SECURITY ON THE INTERNET
REPORT ON INFORMATION AND INTERNET SECURITY

Group Information Security October 2013

LIFE IS FOR SHARING.

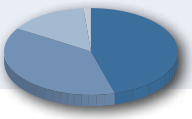
CONTENTS

NEWS

LEARNING

PROTECTION

INTERVENTION



SHARING

Thomas Tschersich
Head of IT Security,
Deutsche Telekom

DEAR READER,

Transparency and cooperation are the guiding principles of our work to combat cybercrime. Twice a year Telekom briefs you on the current threats that Internet users face. In this fifth report about Security on the Internet we show you which trends we have observed in hacks by cybercriminals on our specially devised honeypot infrastructure. We inform you about how we are expanding our sensor network not just quantitatively but also by continually adding new prototypes in order to continue to be able to protect you to the best of our ability from threats from the Net.

We are happy to share our knowledge with you and we cooperate wherever we can with research institutes, industry partners, public institutions such as the Federal Office for Information Security (BSI) and other Internet service providers around the world. Our aim is to make the Internet safer for you, for us and for everyone everywhere. The better we cooperate and the more openly we share our knowledge, the more successful we will not only keep pace with cybercriminals but also succeed in keeping a step ahead of them.

In recent months the threat situation faced by mobile terminal devices has grown more serious. The most complex Trojan for Android smartphones yet discovered has emerged. Mobile botnets are coming to light and this trend can be expected to continue in the future. We have compiled a number of useful hints for you to help ensure that your data and your mobile terminal devices remain secure.

Cybercriminals have also come up with something new to hack corporate infrastructures by means of specific Denial of Service attacks (DoS): intensified attacks with up to 60 times the bandwidth of conventional DoS attacks are the latest trend. Telekom is already working with the BSI as part of a coordinated provider initiative to develop measures to deal with this new mode of attack.

See for yourself what the current threat situation looks like and gain an overview of Deutsche Telekom activities to combat threats and risks. Make your own contribution to Internet security and let us know if you discover security vulnerabilities. We look forward to your assistance and are open for new cooperation arrangements. Our philosophy is straightforward: Security is for sharing.

Yours cordially,

Thomas Tschersich

SECURITY BREACH THREATENS HIGH-TECH HEATING SYSTEMS

In April the heating manufacturer Vaillant warned its customers that due to a security risk in the control system its ecoPower 1.0 micro combined heat and power (CHP) units risked being manipulated by third parties over the Internet. These high-tech heating systems can be controlled not only on the unit itself but also by an iPad app. They can be connected to the Internet, enabling Vaillant technicians to service them remotely. The company called on its customers to unplug the network cable from the controller to disable the Internet connection.

VPN TUNNEL FOR BETTER PROTECTION

© so47 – fotolia.com

Because, according to heise.de, clear-text remote maintenance passwords were very easy to access, third parties were able to pass themselves off to the heating system as houseowners, technicians or developers. The controller manufacturer Saia-Burgess has since issued a security update, but it and other IT experts still recommend using an encrypted VPN tunnel for added protection.

HOSTILE SIM CARD TAKEOVER

Older SIM cards that still use the DES cryptography standard and a 56-bit key can be hacked by text message. Hackers use over-the-air (OTA) communication between the mobile network operator and the customer's SIM card. Providers use OTA regularly to relay updates to their customers' mobile devices without the OTA message showing on-screen. If a hacker, "disguised" as the provider's server, sends an OTA text message to a mobile phone with DES encryption the device sends a reply from which the SIM key can be established. With the aid of this key the hacker can take over the mobile phone, listen and read and reprogram it for criminal purposes. Experts estimate that at least 500 million SIM cards with DES encryption are still in use around the world and are targets for potential text message attacks. In Germany, network operators have for around ten years relied on the more secure 3DES and AES encryption.


© leonardo255 – istockphoto.com

HACKERS SABOTAGE NEW YORK TIMES

Syrian supporters of President Assad in August disabled the New York Times website for several hours. For a while it featured the logo of the Syrian Electronic Army. The hackers had previously waged a targeted phishing attack on the domain name registrar Melbourne IT and used the account data it had captured to change the mapping between the website www.nyt.com and its IP address. The New York Times URL then led to the attackers' website. The domain name system (DNS) is responsible for matching a server's IP address to a more easily readable URL.

FOCUS ON DNS

© WoGi – fotolia.com

On Twitter the Syrian Electronic Army owned up to the attack, saying that for a while it had also taken control of the UK edition of the Huffington Post and the Twitter.com website. The group has also taken over the Twitter profiles of large media enterprises such as the Financial Times, the BBC and the Associated Press.

THOUSANDS OF WEBSITES MISUSED TO SPREAD MALWARE

The Dutch domain name registrar SIDN, the counterpart to Germany's DENIC, was subjected to a hacker attack. Websites hosted by the providers Digitalus, Webstekker and VDX were affected. They included the website of Conrad Electronic's Dutch subsidiary. Visitors were redirected to an "under construction" site that infected their computers with the dangerous Blackhole Trojan via an iFrame.


© KAR – fotolia.com

The hackers had modified the DNS entries in such a way that the URLs led to servers that spread the malware. Although the attack was discovered quickly, the false DNS entries stayed in the caches of most end customers' ISPs for an entire day because their so-called time to live (TTL) is set at 24 hours. For SIDN it was the second attack in a matter of weeks after systems had previously been compromised by an SQL injection and infected with malware.

SMART TV SPIES ON USERS

Security experts at Darmstadt TU pointed out in May that user behavior data was being relayed via the TV standard HbbTV, which stands for Hybrid Broadcast Broadband TV and regulates the way in which TV sets can access online content while the TV program is running. The TV set communicates with the broadcaster's server as soon as the user chooses a station, the researchers claimed, and TV stations can then use the data received to personalize advertising. Without adequate safeguards the standard could be misused. Unauthorized parties might conceivably gain access to functions such as those of the TV camera.

© manaemedia - fotolia.com

ZERO PROTECTION FROM HACKERS

At the beginning of August the IT security experts Aaron Grattafiori and Josh Yavor demonstrated at the Black Hat security conference in Las Vegas how easy it is to hack Samsung Smart TVs. Hackers can gain access to the TV's webcam and microphone and spy on the owner from afar. They can do so mainly via preinstalled apps such as Skype. There were bugs in their program code, consisting of HTML and JavaScript, the experts said. Because Skype accesses the camera and microphone user interface, users' homes can be monitored. The preinstalled browser based on the HTML Rendering Engine WebKit was said to be a further source of danger. If hackers were to attract the user to a website infected with malicious code, they could use a classic drive-by attack to gain control over the TV set.

PING OF DEATH IS BACK TO ITS DIRTY TRICKS

© hainichfoto - fotolia.com

As part of its monthly Patch Day, Microsoft was forced in August 2013 take action against an old acquaintance: the Ping of Death attack in which large data packets are sent to somebody by Internet Protocol (IP) to trigger a buffer overflow and computer crash. This vulnerability first occurred in the days of Windows 95 but was long felt to have been eliminated. It resurfaced with the transition from IPv4 to IPv6 and can affect all Windows versions except XP. A second Ping of Death patch was required for Windows NAT drivers.

INSTALL UPDATES MANUALLY

Along with these two patches, both classified as important, Microsoft published inter alia three further security bulletins on critical security vulnerabilities. They included an omnibus update for Internet Explorer that protects users from manipulated websites and malware. Critical priority was also assigned to a patch for Windows XP and Server 2003 systems that dealt with a security gap in the Unicode script generator. The third critical patch seals a leak in the Oracle Outside In file converter that existed in Exchange Server 2007 to 2013.
A further 13 security notifications were sent out on the September 2013 Patch Day. Microsoft classified four of them that related to vulnerabilities in the operating system, in Internet Explorer, in Microsoft Office and in SharePoint Server as critical. In all, the September update closed 47 security gaps, but some Windows Vista and Windows 7 users had installation problems. They were advised to deactivate automatic updates in the control panel and download updates but install them manually instead.

ROUTER BOTNET TAKEN OFFLINE

In late summer 2013 the Landeskriminalamt of Lower Saxony took a router botnet offline that had extracted confidential access data from networks. The computer magazine c't claimed to have discovered the botnet and informed the police. According to c't hackers had installed a sniffer program on a large number of routers that extracted access data from network traffic and sent it to various FTP servers. The hacker or hackers used a four-year-old vulnerability in the DD-WRT router firmware to install manipulated firmware on the devices along with a sniffer tool that extracts unencrypted access data from network traffic. One of the FTP servers was found to contain tens of thousands of files with stolen access data to, for example, the e-mail accounts of a firm of lawyers and the pictures taken by a bakery chain's CCTV cameras.

