't really tell what the day holds for us. The really critical security incidents are always the first of their kind. To resolve them, we have to constantly realign our defenses," says Bernd Eßer as he sums up the core competency of his team. The experienced security expert has headed Deutsche Telekom's Cyber Emergency Response Team (CERT) for two years. Together with his colleagues he is in the frontline when hackers uncover vulnerabilities or cyber criminals organize attacks.

That is what happened on November 3, 2011, when the FBI informed him that the computers of tens of thousands of Telekom customers might be infected by the DNSChanger malware. "The call came on a Monday evening," recalls Eßer. "We had to assume that the DSL customers affected would be offline the following morning. When a situation like this occurs, companies need a unit that can get all the relevant parties around the table in the shortest time possible in order to find effective solutions to help customers."

Ongoing reconnaissance

The Cyber Emergency Response Team is that unit. On call around the clock, this team of security experts in various fields ensures that the information and network technologies of the Deutsche Telekom Group will continue to work

reliably even in an emergency. In addition to the highest level of technical expertise, the CERT employees offer in-depth knowledge of the business areas and work procedures of the Group. This is the only way they can reliably assess how likely it is that a newly discovered technology vulnerability will jeopardize Telekom or its customers.

CERT receives on average ten messages every day detailing new vulnerabilities that are scrutinized in terms of their relevance for the Group. The most productive external sources are government agencies and CERTs in other companies. The security experts at Telekom maintain highly developed networks with Internet service providers and other telecommunications companies in all parts of the world. It is already established practice, especially in Europe, to warn each other as soon as it becomes known that the systems of the other party have attracted the attention of attackers.

Additional knowledge is made available to CERT employees by law enforcement and government authorities. The information from the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) is particularly helpful as it conveys findings in relation to threats that develop initially in other sectors of the economy before becoming evident in the telecommunications industry. However, important information is also available from internal sources. Apart from the Board, it is primarily the Press Office that disseminates news from journalists and often also from consumers. Deutsche Telekom's CERT has also developed its own input channels, which can be used by all to report security incidents via e-mail (cert@telekom.de).

Among their everyday tasks, Bernd Eßer and his employees evaluate sources such as Internet forums or Twitter in which different hacker communities share their knowledge of vulnerabilities and their potential exploitation. But that's not all. In order to be the first where possible to uncover vulnerabilities, CERT regularly checks all of the Telekom Group's portals and systems that are accessible on the Internet.

For emergency assistance, e-mail cert@telekom.de at any time to report security incidents.

Incident management

If a vulnerability is uncovered that poses an immediate threat to business operations, the incident management process is initiated. CERT puts together a task force of capable colleagues who are responsible for using the affected systems. Suppliers and partners are also often required to become involved. This was the case in April 2012 when a critical security breach in the WLAN operation of several DSL routers became known. The task force included personnel from Sales and Product Development, Procurement and Logistics through to Customer Service, which installed and maintained the equipment.

"When a number of different affected parties sit together around a table and each one understandably focuses primarily on his or her area of responsibility, our task is to define the required steps precisely and push through their implementation," explains Bernd Eßer, head of CERT at Deutsche Telekom. "We often have to convince the parties involved that they have to shorten their established process paths considerably so that we can get to grips quickly with the incident."

Eßer sees the 2012 router incident as a prime example. The firmware of the relevant products had to be updated in order to resolve the security breaches. This is a task that normally involves several weeks of development, approval and delivery cycles. "Together we completed the job in three days. I can still remember clearly that hardly anyone expected us to respond so quickly on becoming aware of the vulnerability." The incident clearly shows, says Eßer, how important it is to respond flexibly to avert danger. "The Cyber Emergency Response Team had the task here to define clear requirements and involve all partners in accordance with their strengths. This sometimes involved reinventing ourselves in order to avert potential damage."

Agenda

The CERT security experts

- coordinate management of critical security incidents;
- determine and assess threats to the Group's core technologies;
- assess and distribute security warnings and recommendations for action;
- audit security architectures and processes as well as system landscapes that are exposed to increased potential danger from the Internet;
- scan vulnerabilities in portals and systems that are accessible over the Internet.

Bernd Eßer
is head of Deutsche Telekom's CERT

"When a risk arises, companies need a unit that can get all the relevant parties around the table in the shortest possible time in order to find effective solutions."

DNS Changer

When four million computers worldwide were infected with malware, Deutsche Telekom, the German Federal Office for Information Security (BSI) and the Federal Criminal Police Office developed a rapid test to allow users to check their PCs online.

The incident created a major stir around the globe. It resulted from a type of cyber criminality, which up to the time of its discovery by the FBI had not been regarded by anyone as a potential threat. Over a period of more than seven years, a group of Estonian hackers infected some four million computers with the DNSChanger malware. DNSChanger allowed the cyber criminals to manipulate the Domain Name Systems (DNS) of the computers. Their business model involved redirecting the hijacked computers to prepared Internet sites when users called up particular portals that all generated high advertising revenues. The Estonians replicated the portals and substituted the advertising banners for those they marketed themselves. The lucrative business allowed the hackers to operate two large computer centers in Detroit and New York, where they used the 1,600 servers available to them to manipulate the infected computers.

The limits of feasibility

Once the FBI had detained the hackers in November 2011, the U.S. Federal Police found out that the computers infected with the DNSChanger malware would no longer be able to access the Internet if the data centers were shut down. Deutsche Telekom's CERT learned of the facts on November 3, 2011. The FBI informed Telekom's security experts by phone that the Detroit data center was to be shut down during the night. The callers requested Deutsche Telekom's assistance to redirect the entire data volume to secure servers in New York. The provider would have to intervene in the DNS configuration of the affected computers for this purpose. Since this was incompatible with German law, CERT decided together with Group Privacy not to comply with the request. CERT therefore had to assume under these circumstances that tens of thousands of customers ran the risk of no longer having Internet access the following morning. Information and help texts were produced during the night for all call centers as well as briefings for the department heads in Customer Service. Crisis management did not have to be activated however since the FBI had found another provider by the morning to redirect the traffic.

The online rapid test helped 19,000 Telekom customers to remove DNSChanger from their computers.

Rapid test sets precedent

Notwithstanding this, another task now had to be resolved. The FBI requested providers worldwide to remove the malware from the infected customer computers within three months. In order to reach as many Internet users as possible, Deutsche Telekom's CERT developed a user-friendly, reliable rapid test together with the German Federal Office for Information Security and the Federal Criminal Police Office. Users could go to www.dns-ok.de and check at the click of a mouse whether their computers were infected with the malicious code. In addition, the website provided assistance on disinfecting the computers. Thanks to intensive media work, with CERT involving Telekom's press department, the rapid test was used more than 22 million times. On the first day alone, Telekom counted 10 million hits. Moreover, the rapid test set a precedent. Fifteen countries adopted it as best practice for developing similar tests.

Parallel to this, Telekom was able to identify 19,000 of its own customers who had captured the malware. These customers were then informed via e-mail how to remove DNSChanger. The rapid test and the direct customer mailing achieved the desired effect. When the FBI finally shut down the New York servers at the start of July, there was no increase in customer requests regarding faulty Internet access.

Peter Franck
has been a member of the Chaos Computer Club for some 30 years. His professional focus is on the development of electronics, software and procedures. He also worked for many years as a technical expert. Peter Franck has been primarily involved in the area of data recovery in recent years.

Preprogrammed vulnerability

Mr. Franck, as an expert and member of Telekom's Data Privacy Advisory Council, how do you rate the quality of critical vulnerabilities? Has anything changed compared to previous years?
Peter Franck: My most striking observation relates to the almost universal presence of exploitable vulnerabilities in practically every type of technical system, be it IT systems or communications systems, mobile devices or microcontrollers, vehicles or industrial facilities.

What does this mean for the users of these systems?
Peter Franck: Users have to acclimatize themselves to a variety of vulnerabilities. It can be assumed that every system has been compromised if compromising appears worthwhile for any moderately skilled attacker. I would therefore predict that the currently prevailing, totally unrealistic confidence in electronically implemented functions will be sustainably undermined.

What are attackers particularly interested in?
Peter Franck: That depends to a large extent on the attacker's motivation. Some hackers just want to play for example. They often inform the operators about their findings. If there is a commercial or criminal motivation behind the attack, then this involves the maximum achievable gain. Politically motivated attackers use attacks more as a means of protest while with institutional attackers it's generally about gaining an information edge or a targeted disruption. The risk therefore has to be assessed individually for every unit in question based on the possible attacker groups and their alleged interests.

Should the affected companies alter their defenses?
Peter Franck: Companies would be well advised to get to grips with the material, since practically everyone is affected. To view this purely as a defensive task is not sufficient in my opinion. The vulnerability of technical systems is virtually preprogrammed by the prevailing industry standards. This should therefore be considered when planning and developing systems. Subsequent networking of formerly autonomous systems should be approached with great caution. I would recommend using verifiable systems exclusively in especially critical units.

For which companies does it make sense to establish a CERT?
Peter Franck: A CERT always makes sense if the business model is highly dependent on the availability of information technology systems and the level of interconnection of these systems is high. It is suitable in principle for limiting or even preventing operational interrupts as a result of induced disruption of technical systems.