According to the manufacturer the firmware vulnerability was eliminated soon after it came to light in 2009, but many Internet users fail to update their router firmware and provide hackers with a long-term target when they make their routers accessible via the Internet. Telekom routers were not affected by the incident. You can find out from the QR code (right) how to avoid the problem of failure to install firmware updates for Telekom routers by means of automatic updates:

HACKER TRAPS AROUND THE WORLD
180 HONEYPOTS DETECT UP TO 800,000

Deutsche Telekom operates an early warning system of its own to get an idea, independently of security providers, of the risk situation on the Internet. 180 honeypot systems detect on a daily basis attacks on, say, standard PCs, ...

Honeypots are systems that simulate computer system vulnerabilities in order to attract hacker attacks. A honeypot might, for example, purport to be a Windows PC on which the manufacturer's latest security has not yet been installed. Telekom sets up these systems via the Internet at strategic access points such as its data centers, DSL connections and its mobile network. Hackers scan them and make use of their vulnerabilities to install malware or to take over what they assume to be a computer. They do so in a controlled environment where the hackers cannot do any real harm. The honeypot systems record how the hackers go about their work, which tools they use, which IP addresses they launch their attacks from, and relay this information in real time to Telekom's early warning system. This system evaluates the data automatically and relays it to the Group's Abuse Team if it finds that the IP addresses used for the attacks belong to Telekom customers. "If that is the case," says André Vorbach, one of the Deutsche Telekom security experts who operate the early warning system, "it will in all probability be customers' computers that have been hijacked by cybercriminals to attack other systems as part of a botnet." The Abuse Team informs these customers and ensures that they are able to remove the malware from their computers (see page 14 for more about the Abuse Team's work).

Telekom uses the early warning system to pursue four successive objectives aimed at protecting customers. It wants to get an idea of its own, independently of security providers, about the risk situation on the Internet. Other sources of information are, as a rule, the security providers, and their findings at times differ substantially from each other. Telekom collates its own findings with those from other sources and thereby achieves its second objective: to offer customers the best possible protection from online risks. Its third objective is to protect its own systems. By finding out which IP addresses hackers use to launch their attacks, it can make it harder for them to gain access to its services.

NEW PROTECTIVE FUNCTION MAKES IT HARDER FOR HACKERS TO GAIN ACCESS

Telekom security research specialists are currently working on a new protective function for websites, the Dynamic Web Application Protector, a first prototype of which already exists. Its function is to make it more difficult in future for hackers to gain access to websites and Web applications of Telekom and its customers. "If an Internet user tries to access a Telekom website, for example," Vorbach explains, "the system compares the visitor's IP address with the IP addresses the early warning system has identified as being used by hackers in the previous 30 minutes." If it finds a match, the visitor must solve a user-friendly Captcha task (Completely Automated Public Turing test to tell Computers and Humans Apart) before he is allowed to visit the site. By doing so, he proves he is a human and not an automated computer system that might be part of a hack. If the visitor's IP address is not on the early warning system's black list, the Internet user is taken to the site without being asked a security question. That may not prevent systematic attacks but it makes automated hacks more difficult.

Finally, the early warning system aims to improve Internet security for the general public. Telekom shares its findings with a number of cooperation partners who are connected to the system. They include research institutes, industry partners and the Alliance for Cybersecurity, a Federal Office for Information Security (BSI) initiative launched in 2012 jointly with the Federal Association for Information Technology, Telecommunications and New Media (BITKOM). In principle Telekom grants every company and every institution access to the data that its honeypot infrastructure generates, provided that the partner itself contributes information. Transparency and cooperation are the basis for greater security on the Internet. "Telekom is open for new cooperation partners," Vorbach says. "The more sources the security community has at its disposal the better we can assess and respond to the security risk."

RASPBERRY PI WITH HONEY – 100 NEW SENSORS IMPROVE DATABASE

Between February and October 2013 Telekom increased the number of its honeypots to 180 active sensors. Most of them were based on Raspberry Pis, very inexpensive credit card-sized single-board computers. That has enabled it to expand its sensor breadth most efficiently. A first prototype was built at the beginning of the year as a mobile Raspberry Pi honeypot that simulated the properties of a mobile terminal device and registered attacks on smartphones. Data that the honeypots collect from attacks is relayed directly to the early warning system for further evaluation and distribution. "We have mainly issued the new honeypots to our international country companies," Vorbach says. "That provides us with an improved view of the current situation."

The security experts have already identified a trend on the mobile Internet. "Around 75 percent of attacks on IP addresses that we allocate to mobile devices come from China." As a rule, the overwhelming majority of other

HACKER ATTACKS PER DAY

... smartphones and server systems. They have recently been joined by a further 100 or so new honeypots that also register and evaluate attacks on Telekom country companies.

attacks is also from China and countries such as Russia and the United States. Germany too is usually one of the top five countries from which cyberattacks originate. "That doesn't mean the hackers are based in these countries," Vorbach explains. "All that we see is the countries where the systems are located that they control over the Internet. They are, for the most, systems infected with malware because security patches were not installed on them."

Computer systems that do not receive security patches from the manufacturer are especially liable to be hijacked by cybercriminals and misused for hacks. Internet criminals use these and other hjijacked computers mainly to send out spam, to spy on credit card and online banking data and to launch Denial of Service (DoS) attacks that can disable websites and entire corporate infrastructures (for more about DoS attacks read the article on page 16). "The better the early warning system works," Vorbach says, "the better we can identify hacking trends and take precautions accordingly."

Telekom is constantly expanding its honeypot infrastructure and developing new prototypes in order to find out more about how cybercriminals go about their business and to help ensure that malware can be deleted from infected computers as soon as possible.

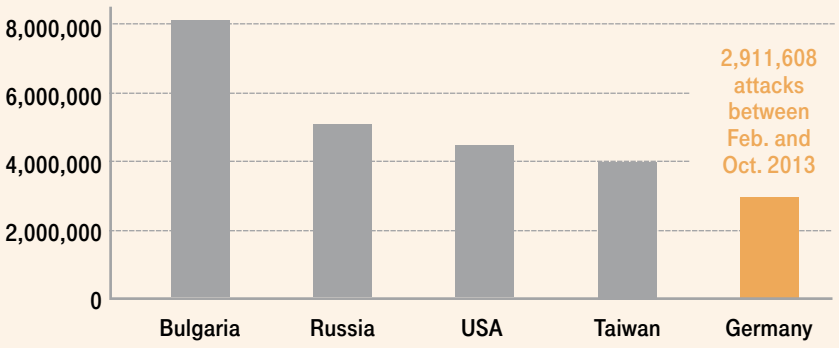
HONEYPOT VARIATIONS

Telekom relies on open-source software for the components of its early warning system. The generic **honeypot** registers incoming network traffic and is able to identify previously unknown attacks. The service-specific honeypot **Kippo** simulates the console access to a server via SSH (Secure Shell) and enables us to reproduce attacks in real time. **Dionaea** is a multi-protocol honeypot which simulates different services that are frequently attacked due to a large number of vulnerabilities. Then there is **Glastopf**, the software that simulates vulnerable websites. In addition to these open-source systems Telekom uses developments of its own that it places at the security community's disposal, also as open-source material. **MySQL-Pot** simulates an accessible database server and registers all attempts to log on to it. **ServletPot** simulates another Web application.

André Vorbach
Deutsche Telekom
security expert

THE TOP FIVE COUNTRIES OF ORIGIN

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



The prototype of a mobile honeypot used by Telekom consists of a credit card-sized single-board computer with a UMTS stick, a SIM card, a display and an additional battery.

EXPERIMENTS WITH NEW HONEYPOTS
RISING NUMBER OF SIMULATED SERVICES

Three new types of open-source sensors are used to measure whether and how industrial controls, e-mail accounts and configuration management systems are being attacked. Test runs are to be extended to new areas.

The new Telekom honeypots also detect attacks on SCADA systems that are used in industrial controllers.

Deutsche Telekom continues to extend its early warning system and is testing new types of honeypot. The newcomers include three more open-source sensors. Two of these open-source solutions are third-party products.