Chaos Computer Club (CCC)

Germany's Chaos Computer Club (CCC) was founded by hackers. The information society, it claims, requires "a new human right to unhindered global communication." That is why the club "advocates cross-border freedom of information and deals with the effects of technologies on society and the individual." Membership is open to all who can identify with these objectives. A registered society under German law, the CCC is based in Hamburg. It was founded to give hackers a platform and to report on activities. People who are active in the CCC do not need to be members.

Competent consulting

Deutsche Telekom's CERT explains current cyber threats to employees and customers.

Deutsche Telekom's Cyber Emergency Response Team (CERT) protects the Group and its customers against threats from the Internet. One of its key tasks is advisory management. The CERT experts analyze the current threat situation around the clock and based on their analysis draw up security warnings and recommendations for action. The total number of security warnings issued in 2012 was 1,120—the same high level as in the two previous years. Many of these cases address vulnerabilities that can lead to denial-of-service attacks or drive-by infections. Looking at the operating systems, there appear to be no significant differences between the market leaders Unix and Windows. While 48 percent of vulnerabilities related to Unix platforms, the figure for Windows systems was 43 percent.

Risk management in Sales

The round table on Security at the Workplace checks data protection and data security at Telekom sales partners.

Various external sales partners support Telekom in marketing its products to customers. Existing customers are also advised of new products and existing contracts are extended via these channels. These external partners must comply with the same high data privacy and data security requirements as Telekom itself. Unfortunately, some partners or employees of these partners do not adhere to the strict requirements. To examine these cases, take legal action where necessary or initiate preventive measures, a "Security in Sales" roundtable was set up in 2010.

This internal advisory and information body meets every two weeks. The members discuss sales-related cases of fraud, such as commission fraud or the use of unauthorized sales partners, and assess these from their own perspective. These cases generally result from unauthorized data processing and data usage over and above the contractually agreed purposes. A decision is then made at roundtable sessions on which options exist to proceed legally against such contractual partners. Members of the roundtable come from areas such as Group Security, Group Privacy, Compliance, Legal Affairs as well as the Sales units. They also develop criteria for sanctions and ensure that Telekom learns from cases of fraud for the long term and closes any gaps. In this connection, the roundtable makes recommendations on sanctions and countermeasures.

Preventive investigations

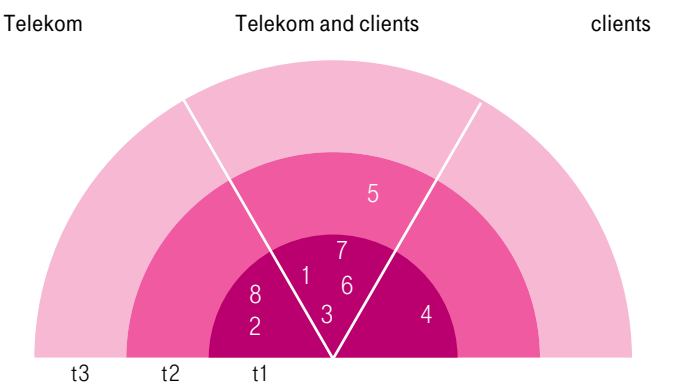
Threat radar plots development of business-critical cyber threats.

Availability is one of the central quality factors in cloud computing. Cloud providers are investing significant resources in the disaster recovery of their systems to prevent possible data losses and loss of service. Telekom certainly does so by providing a second data center alongside every cloud data center to take over its operation should the need arise. The idea that disaster recovery systems might in turn fail was regarded as a purely theoretical until 2011. However, after several incidents with international competitors, the topic has acquired a new dimension.

The changing risk situation is also reflected in the so-called threat radar, which Deutsche Telekom CERT uses to illustrate the development of cyber threats (see chart). The radar supplies reliable information for assessing the business risks that cyber threats pose. Preventive investigations allow Telekom to plan the necessary security measures in advance and implement them precisely.

The radar image depicts the proximity of a threat and the possible points of attack. The special risks associated with a potential threat identified on the radar are then clarified by Deutsche Telekom's CERT in a risk portfolio. The risk portfolio explains the key findings of the risk analysis underlying the radar and provides detailed information on the potential damage. In addition, the risk portfolio quantifies the probability that attackers will exploit an existing vulnerability.

Threat radar



Threats

1 Advanced Persistent Threats (APT)
2 Spear phishing against Telekom employees
3 Mobile malware
4 Attacks on mobile banking
5 Denial-of-service attacks on DNS infrastructure
6 Attacks on DSL routers
7 Loss of cloud services
8 Shitstorms

Development stages

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

Source: Deutsche Telekom

Fall campaign

Denial-of-service attacks are increasingly powerful.

The Domain Name System (DNS) is one of the most attractive targets for attack in cyberspace, and not without good reason. By assigning website names such as www.telekom.de to IP addresses, DNS constitutes the technical communication backbone on the Internet. Against this backdrop, handling DNS attacks is part of an Internet provider's everyday business.

The pressure of attack escalated further once more in fall 2012. Apart from classic denial-of-service (DoS) attacks that attempt to bring servers to their knees with a flood of simultaneous requests, so-called reflected denial-of-service attacks were also occurring increasingly. Instead of adopting the usual approach and setting up a botnet with thousands of computers, this type of attack uses regular DNS servers in the Internet to attack the actual targets indirectly via these servers.

A number of Deutsche Telekom's DNS servers were exposed to a massive attack of this kind at the start of September. The Group's Cyber Emergency Response Team (CERT) prevented the failure of the infrastructure and successfully fended off the attackers. The team used a special security platform in order to analyze the attack and render it harmless. Computers in the data center of a German hosting provider were identified as the origin of the attack. The progress of this attack shows that providers have to cooperate more intensively in order to jointly ward off cyber attacks.

Matter of trust

Telekom keeps out potential attackers of T-Online user accounts.

An increasing number of hackers are abusing the trust enjoyed by Internet users in order to use web portal offers on their behalf. This comparatively modern type of attack is referred to as cross-site request forgery (CSRF). Telekom received an external report of CSRF vulnerabilities in T-Online's e-mail center in 2012, as a result of which potential attackers would have had the opportunity, among other things, to delete e-mails. T-Online users would have logged on to the portal and during the current session accessed a website that had been prepared with malware which would then have controlled the deletion process. Deutsche Telekom resolved the vulnerability as soon as it became aware of it. A transaction-related security feature—a so-called CSRF token—was installed on the affected portal pages, preventing such attacks.

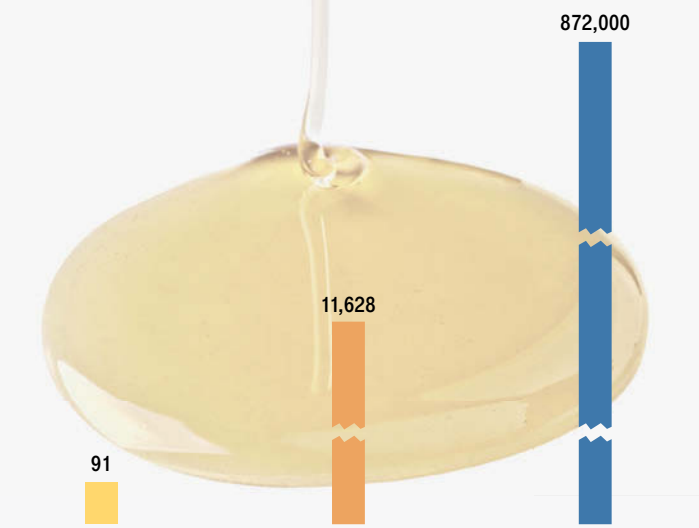
Sweet temptation

Honeypots provide access to the enemy's knowledge.

Attackers are constantly discovering new resources for perfecting their art, and threats to the Internet industry are changing just as quickly. Deutsche Telekom uses a multi-level early warning system to promptly investigate the enemy's capability. One of the central elements of this is what are called honeypots. These are systems that fake vulnerabilities in order to attract attacks and allow them to be analyzed. Deutsche Telekom operates 91 virtual traps of this type worldwide with up to 400,000 attacks a day registered on them in 2012.

All honeypots work in isolation from Deutsche Telekom's actual infrastructure. The Group's infrastructure is therefore not at risk of being compromised. A number of honeypot systems are self-learning so that unknown attacks can also be recorded and investigated. Thanks to this reconnaissance work, Deutsche Telekom can gather reliable information on how the threat situation is changing and how the Group must continue to develop its defense mechanisms.