CONFIGURATION MANAGEMENT

The third sensor is an in-house Telekom development. It provides information about attacks on the Puppet configuration management system. In mid-2013 a Puppet vulnerability that could be exploited from the Internet was revealed, leading to the development of the honeypot. There are plans to publish the source code in full. No attacks have yet been registered.

E-MAIL

In June Telekom launched another honeypot that records spam attacks. Its gateway is an IP address that in normal circumstances no e-mail could reach because its e-mail address is unknown. “We should see no regular traffic on the target computer, so any connection must be seen as either a cyberattack or spam,” says Markus Schmall who heads Deutsche Telekom’s honeypot program. The new sensor is an open-source product that its developer, Karl Krueger, published under the name smtpot. The Java-based solution has so far registered only sporadic spam. “But here, too, no result is a result. This first test run shows us that no comprehensive scans of open e-mail servers are undertaken unless e-mail addresses have been released beforehand. The results must, of course, be validated by means of further installations,” Schmall explains.

INDUSTRY CONTROLLERS

Since May Telekom has used a honeypot to simulate for the first time an industrial control system, SCADA, short for Supervisory Control and Data Acquisition. It is using Conpot by Lucas Rist, another open-source development. The sensor uses the Modbus and SNMP protocols, both of which have relatively poor protection and have many weak points. The honeypot team has so far observed 600 attacks on the SNMP protocol that were considered to be attempts to prepare for a cyberattack. “This result says nothing about the general frequency of attacks on industrial plant, but it seems safe to say that cyberattacks on SCADA systems are not yet as widespread as automated attacks on Web portals,” Schmall notes. In the future further SCADA honeypots are to be set up at relevant points to cover different environments better.

NEW PROTOYPE: HONEYDROID
MOBILE HONEYPOT ON ANDROID SMARTPHONES

A new prototype has brought honeypots to specially adapted Android smartphones. Since the beginning of 2011 Deutsche Telekom has been the first telco to operate dedicated honeypots that simulate in their software the network properties of smartphones. These mobile honeypots, based hitherto on a standard Linux system, behave like a jailbreak iPhone or an Android smartphone with root access. They are connected to the mobile network via coupled UMTS sticks with SIM cards and are an attractive target for hacker attacks. So Telekom has transferred to smartphones what has previously been undertaken at data centers. The Honeydroid mobile honeypoint, specially adapted for the Android operating system, currently runs on two Android terminal devices: a Samsung Galaxy S4 and an HTC Desire. Both smartphones can be used to almost their full scope of functionality, while the installed software detects attacks from the mobile Internet and relays them to Deutsche Telekom’s early warning system. With this addition to its honeypot infrastructure Telekom has further improved the database of its early warning system in order to continue to be able to offer its customers the best possible protection from hacker attacks.

The mobile honeypot Honeydroid runs on adapted Android smartphones.

COMPREHENSIVE SITUATION REPORT
SECURITY DASHBOARD EVEN MORE ACCURATE

New-look security tacho comes up with new functions such as focusing on a specific target country.

Deutsche Telekom has extended the range of its freely available security tacho. Initially, the Sicherheitstacho information portal unveiled at CeBIT 2013 concentrated on depicting honeypot attacks by their country of origin. Since mid-October the new-look platform **www.sicherheitstacho.eu** has also focused on target countries.

The underlying sensor network consists of 180 honeypots set up in twelve different countries. The security tacho shows by country in real time which cyberattacks are launched on the sensors there. Along with the live ticker, Telekom has adjusted the Top 15 overview of countries of origin. Since the relaunch tacho visitors have been able to see for each of the twelve target countries the most frequent countries of origin of cyberattacks on them.

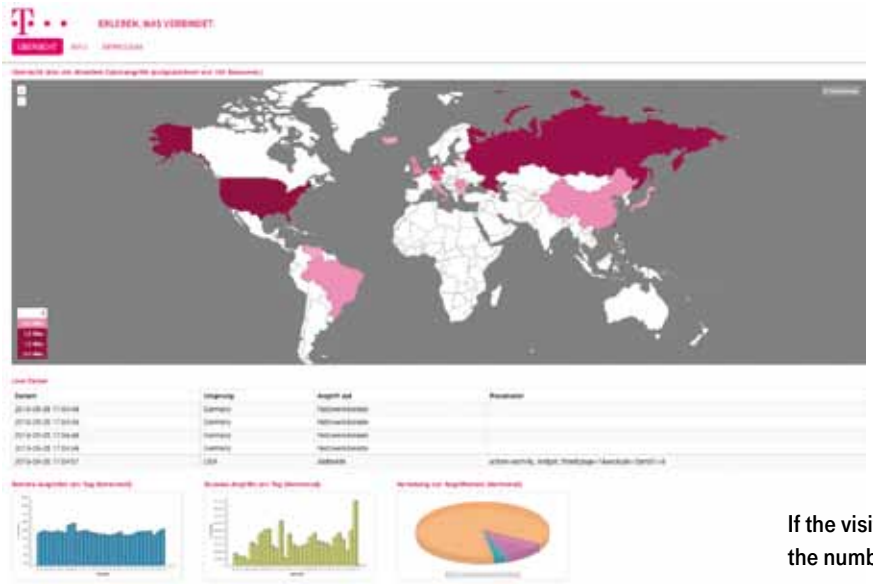
INFORMATION ABOUT THE ATTACKERS

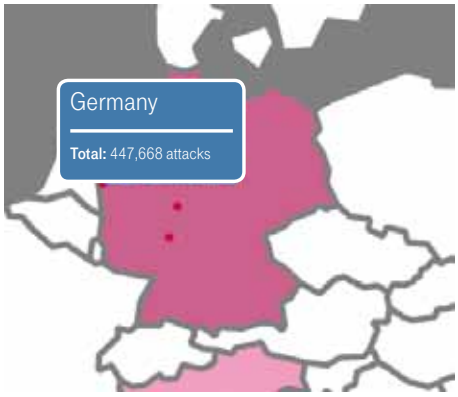
The digital world map illustrates the current state of affairs. The darker the country is colored, the more attacks have been registered from there in the past 30 days. If the visitor points the cursor at one of the colored countries, the absolute number of cyberattacks on this country is faded in. If the cursor hits a red spot on the map, it shows the number of attacks and the geographical coordinates of the honeypot site in question. Inferences cannot be drawn from the sensor network data as to the hackers' countries of origin. Most of the attacking IP addresses will be bot clients that are remote controlled over the Internet. The honeypot cannot see the locations of the command-and-control servers that are working in the background.

The security tacho provides a number of charts that illustrate the monthly distribution and technical alignment of cyberattacks. At the foot of the portal page there are three diagrams of information about the previous month. Two charts show the daily numbers of attackers and attacks. While the number of attackers remains relatively constant, the distribution of attacks reveals significant differences that are due to the nature of the underlying attacks. Botnets are largely responsible for these differences. Depending on what might be termed in their order position, they carry out very different attacks in terms of both quantity and quality. The third chart shows the distribution of targets. It reveals that 90 percent of the cyberattacks are on network services that the honeypots simulate.

NEW: CYBERATTACKS BY TARGET COUNTRY

On request the security tacho's live ticker shows the number of current cyberattacks on sensors in a specific target country. The tacho processes information from honeypots in the country in question in real time.





If the visitor runs his mouse cursor over a country, the number of current attacks is faded in.

NO CHANCE FOR SMARTPHONE HACKERS
SIMPLE RULES FOR MOBILE SECURITY

Hackers have set their sights on smartphones as well as PCs, but by observing five simple rules you will not need to lose sleep over your mobile terminal device's security.

Smartphone users can protect their content from unauthorized access by using a device password. A combination of letters and numbers is best.

Smartphones have indeed become increasingly popular with hackers. In principle threats come from two sides. For one, cybercriminals aim to spy on smartphone users to steal their personal data; for another, they try to gain total control over mobile devices in order to use them for their own purposes. Online banking access data or credit card details enable them to plunder the mobile user's bank accounts. Contact data from the user's address book and other personal information can be used for social engineering. The hacker here uses the data he has acquired to establish a false identity and come by confidential information or services from certain persons. The more the hacker knows about his target person or the better he knows the person he is impersonating, the more successful he will be at his fraudulent business.

Gaining total control over a device is an attractive proposition for hackers for a variety of reasons. Hackers use hacked phones to utilize costly premium services or make calls without the owner noticing. The rude awakening comes at the end of the month when the phone bill is higher than expected. Other hackers specialize in using hijacked devices to send spam or use them as part of a mobile botnet to attack server systems (for more about botnets read the article on page 13). In principle malware-infected smartphones can be used for all of the dirty work that hackers get up to with hijacked PCs. Our mobile companions are, after all, no longer mere telephones but extremely powerful pocket-sized computers.

MOBILE BOTNETS ARE ESPECIALLY ATTRACTIVE

"Unlike PCs," says Wolfgang Bollenbach, head of the Security Team, Office and Communication Services at Deutsche Telekom, "mobile terminal devices are online more or less around the clock. That makes them especially interesting for hackers." If a cybercriminal wants to launch a coordinated attack at a specific time, a mobile botnet gives him greater planning security. While most PCs owned by working people are switched off during the day while they are at work, hackers can work on the assumption that the overwhelming majority of mobile devices they control will be connected to the Internet at any time. "And with the new LTE data throughput rates," Bollenbach adds, "a mobile botnet will soon be more powerful than a traditional botnet of hacked PCs."

Smartphones become part of a botnet of this kind if the user downloads an app that exploits security vulnerabilities or weak points in the mobile operating system. The user can also infect himself with malware by clicking on a link in an e-mail. Toward the end of 2012 the first major botnet for the Android OS with over 10,000 users was identified in the United States, while in summer 2013 a complex Android Trojan hit the headlines by exploiting three previous unknown vulnerabilities in the operating system. The Trojan was able to read all kinds of data and send it to the hacker over the Internet, to use expensive premium services unnoticed and to latch onto adjacent devices via Bluetooth and WLAN. Installing the malware was only possible, however, if the user had authorized the installation of apps from sources other than the Google Play Store. "Users should not authorize this option in their system settings," Bollenbach advises.

JAILBREAK CANCELS OUT SECURITY FUNCTIONS

"The greatest risk faced by mobile terminal devices," he adds, "is to be found in the different versions of their operating systems." For Android devices in particular a large number of different terminal devices is on sale which in some cases use outdated versions of the operating system. That is partly because the manufacturers fail to provide system updates at short notice, but devices with an outdated operating system then no longer comply with the latest security standard and have vulnerabilities that were dealt with in later versions. Malware is especially dangerous with devices manipulated by means of a jailbreak (iOS) or by rooting (Android). Manipulation cancels out fundamental security functions and enables apps to potentially access system functions that the manufacturer has locked. "That," Bollen-

bach explains, “is why all users should install software updates regularly and not manipulate their smartphones themselves or let others do so.”

Even quite ordinary apps can pose a security threat to the user’s data. During installation an app demands access to certain functions of the operating system in order to function properly. Navigation software, for example, will require access to the smartphone’s GPS receiver in order to establish its location. Communication apps want, as a rule, to read the address book and transfer the user’s contacts to their program interface. Yet many apps demand dubious and at times additional rights that have nothing to do with their actual functionality. Must the communication app relay the user’s contact details to the Cloud? “For some users that might be practical,” Bollenbach says, “but at least in a business environment it is strictly unadvisable.” When a torch app requires access to your address book, the alarm bells should definitely start to ring. “In order to protect sensitive data,” Bollenbach adds, “smartphone owners should read the instructions carefully before installing an app.” If the software wants too many authorizations, they would do better not to install it.

SECURITY AT TELEKOM HOTSPOTS

Deutsche Telekom recently made its HotSpots even more secure. Smartphone and tablet owners with iOS and Android devices can now fully encrypt their connections with a Telekom HotSpot by means of a secure VPN tunnel. Setting up the encryption takes only a few steps and it is available free of charge.

For further information about VPN encryption by Telekom visit
www.telekom.de/hotspot-verschluesselung

FIVE HINTS FOR MOBILE SECURITY

At work or in private life, if you observe these simple rules you will not need to lose sleep over your mobile terminal device’s security.

1. DON’T MANIPULATE

Do not manipulate your terminal device by means of a jailbreak (iOS) or by rooting (Android). By doing so, you will cancel out the mobile operating system’s standard security features.

2. USE ONLY OFFICIAL SOURCES

Only download apps from the official app stores (Apple App Store, Google Play). Apps purchased from these stores have passed the security check that manufacturers must pass to sell their apps there.

3. CHECK APP AUTHORIZATIONS

Check before installing it what rights the app requires. Free apps in particular frequently require dubious access rights that enable them to read, say, the contact data on the smartphone.

4. OBSERVE CONFIDENTIALITY

Make sure, before saving corporate data to Cloud resources such as Dropbox or iCloud, that you only save documents there that have the confidentiality level “public”. The US Patriot Act, for one, empowers US government agencies to access this data.

5. KEEP PERSONAL DATA SECURE

Check the sensitivity of content when using social networks like Facebook. Don’t give hackers any opportunity to steal identities and with them knowledge and values.

ROUTER INNOVATION PREVENTS SPAM MAILING

Telekom's new Speedport routers have a function that only permits mailing to a specific list of e-mail servers that the user can amend. All Speedport W724V routers and subsequent router generations come with this function that is activated as the standard setting. If required, the customer can make manual additions to the list or deactivate the function entirely. If a mail program on the user's computer tries to use another outgoing mail server, the mailshot will be stopped automatically. The router thereby prevents malware that may be on the customer's computer from sending out spam. This innovation was an in-house Telekom development and is currently solely available with Telekom's Speedport routers.

The Speedport W724V router has a new Telekom function that automatically prevents spam mailing.

SPAM IS DELETED AUTOMATICALLY

© tarabarscheffe – fotolia.com

"More than two thirds of the world's e-mail traffic are spam," says Telekom security expert Rainer Schmidt who wrote the router specification. Much of this unwanted mail is sent from the infected computers of private individuals. Installed malware frequently includes a mail program. The program reads, for example, the contact data in the user's address book or receives addresses to which to send spam from its controller. It then tries to send spam to the addresses identified or received. The malicious code often circumvents the infected customer's actual e-mail infrastructure (such as the T-Online e-mail server) and communicates directly with the incoming server of the address that is to be contacted. If the customer has one of the new Speedport routers, the journey ends there. If the URL or the IP address of the e-mail server is not on the list of trustworthy outgoing mail servers, the mail is deleted automatically.

E-MAIL MADE IN GERMANY

© bannosuke – fotolia.com

Deutsche Telekom customers have of late sent their e-mail even more securely. In August 2013 Deutsche Telekom and United Internet announced that mail sent by their users via GMX, T-Online and Web.de was with immediate effect being encrypted automatically on all transmission routes between their data centers and was only being stored at secure data centers in Germany. The partners reached this agreement within the framework of the Industry Initiative "E-Mail made in Germany" supplemented by an additional security standard with respect to their customers' e-mail communication.

Both providers process all data solely in accordance with German data protection requirements. They encrypt their customers' e-mail automatically. Neither technical expertise nor additional effort or expense are required. They are also introducing a label for e-mail addresses that will enable a user to see before sending a mail whether his recipient complies with the security standards of the e-mail alliance. The route from the terminal device to the mail server was already encrypted for all customers who used a mail application of the partners or had activated SSL encryption in e-mail programs such as Outlook. From April 2014 Telekom and United Internet are only sending SSL-encrypted mail, so that data traffic which is already transmitted encrypted between server systems will then be secure on all transmission routes within the mail alliance.

For further information about secure e-mail from Germany visit www.e-mail-made-in-germany.de

© cirquedesprit – fotolia.com

ABUSE TEAM MAIL WITH DIGITAL SIGNATURE

In future the Telekom Abuse Team will send mail to customers with a digital signature. From the end of October, mail sent by members of the Abuse Team via the Telekom e-mail center will feature a green trusted dialog check mark with which users are already familiar from trusted mailers like eBay, Otto and Postbank. "We send up to 25,000 e-mails a month to our customers," says Abuse Team member Nicole Riese. "Customers are sometimes not sure whether the mail really is from us." To prove the sender's authenticity, Abuse will in future use the DKIM (DomainKeys Identified Mail) signature procedure. It uses asymmetrical encryption to sign mail digitally and ensure the sender's authenticity.

CYBER ZOMBIES
BOTNETS TURN VICTIMS INTO OFFENDERS

Millions of computers around the world are part of a botnet without their owners being aware of the fact. Zombie computers often show no sign of symptoms as the bot goes about its work unnoticed in the background.