Facts & Figures 2012



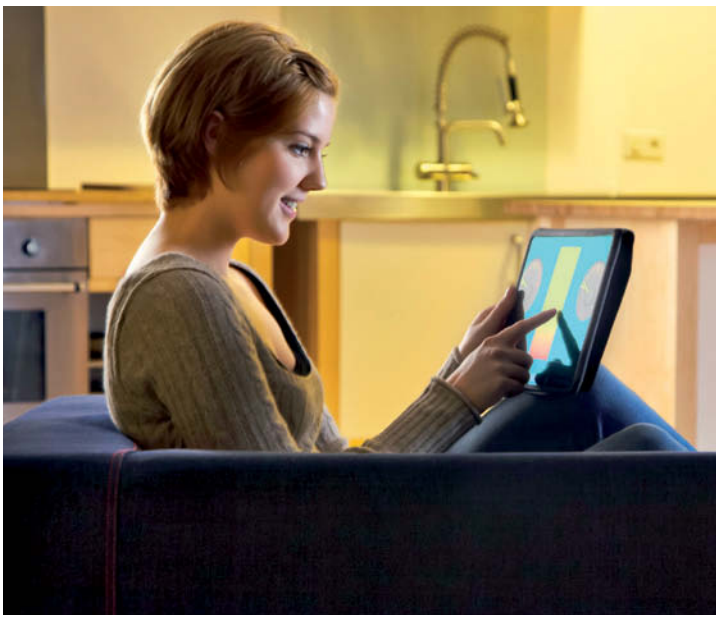
Source: Deutsche Telekom

Safety first

It's never too soon to start looking at data privacy and data security. That is why Telekom assesses the criticality of every system or product development with respect to data privacy and data security at an early stage and ensures appropriate consulting and testing. After all, solutions such as the connected home require the best possible protection. By Thomas Tschersich, Senior Vice President Group Cyber and Data Security at Deutsche Telekom.

There's no question of Deutsche Telekom bringing "banana products" to market whose data privacy and security only mature — or ripen — once they're with the customer. Instead, privacy and security by design is the guiding principle. Assurance of this has been provided since 2010 by the Privacy and Security Assessment process, which has evaluated in excess of 4,000 development projects for IT systems and products. The PSA process ensures that future solutions are weighted according to criticality even before a project begins so as to ensure an adequate data privacy and data security level subsequently during live operation.

Deutsche Telekom developed a simple questionnaire especially for the PSA process. It provides an analytical framework for determining the degree of criticality of all new developments. Using this methodology, projects are categorized as A, B or C according to their relevance in terms of data privacy and data security. Category A refers to complex development projects that are most critical in terms of data privacy and data security. Support, consulting, testing and approvals for such projects are provided directly by experts from Telekom's Data Privacy, Legal Affairs and Compliance Board (DRC) department.



Property owners can control actuators and sensors in the future in the connected home using mobile devices or the PC. The central control element must ensure that sensitive data does not fall into the wrong hands.

Managing the connected home easily and safely

Around a third of all development projects are currently classed as category A, with more than 600 such projects recorded in 2012 alone. Among these A projects is the Connected Home, for which Telekom has developed the infrastructure platform Qivicon. The centerpiece of this platform is the Qivicon Box, which users integrate into their home network and which they use to control numerous actuators and sensors via smartphone, iPad or PC. Users load apps onto their Qivicon Box from various manufacturers and providers such as Eon, Miele or Samsung, with whom Telekom collaborates in the Connected Home project.

For example, room temperatures can be monitored by links to thermostats, or roller shutters safely opened or closed remotely via the Internet. Some systems even register attempts to open blinds from the outside and forward notification to previously defined recipients. The connected home also enables monitoring of power consumption with smart metering. And as soon as smart grids become available, consumers will also be able to reduce their electricity costs, for example by adjusting their suitably fitted washing machines or dishwashers via an app that switches them on at a time when little energy is being consumed and the price of a kilowatt hour is particularly favorable.

While partners are themselves responsible for the security of their apps, Telekom has to ensure that different manufacturers' apps are cleanly separated from each other on the customer's Qivicon Box. This

About the author

Thomas Tschersich is Senior Vice President Group Cyber and Data Security at Telekom. An electrical engineer, he was placed in charge of IT security and information protection in 2000. Prior to his present job he was responsible for technical security services. Since 2001 he has dealt in an advisory capacity with all manner of technical security inquiries for federal and state ministries and public authorities.

is the only way to ensure that sensitive data does not fall into the wrong hands. Apart from personal data, consumption data and cost data, the Telekom solution also protects security-related information such as activation times of roller shutters or activation of alarm systems.

Establishing security precautions in early project phases

A good deal of work was required to identify and implement the appropriate requirements for data privacy and data security. A consultant from each of the Telekom Group IT Security (GIS) and Group Privacy (GPR) units has supported the Connected Home project from the first draft of the idea to the development of showcases for Cebit 2012 and IFA 2012 through to the current pilot stage. They advised the developers on solution design and raised awareness of the special risks associated with this project. The support is to continue until the release for live operation. During this time, the product will continue to be put through its paces.

Product developers had to pay special attention to the option allowing users to use the Qivicon Box to control information from different apps. In technical terms, the strict client separation or multi-client capability had to be anchored in the design.

Furthermore, developers had to observe all relevant provisions of the German Telecommunications Act (TKG) and Telemedia Act (TMG) and were required to encrypt all communication flows from Qivicon without exception. Last but not least, the users must remain the owners of their own data. Customers are therefore given several alternatives for storing and managing their data and apps, be it via local backup, e.g. on a USB stick or in the Telekom cloud.

As with every development project, the security experts worked on the basis of the standardized data privacy and security concept. In addition, GIS and GPR clarified specific issues individually with developers as no standardized requirements set or blueprints existed as yet for an innovative project of such complexity as Connected Home. Nevertheless, experience from projects of a similar thematic nature, such as Smart Metering, were incorporated in the planning of data privacy and security measures. Qivicon Box and Connected Home have since successfully completed the initial pilot phase with the result that the second pilot project can start as envisaged in early 2013.

No product without a green light

Documentation of the data privacy and data security status is produced on the basis of the standardized data privacy and security concept (SDSK). The SDSK is maintained over the entire lifecycle of a product. It not only contains all information from the product description to subsequent enhancements but also the release status of the individual development steps. No product is brought to market unless all essential lights are on green. With category A projects, security experts literally have a right of veto up to the last minute if important data privacy and data security functions are missing.

Data security category A, B or C?

Category	Relevance / Level of support / Approval	Distribution by percent
A	■ High relevance, as projects are complex and/or critical. ■ The project is supported, advised and approved directly by security and/or data privacy experts from GIS and GPR.	25%
B	■ Relevant, but projects are less complex with less sensitive data. ■ Standard requirements are implemented by the project teams themselves, with support from local security organizations if required. ■ Approval is given through a self-declaration by the project manager and, if appropriate, is reviewed by local security organizations; GIS and GPR review these approvals on a sample basis.	37%
C	■ No changes or generally irrelevant. ■ The projects do not result in any changes relevant for security and/or data privacy. ■ No approval is required; GIS and GPR review the project categorizations on a sample basis.	38%

Integrated security

The PSA process is integrated in the Telekom development processes. At the decision gates between each process step, a decision is made on whether the next process step is to be taken. This requires an explicit gate decision by the responsible management. The PSA process is linked to the decision gates at the start of the project and at the launch of live operation. At the start of the project, in the idea generation phase, the project is categorized in terms of its security and data privacy relevance. At the end of the implementation phase, i.e., before the launch of live operation, the PSA process must have been completed successfully. As such, all necessary approvals must be in place. If live operation is subject to certain conditions, the resulting measures must be implemented by the time the project is completed. If GIS and GPR are not directly involved in consulting the project, the quality and effectiveness of the PSA process are tested on a sample basis.

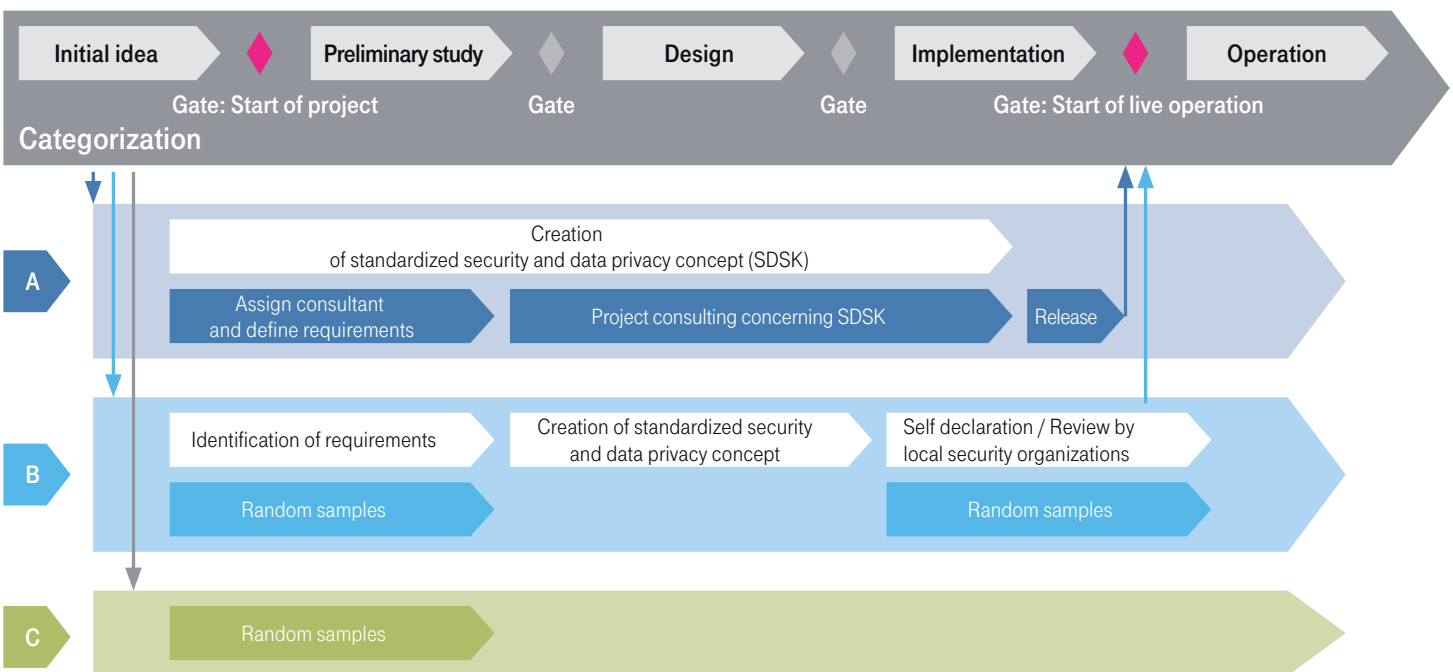
New projects with enhanced PSA process

The PSA experts also have a number of other tasks to accomplish in 2013. Many new category A projects are due to commence while a number of ongoing projects are coming to an end or being enhanced comprehensively. They include the Business Marketplace for small and midrange enterprises, the continued expansion of the 4th generation LTE (Long Term Evolution) mobile network, and the transmission of television programs to tablet computers as part of "Entertain to go."
In the meantime, Deutsche Telekom has further enhanced and improved the PSA process, for example by revising individual tools and documents, enhancing training concepts and including resources such as simple checklists for project managers and system administrators. Moreover, new requirements with respect to data privacy and data protection had to be integrated. Last but not least, the experts developed a workflow tool to guide users through the PSA process without media discontinuity—with the development of this tool being categorized and tested of course according to the PSA process.

Data privacy and data security as design criteria

While the effort required at the beginning of a development project seems higher than before since the introduction of PSA, consistently structured work practices are now possible thanks to the early incorporation of data privacy and data security, with the result that expensive reworks are a thing of the past. Deutsche Telekom is following the only correct path: data privacy and data security are critical design criteria. Because data protection and security advisors are involved right from the initial project draft, their work is more structured and transparent. End customers and business customers benefit equally from a suitable level of data privacy and data security as is ensured by the standardized PSA process model.

The PSA process at a glance



Criminal prosecution of cyber attacks

Can cyber attacks be prosecuted? If so, how? Telekom has specialists in the area of business crime law who are on hand to deal with this.

If criminal law scrutiny reveals an initial suspicion, Telekom files criminal charges, usually against person or persons unknown.

Regardless of whether denial-of-service (DoS) attacks, hacking, phishing or mass spam, whenever Telekom is confronted by a cyber attack, the Cyber Emergency Response Team (CERT) involves the busines crime law department following initiation of preventive emergency measures. If, following careful examination of the facts, the legal experts find initial grounds for suspecting a punishable offense they immediately contact the investigating authorities and file a criminal complaint – generally against unknown persons since the potential offender can rarely be identified directly in the virtual world of the Internet.

Quick action is critical since the offenders only leave digital tracks of their attacks, if any at all. This would typically be IP addresses of servers as well as the date and time of the attacks. The problem with this is that as long as no prosecution is launched by the relevant public prosecutor's office, such evidence is subject to the same legally defined retention periods as data recorded under non-criminal circumstances, in other words for a maximum of seven days. If this period expires before a criminal complaint is filed, all data relating to the origin of the attack is deleted.

If Telekom has filed the criminal complaint in good time, the investigating authorities generally approach the regional offices for special government regulations (ReSA) without delay, which as the state-mandated authority can evaluate the IP addresses on the basis of a court order or by order of the public prosecutor. Only when the IP addresses can be assigned to one or more owners can the investigating authorities perform searches or question the owners and witnesses. If there are adequate grounds for suspicion, the public prosecutor will generally bring charges.

It is especially difficult for investigators if attackers use a botnet to carry out their crime. The perpetrators set up illegally operated computer networks in this case, often using private PCs without the knowledge of their owners but also company mainframes. They smuggle malware, such as viruses and Trojan horses, unnoticed onto the computers and connect them together to form a virtual network. In this way they send spam and phishing mails, for example, from these remote computers, which then leave behind their IP address as "evidence."

Cases of botnet attacks are often forwarded by the investigators to the "Black Hat" investigating team of the State Office of Criminal Investigation in Düsseldorf. The Black Hat investigators then try to identify the individual computers involved in the botnet and render them harmless. They also try to protect the relevant computers from other botnets using measures such as firewalls and virus scanners.

The German Criminal Code (StGB) contains a number of penal provisions which are relevant for cyber attacks. For example, § 303a StGB states that whoever unlawfully deletes, suppresses, renders unusable or alters data shall be punished with imprisonment for not more than two years or a fine. Even the attempt is punishable. Mass spams could fall into this category. § 303b StGB deals with computer sabotage and is the relevant provision when it comes to denial-of-service attacks. §§ 202a and 202b StGB, which penalize data espionage and interception, are the basis for prosecuting hacking. In cases of phishing, several of the aforementioned penal provisions may apply depending on the scenario.

Comprehensive protection for the cloud

Skeptics are still warning about the data privacy and data security risks associated with cloud computing, even though the risks are scarcely higher than in classic IT outsourcing. And any additional risks are certainly manageable.

About the author

Reinhard Clemens has been a member of the Deutsche Telekom Board of Management and Chief Executive Officer (CEO) of T-Systems since December 2007. He previously worked at EDS in Germany, which he joined in 2001, where he was responsible as chairman of the executive board for sales, business operations and strategy in Central Europe.

The advantages of cloud computing are undisputed from a business perspective while the trend toward using industrialized and largely standardized IT from software and hardware factories continues unabated. Fewer and fewer companies want to run expensive data centers, preferring instead to take standardized IT services from the cloud, which is now more cost-effective than ever before. With no expensive upfront investments (CAPEX), companies are instead converting IT expenditure to running costs (OPEX). Moreover, IT resources can be procured much more quickly than before, which means that companies can respond more flexibly to changing market requirements.

Telekom is extending its existing data center in Magdeburg, which will form a twin data center for cloud services together with a new data center in Biere.

Owing to these financial benefits of cloud computing, companies are set to take the majority of their IT requirement from the cloud within the next decade. However, while private customers in the age of social media, online shopping or mobile services seem less and less concerned about the protection and security of their data, many corporate clients do not trust the cloud providers quite so completely. They fear that their data will no longer be secure with cloud computing and access to the data – in other words availability – will suffer. This skepticism is understandable since data is now the new oil in the gears of our economic machinery. Data and its efficient usage are critical factors for the success of companies. Data is valuable in its own right and should not be squandered recklessly by companies.

Few new risks with cloud computing

The public debate on cloud security often does not differentiate between the so-called public cloud and highly secure private clouds as offered by Telekom. It may be too much to speak about business as usual. But for serious providers like Telekom, which has been processing customer data for many years in the context of classic outsourcing and steadily driving forward the development of cloud computing in a pioneering role, topics such as protection against data abuse or data loss are not at all new. Telekom experts are constantly striving to minimize the external and internal risks of cloud computing. Telekom addresses this task holistically, checks all possible sources of danger and introduces protection measures in a structured way. It's not simply about using what is technically feasible. Cloud users and providers reduce the risks of cloud computing significantly by taking procedural safeguards as well as technical safeguards in

various areas in close collaborative partnership. Telekom has developed a security topology for this purpose, covering twelve task areas that should be observed by every company in the interest of securing their own data and applications in the cloud.

And Telekom has again increased the existing very high level of data privacy and security in its own data centers for its cloud services. Extended risks in the cloud include data loss and data espionage, for example, or hosting of IT on an infrastructure that a company or a private individual shares with others. The risk of data loss can be overcome by mirroring data centers. Virtual Local Area Networks (VLAN) are used to separate clients running on the same physical servers. They prevent a customer from accessing applications or data of another customer in the data center. Accordingly, each computer has precisely as many separate access channels as there are customers set up on it. Access channels and/or networks are completely isolated.

ISO certification and IT Baseline Protection Catalog

Companies should therefore proceed with caution when selecting a cloud provider and agree an absolutely high service level. Any provider who does not offer transparency regarding risk provisioning inspires little trust. And without trust in the cloud provider, companies would do well to consider whether they should go to the cloud.