© jim - fotolia.com

The botnets are marching on. Botfrei.de, the industry association eco's anti-botnet advice center, estimates that up to a quarter of all computers on the Internet form part of a remote-controlled computer network. The extent to which illegal networks have expanded is indicated by the prices that cybercriminals pay for using them. For a mere ten euros a day they hire a bandwidth of two gigabits per second, which gives them sufficient computing power to create serious difficulties for more or less any company with a Denial of Service (DoS) attack.

BOTNETS SPREAD BY INFECTION

Malicious code used to be spread mainly by contaminated e-mail attachments, but the primary path of infection today are so-called drive-by attacks during a visit to an infected website. Microsoft Windows PCs continue to be the principal target. Specifically, cybercriminals have for 18 months increasingly focused on vulnerabilities in the Java runtime environment, whereas two years ago they concentrated on Adobe products (Acrobat and Flash).

Infections today are mostly the handiwork of commercial attack tools like the Blackhole exploit kit and others. These toolkits can be hired by the week and usually lend a hand within days of the news of a new vulnerability. Some developers go so far as to claim that vulnerabilities can be purchased in the black market.

BOT CLIENT MUTATES INTO MULTIPLE OFFENDER

After the initial infection additional malicious code is usually sent in. Its use ranges from mailing spam for advertising to large-scale Denial of Service attacks that involve a large number of bot clients simultaneously. Subject to the order situation, botnets involve their clients in a wide range of activities. Attacks are not infrequently aimed at the client itself. As its system files can be read in full, a key logger might be employed to capture the user's passwords and access data.

In keeping with the wide range of scenarios, many different malware programs are used. That is why bot clients are by no means limited to a single Trojan as many Internet users mistakenly assume. Over time the hijacked computers evolve into a kind of farm for breeding malware pests. In this way the bot client increasingly mutates into a multiple offender. To regain control of your computer, you would do well to take external advice. Valuable information is available from, for instance, the above-mentioned portal botfrei.de. Moreover, every ISP operates a so-called abuse service that informs customers about relevant threats and in the case of infection provides help to help you help yourself. Deutsche Telekom's Abuse Team can be reached at abuse@telekom.de.

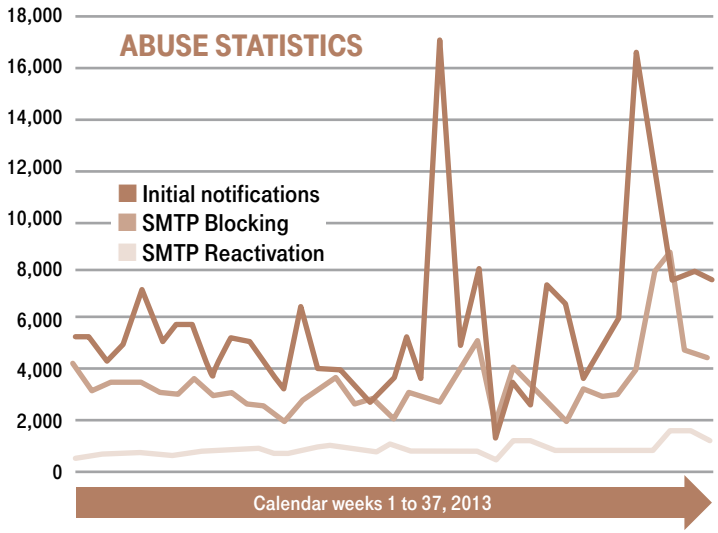
BOTNETS

Botnets are illegal computer networks that take over Internet-enabled computers without their users being aware of the fact. If a computer is part of a botnet, it can be remote-controlled by a so-called command and control (C&C) server. Botnets consist, as a rule, of many smaller, regionally structured networks. In this way their operators are able to pursue their activities all over the world. When the FBI and Microsoft took down the Citadel network in mid-2013, the investigators came across more than 1,000 smaller networks in 80 countries.

16,762 CUSTOMERS IN A WEEK
BOTNET BREAKS ABUSE RECORD

After the Citadel botnet was taken down, the Telekom Abuse Team was bombarded with reports of abuse. Within a week members of the team contacted 16,762 customers – more than three times as many as usual.

Until the end of May it was business as usual. The Deutsche Telekom Abuse Team informed an average 5,000 customers a week that their IP connections were being misused (see Abuse Management sidebar). The situation then changed abruptly. In a single week the Abuse Team sent out three times as many notifications as usual. A few days earlier the FBI had taken down large parts of the internationally operating Citadel botnet. The network specialized in stealing bank customers' data. Its operators are said to have stolen over $500 million in 18 months. It is claimed still to be partially active and its operators have yet to be apprehended.



HALF OF THE CUSTOMERS RESPONDED

The operation against the network has so far revealed 93,885 IP addresses of Deutsche Telekom customers. In the course of processing the abuse all of them were identified and notified. Experience has shown that around half of them act on the abuse specialists' advice and remove the malware from their computers. The others are contacted again. After a four-day waiting period Telekom blocks individual services that these customers use in order to stop the malware from spreading and to protect other Internet users. After the waiting period the number of computer shutdowns rose temporarily to over 8,000 per week, only to settle down at the usual 3,000 or so at the end of June.

ABUSE MANAGEMENT

Deutsche Telekom's Abuse Team receives around 1 to 1.2 million notifications per month of presumed abuse of its Internet services. Abuse is, for instance, if a customer's malware-infected computer is used to attack other computers

© alphaspirit – fotolia.com

or to mail spam via a Telekom Internet connection. Security organizations, Internet service providers and Deutsche Telekom's honeypots are among the most important sources of information. The Abuse Team checks the notifications for relevance, identifies the customers affected and sends them by e-mail and surface mail instructions on how to remove the malicious code from their computers. If attacks continue to be waged from a customer's computer, Abuse Team members initiate further moves. To protect other users they can temporarily block individual customer services such as the ability to send e-mail.

SEVEN DAYS IN WHICH TO REACT

The Abuse Team has seven days in which to follow up external information and identify the customers affected.

© Alexey Potapov – Fotolia.com

After seven days have elapsed, the IP addresses that were saved are deleted. This practice is in line with the provisions of the German Telecommunications Act and was last confirmed as being legal by the Frankfurt Higher Regional Court on August 28, 2013.

INTERVIEW

Markus Weyrich
Telekom Abuse
Team member

BEWARE OF UPDATES!

Phishing was yesterday. Botnets now have much more effective ways to take control over other people's computers. Markus Weyrich, a member of the Telekom Abuse Team, explains what users need to know and how they defend themselves successfully by simple means.

How do botnets manage to take control over Internet computers?
Markus Weyrich: In a wide range of ways. E-mail phishing was long considered to be the ideal way to do it, but user awareness has increased to such an extent that next to nobody is caught in this way any more. So botnet activists have resorted to other methods. The method most frequently used by far at present is the so-called drive-by infection. It uses well-camouflaged malware such as the ZeroAccess Trojan that is currently giving our customers the most trouble. At the end of August we had to notify three times more customers than usual that their computers were infected – three times more than we need to notify in normal weeks (see chart on page 14).

How does this pest go about its dirty work?
Markus Weyrich: Infiltrated Web servers on which cybercriminals have installed their malware are the starting point. Drive-by infections then typically take place in consecutive stages. If an Internet user visits an infiltrated website, the malware first checks his computer for standard vulnerabilities. The attackers often exploit their victims' good nature. A victim may be given to understand that there is a new software update for a popular application or that an additional component must be installed to play a certain film. Insidiously, the attackers use the very technologies for which users have grown accustomed to frequent updates such as Java, Adobe products or the Internet browser add-ons. By taking up the fake update offer, the victim throws the door wide open for the botnet to install any amount of malicious software on his or her computer.

How can I as a layman tell which update notification can be trusted?
Markus Weyrich: Well, even a professional has to look very closely to distinguish a bona fide notification from a well-made fake. That is why we advise all users to consistently ignore pop-up checkboxes and switch to the software manufacturer's website instead and download the update from there. That may not make life any easier but it is a sensible precaution and a highly effective way to limit uncontrolled growth on our computers. Once we assumed personal responsibility for updating software, we will think much more carefully about whether we need the application and what we need it for.