Anyone who relies on a cloud provider should first check the provider's level of certification. However, here lies the crux of the matter at present. Accepted certifications already exist with the ISO 27001 standard, including the IT Baseline Protection Catalog formulated by the German Federal Office for Information Security (BSI), which focuses on protecting the technical infrastructure. Nevertheless, the ISO 27001 standard does not explicitly target cloud computing risks as yet. Specifications are lacking, for example, in relation to networks, virtualized routers and switches and cloud management but also internal handling of risks. Despite this, certification under ISO 27001 offers an initial starting point for selecting the cloud provider. This is also confirmed by the Federal Office for Information Security. The standard comprises more than 130 elements, which among other things specify the requirements for manufacturing, deploying, operating, monitoring, maintaining and enhancing a documented information security management system. This seems like a lot of work, and it is, even for specialists like Telekom.

Because ISO 27001 looks at IT security from the perspective of processes and workflows within the company, it highlights the fact that IT security also concerns all employees and should not just be looked at in a purely technical manner. A central element of ISO 27001 is the implementation of an IT security management system (ISMS). This requires, for example, that the cloud service provider create and implement an information security policy and have this audited at regular intervals through independent expert audits.

Deutsche Telekom is doing everything in its power to make cloud computing secure. Even international corporations are now entrusting their data to Telekom's cloud data centers. And increasingly more small and medium-sized enterprises are overcoming their reluctance with regard to the cloud. They trust Telekom's integral approach to security and recognize that it is best to have their data managed by a cloud specialist.

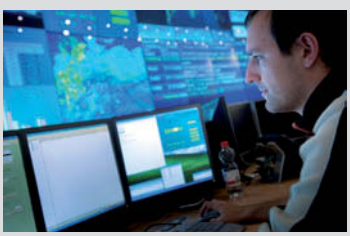
by **Reinhard Clemens,** Member of the Deutsche Telekom Board of Management and CEO of T-Systems

Secure cloud computing must take the following aspects into account:

1. Administration of identities with roles and rights, endpoint security and access control
2. User infrastructure and secure communication in the cloud
3. IT systems in the data center
4. Secure communication within the cloud and service orchestration
5. Protection of IT systems on the part of the service provider
6. Data center security
7. Security organization and secure administration
8. Service management and availability
9. Contract design, process integration and migration
10. Security and vulnerability management
11. Documentation and incident management
12. Requirements management and compliance

Secure cloud data centers

Telekom pays special attention to security in its cloud data centers. It has therefore created a comprehensive, systematic security architecture known as the Enterprise Security Architecture for Reliable ICT Services (ESARIS). ESARIS describes the standards by which Telekom ensures the security of cloud services in fully hierarchical and modular documentation. These standards contain all the technical, organizational and process-related measures that enable secure, industrialized ICT production. ESARIS takes account of all risks of the security topology for cloud computing and presents the achieved security level transparently for the customer. The methodological approach leaves nothing to chance. It guarantees that no element is forgotten or ignored when it comes to integrating the customer in the cloud. For this to happen and so that the achieved security level is continuously examined and enhanced, Telekom operates a comprehensive information security management system (ISMS).



Employees monitor not only operation of the servers in the data centers, but also the security of the data.

The Cloud Security whitepaper illustrates how an integral security topology makes cloud computing secure.

Security at a glance

Telekom bundles know-how about security products and averting risks in two new web portals.

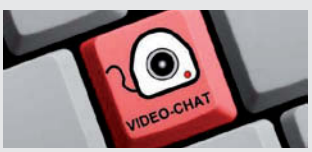
Around 100,000 new types of malware emerge each day, and numbers are still rising. At the same time, Deutsche Telekom's honeypots are recording a consistently high level of attacks on web portals. The good news is that 90 percent of attacks can be averted by properly maintained IT systems. With around 100 security experts, Telekom makes products secure for its customers. Telekom continues to build on its communications work so that no targets arise on the customer side. Two new web portals provide consumers, business and corporate customers with information on relevant dangers and effective remedies. While the product portal www.telekom.de/sicherheit provides a general overview of the security portfolio, the knowledge portal www.telekom.com/security outlines best practices for increasing own security. Moreover, Deutsche Telekom provides the accumulated security requirements for product development in a package on this portal for downloading free of charge.

Cloud service scores top marks for user friendliness, data privacy and security.

Computer Bild magazine rates the TelecomCloud the clear winner in a comparison test with Apple's iCloud. Both storage clouds were put through an extensive test course by the magazine in Issue 2/2012. The scope of the offering as well as its functions were included on the test agenda. So were user friendliness, rights, data privacy and data security. With an overall result of 2.47, the TelecomCloud fared considerably better than the iCloud, which scored 5.00 on a scale of 1 to 6.

A particularly positive aspect, according to the testers, was the fact that the TelecomCloud can be used with all Internet-ready PCs and with all Apple iOS, Android and Windows mobile phones. Because data exchange with the TelecomCloud is fully encrypted, the highest score, 1.62, was achieved in the Rights, Data Privacy and Security test category. The greatest differences between the tested products were revealed in a legal examination of the General Terms and Conditions with the TelecomCloud receiving a "Good" rating in this area.

Limitless communications



New technology reliably integrates voice services, office IT and conference solutions.

Identical voice services for office telephones, tablet computers and Office PCs, free access to videoconferences with smartphone, video phone or telepresence. These scenarios indicate how Telekom provides employees and partners with ICT solutions that optimally support their current tasks. T-Systems, the business customer subsidiary of Deutsche Telekom, has developed a technology platform for this purpose on which the Group's voice services, office IT systems and conference solutions work together securely. What previously had to be run separately for data security and privacy reasons has now been brought together by the new platform in user-friendly solutions. For example, Telekom had separated the voice and office infrastructure in order to create adequate protection against interception. In terms of voice traffic, this meant that only telephones, but not PCs, could dial in to the voice-over-IP network. Compared with this, the individual systems can connect to the new integration platform without jeopardizing data privacy and data security.

Europe tries out the real thing

Cyber Europe 2012: 400 experts from 25 countries ward off large-scale botnet attack.

Hackers set up an international botnet and attack Europe's financial sector with massive Distributed Denial of Service (DDoS) attacks. This was the attack scenario that the European Network and Information Security Agency (ENISA) used to confront the 400 participants of the defense exercise Cyber Europe in October 2012. In addition to government agencies from 25 member states of the European Union and the European Free Trade Association (EFTA), private companies took part for the first time. One of them was Deutsche Telekom in the role of an Internet Service Provider (ISP) that warded off attacks against corporate customers with the assistance of the Cyber Emergency Response Team (CERT).

The core task of the security experts was to jointly develop and implement defense measures. The key to success was setting up close-knit communication in order to exchange information on attack patterns, vulnerabilities and solution paths across states. The servers in the attacking botnet were deliberately switched off in a concerted action by all national CERTs. In total, Cyber Europe 2012 participants solved more than 1,000 security incidents. Public and private bodies proved their ability to maintain operation of the Internet even under massive attack. The next exercise is planned for 2014.

Experts successfully tested warding off cyber attacks in Cyber Europe 2012.

Security from the outset

Telekom has made data privacy and security a design criterion for its developments, in other words, no product reaches the market if it does not fulfill the relevant requirements. The worldwide developer community has been able to examine just what this principle means in practice on the Internet since September 2012. Telekom has published more than 1,300 technical security requirements on its new knowledge portal www.telekom.com/security that apply to the Group's products and processes. They range from a general, technology-neutral level (how a database system can be backed up) to product-related requirements, such

as for MySQL databases in which user data is stored. The document provides numerous implementation examples in order to provide developers and technical project leads with specific recommendations for action wherever possible. "We rely on transparency: On the one hand, developers should be familiar with our requirements from the outset. On the other, we engage in discussion on the criteria and can continue to improve these based on internal and external feedback," explains Thomas Tschersich, Senior Vice President of IT Security at Telekom. Telekom intends to update the published security requirements twice a year to ensure that the status of criteria development is constantly up to date.

How much regulation is necessary? How much mandatory reporting is possible?

The German Federal Ministry of the Interior published initial details of a planned IT security law in November 2012. Deutsche Telekom welcomes the initiative.

One of the key points of this initiative is the improvement of security measures by operators of critical infrastructures, such as telecommunications companies or energy and water utilities as well as Internet providers. In this context, the German government wants to establish a minimum security standard for critical infrastructures. Extended mandatory reporting of IT security incidents is also envisaged. The German Federal Office for Information Security (BSI) is to play an increasingly important role in this regard. Among other things, the Federal Office for Information Security is to obtain powers to test security-related hardware and software and the right to publish the results.

The dialogue initiated by the German government with the different industries as well as operators of critical infrastructures is an important element of the initiative. Such a dialogue ensures that the security level in individual industries will continue to develop through an external impetus. Only then can a consistently high security level be achieved among the different operators.

Self-regulation is the best way forward given the pace of development.

However, there are also arguments against individual legislative measures. IT attacks on systems in companies and administrations are changing and becoming more refined at an extremely high pace. A long legislative process is only of limited use for keeping up with this rapid pace. It would therefore also be conceivable for the different companies in a sector to agree on commonly high security standards in the framework of self-regulation.

The German government wants to use the IT security law as a common protective screen for critical infrastructures.