Are there any other points that Internet users should bear in mind?
Markus Weyrich: There are. Yet in the final analysis there are not really that many of them. To start with the most important advice of all: only visit the Internet when you are registered as a dedicated user on your computer. Malware will then have no access to the administrator's right to make itself at home on your computer. If you surf the Net as an administrator, you run every risk in the book. You should also ensure that your operating system is updated regularly and that the security tools which come with it, first and foremost the operating system's firewall, are activated. If you then also use an up-to-date virus scanner, you will have done everything that an ordinary Internet user should do.

ZEROACCESS

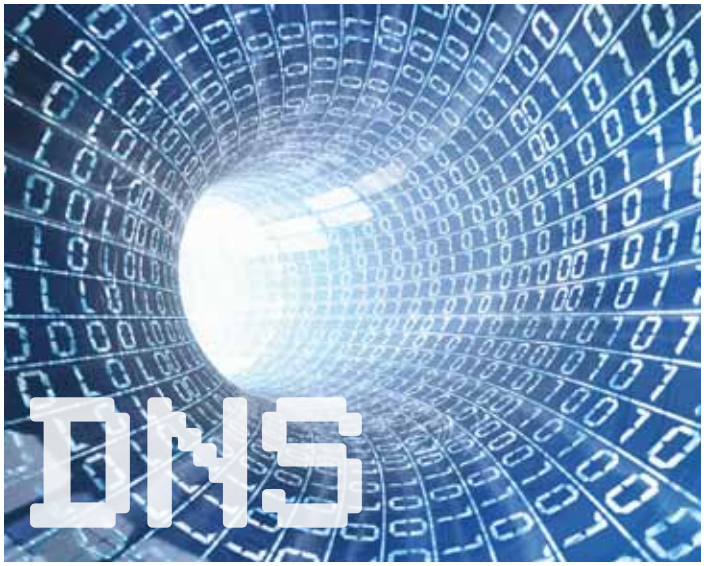
The ZeroAccess Trojan attacks Microsoft Windows operating systems. It loads additional malware onto an infected system to set up a botnet. ZeroAccess uses rootkit techniques to conceal itself from the user.

NEW THREAT TO WEB INFRASTRUCTU
DANGEROUS MISCONFIGURATIONS IN

Reflected Denial of Service (DoS) attacks are up to 60 times more powerful than conventional DoS attacks. They pose a threat not only to the ICT systems of the companies they attack but also to parts of the Web infrastructure. Deutsche Telekom is taking part in a provider initiative coordinated by ...

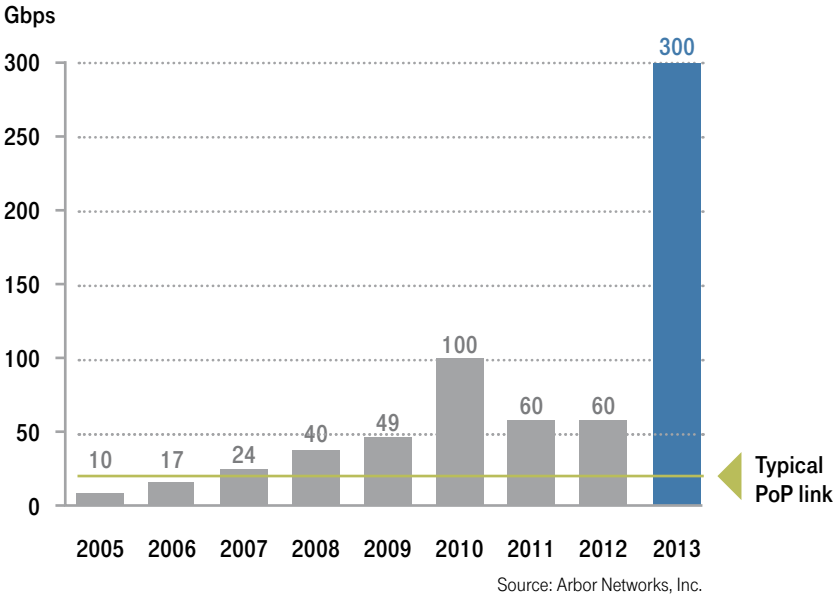
Keeping DoS attacks at bay is part of every Internet service provider's daily business and the threat situation has grown significantly more serious since the end of 2012. Alongside classic DoS attacks (see info box) Reflected DoS attacks are now making an appearance. In this kind of attack the attacker uses open DNS servers that are accessible to everyone to boost the bandwidth of his DoS attack 30-fold to 60-fold.

The most powerful attack of this kind registered to date was aimed at the anti-spam organization Spamhaus Project where traffic peaks of up to 300 gigabits per second (Gbit/s) were measured in March. That was more than enough to overload not only the actual target but also the network infrastructure connected to it. The access servers of a broadband network are typically designed for a data throughput of 20 Gbit/s. A Reflected DoS attack exhausts this bandwidth in one fell swoop, leading to service outages at all companies and of all private customers' connections that use the access server.



© alphaspirit – fotolia.com

THE MOST POWERFUL DDOS ATTACKS



The bar chart shows the largest known DDoS attacks since 2005. The line at 20 Gbit/s marks the typical capacity of a broadband access server. In 2013 the most powerful DDoS attack that has yet been known to happen in the history of the Internet took place. It was aimed at the anti-spam organization Spamhaus.

DISTRIBUTED DENIAL OF SERVICE (DDOS)

Denial of Service (DoS) attack is the generic term for attacks on the availability of network services. It most often takes the form of bombarding a target system such as a Web server with queries so that it is barely or even no longer able to respond to queries by regular users. If an attacker uses a large number of synchronized computer systems for an attack, it is referred to as a Distributed Denial of Service (DDoS) attack.

RE
DNS SERVERS

... the Federal Office for Information Security (BSI) to develop timely action against this new form of attack. The focus of collaboration is on open DNS servers that cybercriminals abuse in order to boost the bandwidth of their attacks many times over.

REFLECTED DENIAL OF SERVICE ATTACKS

A Reflected Denial of Service attack is launched, like a regular DoS attack, from computers that cybercriminals have taken over without the users' knowledge and interconnected to form a botnet (see article on page 13). The first fundamental difference between them is that the attacking bot client does not send its query directly to the victim. Instead it addresses an open DNS server that can be accessed across the network and answers queries by any Internet user. The most common query is "Tell me the IP address of an Internet domain" (such as www.telekom.de). The attack continues with the DNS server sending its answer not to the bot client that made the original query but to the computer the attack is targeting. Redirecting the answer is the work of a camouflage technique known as IP spoofing. This technique enables attackers to use the victim computer's IP address as the sender of the query (see sidebar "Traceability is impossible").

TRACEABILITY IS IMPOSSIBLE

A Reflected DoS attack cannot be traced. The IP spoofing camouflage technique enables a botnet to change the source identifier of its queries. Instead of the IP addresses of the bot client that submitted the query the DNS server is provided with the IP address of the computer that is targeted. All that shows up in its log system is the IP address of the abused DNS service, so tracing the attack is impossible. To rule out the possibility of bogus queries being sent from its own DSL network, Deutsche Telekom checks all outgoing queries for IP spoofing. Telekom cannot tell whether queries from other networks have the right sender. That is something only the other network operator can check.

Many Reflected DoS attacks develop considerable leverage in order to increase their impact many times over. An attacker may, for example, call on an open DNS server to send all of an Internet domain's IP addresses at once. In this way a query that is only few bytes long can trigger as a reply a data packet that is kilobytes in size. By making maximum use of the protocols' mechanisms, botnets can increase the bandwidth of a Reflected DoS attack by a factor of between 30 and 60. If, for instance, an attacker uses 200 bot clients each of which have a 1-megabit DSL connection, a query volume of up to 0.2 Gbit/s can be generated. Boosted by a factor of 50, the potential impact of the attack is increased to 10 Gbit/s. In this way even a smaller botnet can pose a threat to a large corporation's Internet connection.

ELIMINATING DNS VULNERABILITIES ACROSS PROVIDERS

To avoid Reflected DoS attacks, Internet service providers must control the open DNS servers in their networks. This is by no means only a matter of the provider's own systems where any existing vulnerabilities can be eliminated at relatively minor expense. The main burden of the work is on DNS services that are incorporated in the customers' DNS services. According to a preliminary market estimate Deutsche Telekom assumes that there are at least 25 kinds of DNS system and that they are built into hundreds of widely different ICT products.

Overall, providers have an extraordinarily heterogeneous system world to deal with, but regardless of that they must provide their customers with easy-to-understand instructions on how to configure the DNS services of their products, so that only authorized users can access them. To assign the documentation work that is required to as many shoulders as possible, the Federal Office for Information Security (BSI) has set up a working group of leading Internet service providers. Deutsche Telekom is involved intensively in this collaboration which gets under way in October 2013. The aim is to set up by mid-2014 a Web portal where instructions for all standard DNS servers are stored.