It is also important in this regard for operators of critical infrastructures, in particular, to find ways to ensure the security and protection levels of their products and services throughout the entire lifecycle. With this in mind, Telekom introduced a Privacy and Security Assessment process three years ago. This process is mandatory for all of Telekom's products and services and takes account of the concept of security by design. Such processes could be implemented in every company. A law would simply have to define the framework for further self-regulation.

It is crucial that IT security incidents are published clearly and transparently for customers and users. Telekom is already practicing this reporting process and exchanging findings across sector boundaries. For example, Telekom informs end customers and users of concrete threats using existing customer contact channels or portals and offers suitable security solutions.

How much mandatory reporting makes sense? And what responsibility does the customer have?

It is still unclear what added value the mandatory reporting outlined in the Federal Ministry of the Interior's key points offers over existing reporting requirements, given that appropriate reporting requirements have long since been anchored in the German Telecommunications Act (TKG), the Act Ensuring the Provision of Posts and Telecommunications Services (PTSG), the Telemedia Act (TMG) and the Federal Data Protection Act (BDSG).

An extension of the reporting requirement would be difficult to accomplish in practice. Even now, Telekom's computer systems are attacked more than 100,000 times every day. It is questionable, therefore, whether it would make sense to report all incidents. Telekom believes there is further need for clarification in this regard.

In addition, owing to the complexity it cannot be ensured that customers are fully informed. The responsibility assumed by providers but also by customers therefore has to be clarified.

About the author

Wolfgang Kopf has been Senior Vice President Group Public & Regulatory Affairs at Deutsche Telekom AG in Bonn since November 2006. In addition to representing the Group's interests at the national and international levels, he is responsible for the Group's regulatory affairs, spectrum and media policy as well as involvement in industry associations. Wolfgang Kopf studied Law at the Universities of Mainz, Speyer and London.

Common direction

All of Telekom's action areas in relation to security management are integrated in a single policy framework. This allows the Group to achieve common global security standards and a suitably high level of security.

Do traditional topics such as building protection or human resources security still play a role in the face of growing cyber threats? There is no doubt that the progressive digitization of the economy has brought its own threats to the data world. Nevertheless, digital and physical security can in no way be considered in an isolated way. Rather, they influence each other and are inextricably linked to one another.

Security in cloud computing is a prime example. Cloud data is obviously not stored somewhere in the atmosphere, but in data centers. If this data is only protected from digital access but not from physical access, this is worthless when unauthorized persons actually gain access to the computers. A virus such as Stuxnet, which apparently infected the nuclear facilities in Natanz, Iran, is excellent proof that even high-security systems are vulnerable to attack if relevant action areas are overlooked. Viruses that infiltrate computers via the USB interface do not come from the data network. They generally pass through the security checks on USB flash drives that are inserted by humans.

The more digitization progresses, the more vital it will be for businesses to integrate all security tasks in an end-to-end security management system. Experts call this the convergence of classic security and technical security, in other words corporate and cyber or data security. To respond accordingly, Telekom coordinated its Group security policies in 2010 in a common framework. This Security Policy Framework covers all key areas of security management (see illustration), ranging from information security and data protection to continuity and situation management to personal and event protection. In 2012 the Group intensified its focus on the Group-wide aspect – the third dimension of the governance model.

Security as a business enabler

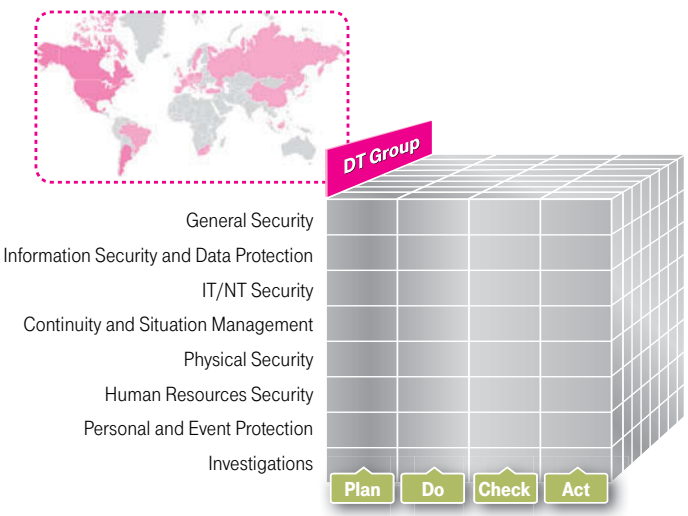
To implement the policies successfully, Group Headquarters needs to make sure that they are transferred to the individual corporate units with good judgment. In order to achieve sustainable security management, the current development status of the subsidiaries has to be taken into account. Depending on the size, situation, business model and level of experience, careful modification must be possible in order to strike a proper balance between the appropriate security level and economic performance.

For example, newly acquired companies should be given a fair chance to grow organically into the security framework. It is essential, especially with smaller companies, to maintain a sense of what is actually feasible while appreciating the need to agree a transparent approach with binding implementation steps in which minimum standards are formulated that can gradually be extended until the companies fully comply with Group policies. This allows us to adapt all standards in a way that is compatible with the business and to avoid security management that only exists on paper. If security management has a self-conception as a business enabler and if it is accepted as such in the company, business areas can be developed without neglecting security.

Group Security is in constant contact with security officers in the individual corporate units. The goal is to establish a mutual learning process at eye level. We use the expertise of all parties in order to continuously enhance both the policies and individual measures. In accordance with ISO standard 27001, based on which Deutsche Telekom's central security management system has been certified since 2010, we control the life cycles of our regulations and activities based on the Plan-Do-Check-Act process.

Managing life cycles

Translated to the policy process, this means: Which requirements do we need (Plan)? How do we implement them (Do)? Are companies, departments and employees implementing these regulations adequately and observing them (Check)? What can we learn from this for optimizing regulations on an ongoing basis (Act)? Based on the findings of the Act phase, the continuous improvement process starts again with the Plan phase and a new iteration begins. In this sense we are in the process, for example, of further harmonizing Group-wide security reporting and acquiring an even more reliable big picture at security.



By **Axel Petri,** Group Security Coordinator at Deutsche Telekom AG

About the author

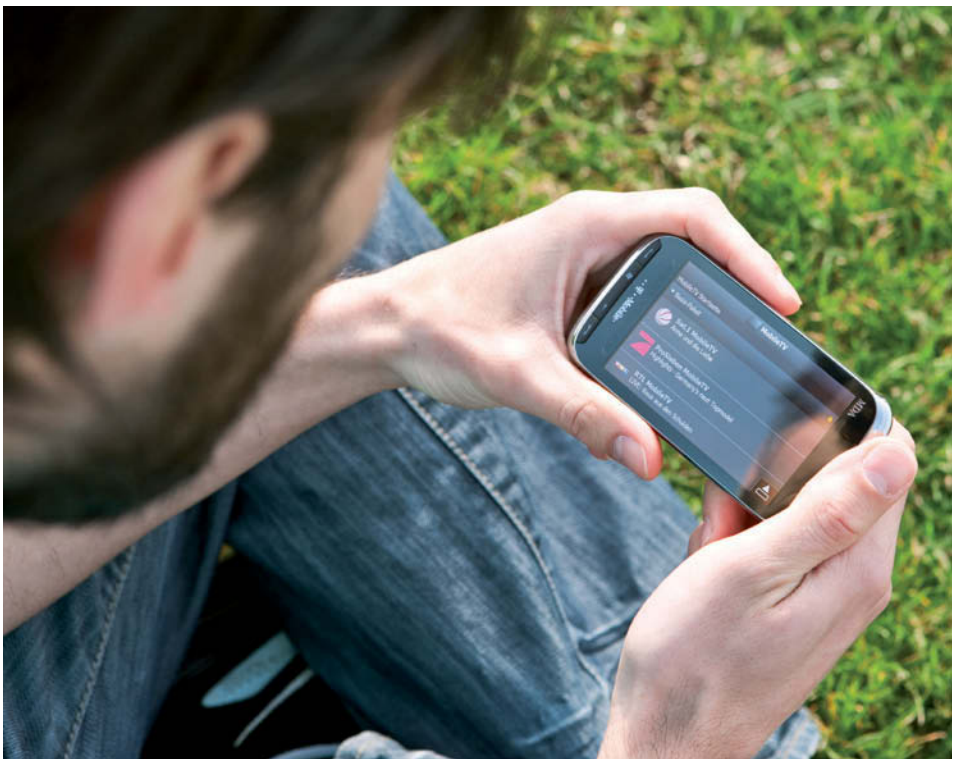
Axel Petri has been Senior Vice President of Group Security Policy and Public Safety at Deutsche Telekom since 2010. As Group Security Coordinator, he is responsible for assuring an holistic security approach that extends from classical business security to cyber and IT/data security. He joined Deutsche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

Changing times

The mobile Internet is beeing targeted by attackers. Superfast mobile communications standards such as UMTS and Long Term Evolution (LTE) along with powerful operating systems such as Apple iOS and Google Android are affording new opportunities not just for users but also for cyber criminals to achieve their objectives more easily. To manage the looming threats, companies must learn from the attackers and follow new trends in a timely manner.

The new quality of attacks has been identified by Deutsche Telekom's early warning systems since the beginning of 2012. Two years previously, the Group's security experts established so-called honeypots that simulate vulnerable smartphones in order to lure potential attackers. The digital bear traps allow the actions of the virtual burglars to be tracked in real time. The mobile honeypots were attacked on average 30,000 times a month in 2012. Thirty of these attacks gave particular cause for concern. Instead of the usual automatic search for suspected vulnerabilities, the hacker attacks were extremely targeted. For example, the honeypots received customized queries that the attackers planned to use to read the address books on the smartphones. Telekom experts also observed attempts to upload malware in order to ensnare the smartphones simulated in the honeypots in botnets.

Cyber criminals link many thousands and often even millions of Internet computers in botnets in order to increase the reach and power of their attacks. The fact that Internet-enabled cell phones could likewise be abused was still regarded as a theoretical threat until spring 2012. Based on the new findings, security experts at Deutsche Telekom are working on the assumption for 2013 that a number of botnet activists are concluding their experimental phase and will escalate their previous attacks. The first major botnet for the Android operating system, involving more than 10,000 users, was discovered at the end of 2012 in the U.S.



Experts are now noticing attempts to smuggle malicious code into smartphones and integrate them into botnets.

Individual responsibility

The majority of users are largely unprepared for the rapid change. Anyone trying to find ways to safeguard smartphones is up against a deeply rooted structural problem. It is a problem that gives cause for concern, particularly for business users. As soon as companies equip their employees with mobile devices, they have to find a solution for the fact that roles in security management are shifting by 180 degrees. While PC users can assume that the required security patches and updates are installed in the background without their assistance, the situation with smartphones is essentially different. If the threat situation changes, the only effective protection is generally to update the firmware of the devices.

With the exception of Blackberry, however, none of the market-leading operating systems offers an adequate management solution for loading the security mechanisms currently required via remote maintenance. Companies are therefore reliant on the activity of their employees. Updates of this type however are anything but trivial for many end users. And even users who manage to do it have a tendency to delay it because it means extra work. Weeks if not months often pass in practice until users decide to install an essential update. In the meantime, the vulnerability of mobile devices increases permanently.

Security through greater user friendliness

Companies can influence users' habits only indirectly. User agreements help them to prepare employees for their new role in security management. Training is valuable for conveying the necessary knowledge to end users. In everyday

The universal spread of high-speed mobile networks has led to the emergence of new attack scenarios for professional hackers.

business, however, companies only have a single sharp sword in order to actually push through the update regime. They use precisely tailored access controls to ensure that only those devices whose firmware version has the required security mechanisms can also actually dial in to the corporate network. All other devices remain excluded until their users have performed the required updates.

Central access control is one of the key tasks of a universal management solution as developed by Deutsche Telekom in the last two years. This mobility platform offers all required services for managing mobile devices. At the same time, it provides users with a constantly increasing number of mobile applications. At the end of 2012, all Apple iOS and Android devices approved by Deutsche Telekom for internal use could be connected.

Depending on the information required, two different access routes are available to mobile employees. If users want to synchronize their e-mail, contact information and calendar dates, the mobility platform uses Microsoft Exchange Server. In cases where employees want to access the intranet or the Group's business applications, a special access with additional security is provided. Deutsche Telekom has developed an authentication method that provides maximum security without restricting ease of use. In practice, users only have to enter a single feature, i.e., a password or user name. The application and platform generate an additional security feature in the background. If all features match, the user is granted the desired access. The new method replaces the otherwise typical process of dialing in to a virtual private network (VPN) that many users find cumbersome.

Knowledge transfer

The data protection experts in Group Privacy (GPR) and the data security experts in Group Information Security (GIS) have been monitoring the development of the mobility platform. They have ensured through the Privacy and Security Assessment procedure that data privacy and data security are firmly anchored in the platform design. Product developers call this principle "security by design." The specific requirements incorporated in the development work are demonstrated by Telekom experts on the knowledge portal www.telekom.com/sicherheit. The portal provides software engineers and project managers with a comprehensive catalog of technical security requirements that the Group's products must fulfill. Deutsche Telekom shares this knowledge in the conviction that security by design is the most effective form of risk prevention. If this principle is used in solutions such as the new mobility platform, companies will create for themselves a way to exploit the added value of the mobile Internet without losing sight of the risks of the new technologies.

Central security requirements

- One platform for managing the devices
- All devices have to be fully encrypted
- Secure access to the internal corporate network must be provided
- Secure access to the mail backend must be provided
- A filter must be installed to verify if the hardware has access authorization
- A filter must be installed to check the required operating system version
- A means of secure remote deletion must be provided
- If use of apps is permitted, a user agreement is required between the company and the employee
- The security policy must not be alterable by the user

Customer service at the cyber front

The Abuse Team is the contact point for anyone who wants to report abuse of Deutsche Telekom's Internet services. The security experts followed up more than one million reports in 2012.

Abuse of customer accounts is multi-faceted. Transmitting unsolicited e-mails is as much a part of this as hacker attacks on customers' computers or compromising homepages. Active awareness campaigns are therefore part of the core competency of Telekom's Abuse Team. In 2012, a total of 337,257 customers were informed in this way that their computers were infected with malware.

In most cases, the Abuse Team has reliable findings at its disposal to determine which malware is at play. The security experts at Telekom can therefore provide affected customers with precise information as to how they can "disinfect" their computer systems. In the course of 2012, increasing numbers of reports were received of infections with the Trojan horses "ZeuS/ZeuS peer to peer" and "bankpatch/multibanker." While a total of 5,069,147 reports were received by summer, the number in the second half of the year rose to 8,250,571. These are Trojan horses that infiltrate end customers' computers via botnets and retrieve online banking access data. Thanks to timely notification by the Abuse Team, the risk of the malware achieving its goal was reduced for customers.

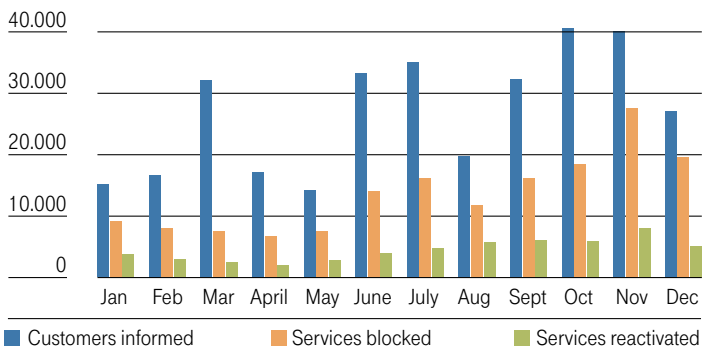
In 2012 the Trojan horse ZeuS stole online banking access data from computers.

Knowledge edge

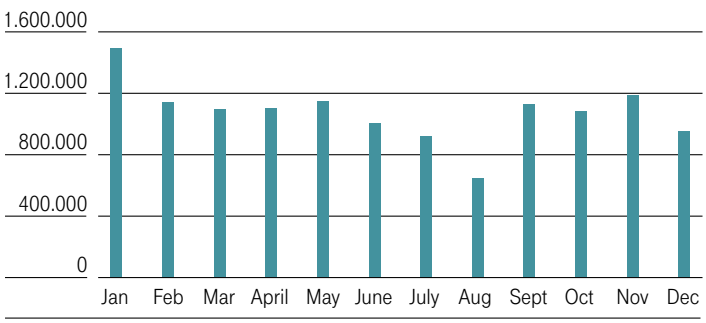
"This very specific knowledge is thanks to close cooperation with external security organizations that clarify the abuse of Internet services and inform the providers of the IP addresses of the affected computers," explains Markus Weyrich, a member of Telekom's Abuse Team. "Our most important source is the Shadow Server Foundation, an organization of voluntary network activists dedicated to the struggle against botnets. In addition to the IP addresses, we receive information on the malware active on customers' computers."

The Abuse Team has a time window of seven days to resolve the IP addresses supplied and identify the customers affected. Once that seven-day window has passed, the traffic data is deleted. Telekom received 1 to 1.2 million reports per month in 2012. The central input point is the mailbox abuse@t-online.de. All reports are first checked for accuracy and relevance. Just under ten percent of reports are then processed further. Those remaining usually involve duplicates that are received from different sources. Apart from the previously mentioned Shadow Server Foundation, security organizations such as Abusix Abuse Reporting, Gossler, JunkEmailFilter, Scomp, SpamVZ, Trendmicro and Uceprotect are among the reporting parties. In addition to this are messages from other Internet Service Providers, reports by investigating authorities as well as queries from customers.

Customer contacts in 2012



Reports received in 2012



New paths

One of the key activities in 2012 again was the battle against botnets. These are networks of Internet computers that are linked to one another by means of malware without their users' knowledge. If a computer is part of a botnet, it can respond undetected to remote commands, for example in order to send spam mail or infect other computers. Although the activity of the botnets, which are usually active on a global scale, was still very high in 2012, Deutsche Telekom registered a decline in the number of cases. Compared with 2011, the number of reports received fell from 9,146,790 to 8,250,571, corresponding to a 9.79 percent decline. At the same time, the number of service restrictions (port 25 blocks) decreased from 205,737 to 132,906.