ON THE TRAIL OF SECURITY BREACHES
INTERVIEW WITH BERND EßER

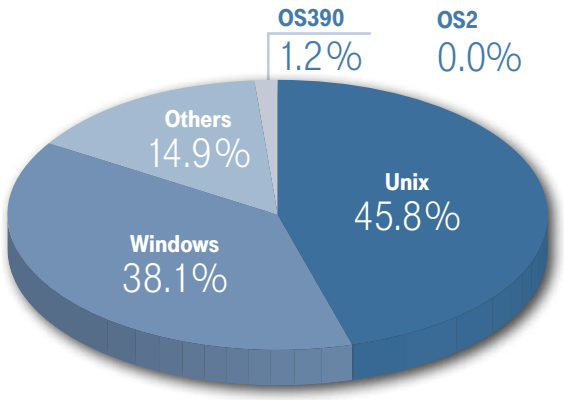
Managing security instructions is one of Deutsche Telekom CERT's core tasks. The starting point are security alerts issued by hardware and software manufacturers about vulnerabilities in their products. CERT receives more than 100 of these security advisories per month. They contain an initial risk assessment and basic information on how to deal with the vulnerabilities. CERT specialists check what damage these security breaches can do to the ICT systems of customers and employees. If action is found to be required, CERT issues guidelines for Deutsche Telekom Group system managers to show them how the security breach can be closed. Bernd Eßer, head of CERT, explains which technologies are the worst affected and how critical security breaches can be identified in a timely manner.

The number of vulnerabilities identified continues to be high. Is that a permanent state of affairs to which we must accustom ourselves?
Bernd Eßer: Well, hope springs eternal, of course, but realistically we must assume that the present level will be maintained. New security gaps are constantly coming to light even in IT products that have been on the market for years and are frequently updated and improved. An outsider might well imagine that the search for vulnerabilities stands little or no chance of success. But the opposite is the case.

So we cannot sound the all clear anywhere?
Bernd Eßer: I can't see where. To gain an idea of the dynamism that is involved, it is worth considering two fundamental trends that will continue to accompany us in the years ahead. One is the ongoing triumphant advance of the Internet Protocol (IP). With every IT system and every communication service that the protocol pervades IP-assisted methods of attack gain an additional target. That is especially apparent in consumer electronics. More and more devices such as TV sets have additional functions for which they need to be connected to the Internet. Manufacturers must take precautions to ensure that hackers stand no chance of gaining control over cameras, for example, or hacking e-mail accounts.

Where is the second trend?
Bernd Eßer: In operating systems where for years a far-reaching process of standardization has taken place. From the hackers' viewpoint that means two advantages at the same time. For one, they can focus their resources on a few platforms in order to identify fresh vulnerabilities. For another, they can sell their hacking expertise at a significantly higher price, if the operating system in question covers accounts for an increasingly large share of the user market.

DISTRIBUTION OF SECURITY ADVISORIES BY OPERATING SYSTEM BETWEEN JANUARY AND AUGUST 2013



Talking of operating systems. Most security advisories by far still relate to Microsoft and Unix, with Unix even heading the list. Why is that the case?
Bernd Eßer: For communication reasons. In Microsoft's case we have a process that the manufacturer controls, whereas in the Unix world the users generate the information. The predominant operating system, Linux, is an open OS in which every user is at liberty to look for vulnerabilities and to publish his findings. Microsoft too has this type of responsible user but third-party vulnerability researchers have, as a rule, undertaken not to make their findings public by themselves.

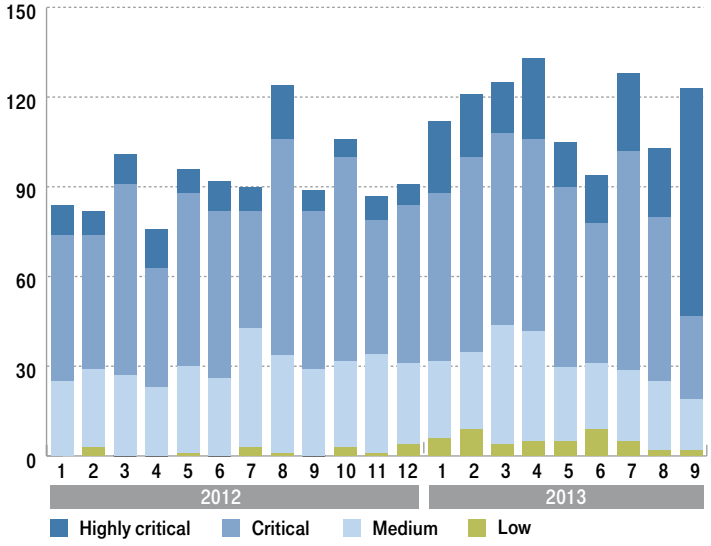
So much for operating systems. Where do we stand on applications? Where are the biggest construction sites in this area?
Bernd Eßer: Java, Internet Explorer and Adobe continue to account for the bulk of our work. Of this almost classic trio the Java platform leads the field yet again this year. Since January we have received security advisories about serious Java vulnerabilities almost weekly. In terms of criticality, however, Internet Explorer advisories are also strong contenders. Two instances caused an especial stir, with the manufacturer's counter-measures taking so long to appear that the Federal Office for Information Security saw fit to advise users to use other Web browsers. In terms of advisory management that is the last resort.

Bernd Eßer
Head of Deutsche Telekom CERT

How does Deutsche Telekom assess the criticality of vulnerabilities? Are there generally comprehensible approaches that lead to reliable figures?

Bernd Eßer: There are. We use the industry standard CVSS to filter out of the flood of security advisories those that are of practical relevance for our business solutions and for our customers' systems. CVSS stands for Common Vulnerability Scoring Standard and is based on three kinds of criteria. It first examines how costly and time-consuming it is for attackers to exploit a vulnerability. The second category of criteria relates to who knows what about a vulnerability. The key issue here is whether functioning defense mechanisms already exist or potential attackers are still ahead of the game. The third category takes into account which ICT systems are affected by a vulnerability and how high their specific threat potential is. On the basis of these criteria the CVSS standard rates criticality on a scale from 0 (uncritical) to 10 (highly critical). We use this rating to classify in four categories the vulnerabilities that are important for us and for our customers. The only categories that really require action are "critical" and "high."

NUMBER OF SECURITY ADVISORIES PER MONTH BY CRITICALITY



DEUTSCHE TELEKOM CERT

The Cyber Emergency Response Team (CERT) ensures that the Deutsche Telekom Group's information and network technologies can continue to function reliably in the event of an attack. Along with a maximum of technical expertise, CERT employees have an in-depth knowledge of the Group's lines of business and workflows. This enables them to assess reliably how seriously newly discovered technology vulnerabilities pose a threat to Telekom or its customers. Deutsche Telekom's CERT can be reached around the clock by customers at cert@telekom.de.

COOPERATION MEANS MORE SECURITY

When third-party informants alert CERT to a vulnerability in a Telekom service, CERT gets to work right away. It did so, for example, when it transpired that hackers could in theory delete Telekom customers' e-mail, if users failed to log out when quitting the E-Mail Center. CERT employees devised an ad hoc workaround to ensure that this vulnerability could no longer be exploited. After this provisional first aid Telekom reprogrammed the service module in the E-Mail Center and closed the security breach permanently. As a rule, CERT employees come up with a workaround in a matter of hours and it often takes only a day or a day and a half to eliminate the vulnerability once and for all.

FOREWARNED IS FOREARMED
STRATEGIC THREAT RADAR IDENTIFIES CYBERTHREATS IN GOOD TIME

Deutsche Telekom CERT's Strategic Threat Radar illustrates the development of cyberthreats. It is a tool that enables the company to identify threats and plan counter-measures in good time.