The Abuse Team identifies the affected customers and advises them by e-mail and letter post to remove the malware promptly using up-to-date virus protection software. If the customer does not perform the recommended cleanup and if the customer's computer continues to attack other systems, the Abuse Team can initiate further steps. As a last resort, individual services are blocked, for example sending e-mail.

For the first time in late summer 2012, the Abuse Team felt obliged to deviate from this standard procedure. Services had to be blocked without the relevant customers being informed in advance in order to respond appropriately to a new type of threat. What happened? A new network had become active in the Asian region that broke new ground. Botnet abuse normally focuses on a relatively small number of computers. As long as these computers remain online, the attackers exhaust their resources, for example in order to send as much spam mail as possible. The remaining computers in the network are left alone in the meantime.

The newcomer from Asia turned the usual procedure upside down, however. It distributed relatively few queries per computer, but used all logged on computers at the same time to do this. "Since many customers were now affected at the same time, we had to change the standard procedure," explains Markus Weyrich. "Informing every customer first as usual would have exposed too many customers to a high risk for too long. We therefore decided to block services and inform customers in parallel."

A mediating role

This case shows that the Abuse Team has to constantly realign its work against the backdrop of constantly changing patterns of abuse. Sometimes security experts even have to take a mediating role. This was the case in early summer 2012 when the search engine provider Google put an entire Deutsche Telekom IP address range on a black list. This was because of a corporate customer of Telekom, who obtained IP addresses from this range and attempted to influence search results in such a way that Google interpreted this as manipulation.

As a result, Google set so-called captures for the entire IP address range. These are special security queries made up of letters and numbers that data providers can use to ensure that queries are actually coming from people and not from software programs. From this time on, all Telekom customers in the affected address range – users from the greater Berlin area – had to answer the required security question to perform any Google searches. "An extremely tedious process for Google users," explains Markus Weyrich. "We therefore discussed the allegations by Google with our business customer. Because the company was able to show that its actions were covered by German law, the service block requested by Google was not considered. Instead, we began to mediate between the two parties. A certain rapprochement is already evident. However, since very different interpretations of data abuse came into play here, the mediation work will continue in 2013."

Tasks of Deutsche Telekom's Abuse Team (excerpt)

- Receipt of unsolicited e-mails with promotional content (SPAM)
- Receipt of e-mails with viruses and worms
- Receipt of phishing e-mails
- Hacker attacks on customer computers
- Participation of Telekom customers in botnets
- Suspected abuse of access data
- Suspected mail server blocking
- Suspected abuse of guest books (e.g. slander)
- Abuse in forums and chat rooms by Telekom customers
- Criminally relevant content on our customers' homepages
- Queries regarding copyright infringements

Allianz für Cyber-Sicherheit,

a cyber security initiative for greater

Internet technologies have led to major innovations in recent years in the IT and telecommunications industry. The rapidly advancing networking of IT systems over the Internet has resulted in new opportunities and prospects both for citizens and for organizations, businesses and administrations. Almost every area of life or economic sector is affected in some way or other by information technology and is therefore part of cyberspace. Value-added processes in the real world, too, are now linked intensively through virtual space and are scarcely conceivable any more without it. This development requires continuous debate by all stakeholders on the undeniably significant innovation potential that IT solutions can offer, but also on the risks and security measures that are needed to operate IT securely and reliably and to use data responsibly. The pursuit of secure cyberspace is a challenge that can only be overcome through joint efforts by business, science and administration. This is the reason for founding the Allianz für Cyber-Sicherheit initiative by the Federal Office for Information Security (BSI) and the Federal Association for Information Technology, Telecommunications and New Media (BITKOM) as a platform for exchanging information and expertise in this area.

Cyber attacks are carried out by different criminal groups with different objectives. They range from denial-of-service attacks by activists and blackmailers to manipulation of Internet banking operations by criminals through to spying and sabotage by foreign government agencies. Many targets can be attacked quite easily and the attack routes effectively obscured. In addition, today's information technology is not flawless owing to its complexity and therefore always vulnerable. There is no question that this threat situation endangers not only individual institutions. IT systems in critical infrastructures where availability and reliability are especially important for our society, are also part of cyberspace and therefore exposed to the risks outlined.

Acting together: Allianz für Cyber-Sicherheit

The question here is how effective and efficient protection against cyber attacks can be provided in view of this threat situation and what risk is sustainable. Findings by the Federal Office for Information Security (BSI) show that well over 80 percent of known attacks can be averted using standard protective measures, e.g., as part of basic IT protection. Unfortunately many institutions still have a lot of catching up to do when it comes to implementing such measures.

Long-term security can only be achieved by means of a cooperative approach by all parties in business, science and government and continuous adjustment of all measures for preventing, recognizing and responding to the threat situation and the methods of the attacker. The Federal Office for Information Security (BIS) along with BITKOM initiated the Allianz für Cyber-Sicherheit (www.allianz-fuer-cybersicherheit.de) as a cooperation platform.

Allianz für Cyber-Sicherheit

Uniting all the key parties in the area of cyber security in Germany, the alliance aims to increase information security in Germany and strengthen the resistance of IT systems to cyber attacks. The Allianz für Cyber-Sicherheit is setting up a comprehensive knowledge base for this purpose and supports the exchange of information and expertise. A number of cooperation models are feasible for companies and organizations, depending on the manner and way a particular institution wants to become involved.

Partners of the Allianz für Cyber-Sicherheit can be institutions that are interested in organizing, promoting and improving cyber security in Germany by active contributions. These could include, for example, computer emergency response teams (CERTs), IT manufacturers and providers, Internet infrastructure operators or research institutions. Institutions both in the private and public sector that would like to benefit from the information and services of the alliance and would like to improve cyber security in their institutions are invited to participate in the Allianz für Cyber-Sicherheit.

Michael Hange
is President of the Federal Office for Information Security (BSI)

"The Allianz für Cyber-Sicherheit addresses all German institutions in the private and public sector."

protection through cooperation

The Allianz für Cyber-Sicherheit addresses all German institutions in the private and public sector. The multipliers of the Allianz für Cyber-Sicherheit therefore have the task of increasing the Alliance's coverage, for example by conveying up-to-date information to its members or other interested parties or creating awareness for the topic of cyber security through their work in various bodies or in the field of public relations. Business associations, chambers of commerce and industry or media can support the Alliance in the role of multipliers.

Services offered by the alliance

An important service offered by the Allianz für Cyber-Sicherheit is the promotion of dialog between all participants, namely companies in the IT industry and their users. Information on the use of IT is made available to the users and comprehensive opportunities are provided for the exchange of experience. The services include, for example, warnings regarding current cyber threats, best practices, standards and solutions for safeguarding the systems used but also recommendations on the general secure use of IT components. Apart from central distribution of information, the alliance also relies on a direct exchange in smaller groups, for example, in regional and industry-specific working groups or at regulars' tables.

In order to be able to assess risks correctly and to improve the IT security level in Germany, profound knowledge of the current security situation is essential. The Federal Office for Information Security therefore provides up-to-date information about the situation as part of the Allianz für Cyber-Sicherheit initiative, which institutions can make use of as a basis for their activities. To further improve the completeness of this situational information, it is also possible for partners and participants to bring their own findings on board or report events in conjunction with cyber attacks to the Federal Office for Information Security.

The enhancement of cyber security is a joint task for government, business and science. By participating in the exchange of expertise or actively contributing as a partner or multiplier, institutions can contribute to further enhancing cyber security in Germany and actively shaping it. All German institutions are called upon to get involved in this process!

By **Michael Hange**, President of the Federal Office for Information Security (BSI)

Together they are strong

The nationwide Allianz für Cyber-Sicherheit initiative was launched at the beginning of 2012. The initiative in which Deutsche Telekom participates actively and intensively pursues the goal of providing information on cyber security in Germany and enabling a comprehensive picture of the current threat situation. The initiative is aimed at IT and security managers in companies and organizations independent of size. In the framework of the cyber security strategy for Germany, the alliance therefore builds on the measures of the KRITIS (National Strategy for the Protection of Critical Infrastructures) implementation plan, which are taken for critical information infrastructures.

The nationwide Allianz für Cyber-Sicherheit initiative brings together IT and security experts.

The Allianz für Cyber-Sicherheit is a joint initiative of the Federal Office for Information Security (BSI) and the German Association for Information Technology, Telecommunications and New Media (BITKOM) and invites manufacturers, IT and telecommunications providers, Internet infrastructure carriers, CERTs, user industries with intensive use of IT as well as multipliers from media and science to participate in the alliance.

"We need a reliable and up-to-date situational overview of cyber security for Germany as well as an exchange of expertise and assistance on site in case of incidents," said Professor Dieter Kempf, President of BITKOM, when he presented the idea for the initiative at CeBIT 2012 in Hanover.

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 Telekom AG,
Fotolia, iStockphoto, Kai Mörk

Date of publication 1/2013

www.telekom.com/dataprotection

www.telekom.com/security