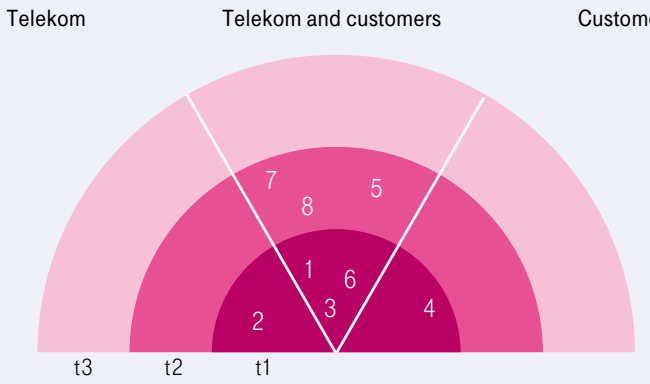
To assess threats accurately and arm yourself against them, you need to identify them at an early stage. That is why Deutsche Telekom CERT operates its Strategic Threat Radar that maintains a constant watching brief on latest developments such as a presentation by US security expert Charlie Miller that caused a furor at the Def- con hacking conference in August 2013. He and his colleague Chris Valasek had succeeded in breaking into the computer controls of a Toyota Prius and a Ford Escape and taking over control of the vehicles. The IT specialists also hacked critical driving functions and operated the steering wheel, brake and gas pedal from their laptop. They gained entry via the cars' bus system, a standard industry protocol via which the vehicles' micro-controllers share information.

"In theory it had for years seemed likely that CAN bus systems could be compromised, but the US colleagues have now come up with the practical proof, the proof of concept," says Bernd Eßer, head of Telekom's CERT. Threat situations in general grow more serious when proven in practice. "Proof of concept is an important milestone in our threat education. If it is furnished for a vulnerability, we develop methods to close the gap before an attacker can exploit it. Telekom was not affected in this case by a change in the risk situation, but it is becoming clear that cross-industry collaboration in exchanging protection and security concepts is required," Eßer explains. Protective measures that are well-known in classical IT environments might be applicable to new areas of use such as vehicle control. "It is important not to take too narrow a view of threats. Scenarios with reverse conclusions might be possible," he continues.

PREVENTIVE EDUCATIONAL WORK

As soon as the potential threat, posed by a vulnerability, changes, CERT alerts its partners or all of the product and system managers at Telekom whose lines of business it affects. As its central means of communication CERT uses its Strategic Threat Radar which provides business units with reliable information to enable them to assess business risks that cyberthreats pose. Preventive educational work enables Telekom to plan ahead for essential security measures and to implement them precisely.

STRATEGIC THREAT RADAR



THREATS

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

DEVELOPMENT STAGES

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

WHO IS THREATENED?

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

RADAR ASSESSES EACH NEW THREAT

"We have between 15 and 25 new threats a year that are of relevance for Deutsche Telekom's business fields," CERT's Bernd Eßer says, stating numbers. Before a threat is taken up Deutsche Telekom's radar developers clarify three key issues:

1. What stage of development has the vulnerability that poses the threat reached? Is it only known theoretically? Is it a practicable mode of attack? Are hackers already using it?
2. How likely is it that the vulnerability will actually be exploited? How much time and effort will it take attackers to gain access to the systems affected?
3. What damage can it do to Deutsche Telekom and its customers?

WHAT THREATS ARE WE FACED WITH?

CERT is currently monitoring 60 threats. Eight of the most popular threats are listed (left). Six of them (below) affect both Telekom customers and Deutsche Telekom itself:

- **Advanced persistent threats (1):** Private and business users are subjected to continued attacks using different tools.
- **Mobile malicious code (3):** Malware from app stores takes over mobile terminal devices to use them in, say, botnets.
- **Denial of Service attacks on DNS infrastructure (5):** Mobile malware attacks IP-based network components to set up mobile botnets.
- **Attacks on DSL routers (6):** Malicious software affects routers and modems with security settings that are too weak.
- **Attacks on automotive CAN bus systems (7):** Hackers force their way into the computer controls of vehicles and take over control of driving fuctions.
- **Attacks on smart TVs (8):** Vulnerabilities in smart TVs and set top boxes enable hackers to steal user data.

HOW FAR HAS A THREAT BEEN DEVELOPED?

The more advanced the stage id that a threat has reached, the more central its position is on the radar. The inner circle **(t1)** contains known security vulnerabilities that hackers are already exploiting. The middle circle **(t2)** is reserved for vulnerabilities that have been proven to be exploitable. The outer circle **(t3)** contains theoretical threats. When the CAN bus threat's proof of concept was made public (see above), it moved from the outer to the middle circle.

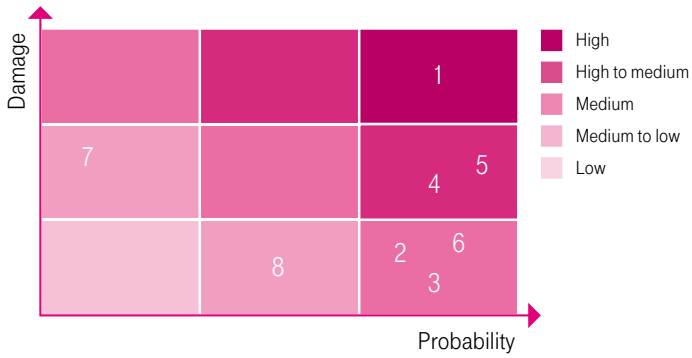
"Wherever possible we quantify the damage," Eßer explains, "but specifying amounts in euros is not trivial. We are mostly dealing with theoretical threats. Reliable information about a potential attacker's intentions and the attack scenarios is rare." Assessing new threats reliably is one of the most exacting tasks of radar development. To make its findings comprehensible, Telekom often relies on standardized methods like the CVSS procedure (see interview on page 19).

BOT ATTACKS WARDED OFF SUCCESSFULLY

This differentiated approach gives product managers a valuable information advantage, so that they can protect their systems in good time. These include mobile Internet offerings. In Spring 2012 a threat moved into the radar's inner circle that had previously been seen as theoretical. It basically involved connecting smartphones to set up botnets with a view to damaging material parts of the network infrastructure. A mobile network's DNS servers that connect a website's clear-text name with its IP address are a potential target. A DNS server failure would lead to mobile surfers only being able to visit a website, if they knew its IP address off by heart which is impossible.

"We took the threat very seriously and immediately approached the colleagues whose job is to develop the mobile networks. Although they were working flat out to adjust network capacities to the rising tide of demand, we quickly found a solution that enabled us to protect the DNS servers on a lasting basis," Eßer recalls. This swift action paid dividends. Since the end of 2012 Deutsche Telekom has registered bot attacks on DNS servers in mobile networks. All have been warded off successfully because the threat was identified and dealt with in good time.

RISK PORTFOLIO



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

The risk portfolio documents the findings, with the main focus of the analysis on how likely to occur the risk is and how much potential damage it can do. A matrix shows how security experts currently assess the situation.

MORE TRANSPARENCY, PLEASE
INTERVIEW WITH INTERNETWACHE

Sebastian Neef and Tim Schäfers are technology-minded young hackers who work for security on the Internet. They jointly run Internetwache, a project that checks the security of websites and alerts their operators to any vulnerabilities they find. They have helped Deutsche Telekom on several occasions. In this interview with the Security Report Sebastian Neef explains what motivates him and how companies that he contacts react.

What exactly do you do at Internetwache, Mr Neef?
Sebastian Neef: We check the websites of companies of all kinds to see if we can find security vulnerabilities. If we find any, we contact the site operator so that he can deal with them. We don't hack the sites ourselves but merely check whether it would be possible to do so. The way a website behaves often shows us that it has a vulnerability. We also use tools like the intercepting proxies BURP and ZAP to take a closer look at a site. Using these tools we intercept HTTP traffic between the Web browser and the website's server and check every query.

Why do you do it?
Sebastian Neef: When I started to program websites and smaller projects I was struck by the number of reports of hacked companies and customer data. I wanted to know how it was done. Then I realized that I too visit websites and use online services. So I began to check them for vulnerabilities. Curiosity and fun eventually led to our Internetwache project. We want the Internet to be safer. Internetwache is also a good reference project for my career. At present I am a third-semester computer science student but Mr Schäfers and I also conduct security audits.

Which security vulnerabilities do you generally discover?
Sebastian Neef: There is a non-profit organization by the name of OWASP that, much like us, has set itself the task of improving the security of applications and services on the Internet. OWASP stands for Open Web Application Security Project. Once a year OWASP publishes a list of the Top Ten most widespread security vulnerabilities. It tallies with our observations. So-called cross-site scripting vulnerabilities – also known as XSS vulnerabilities – more or less head the list. They enable a hacker to execute JavaScript code, for example, in the contact form of a Web shop or forum.

Programming a website does not normally allow code of this kind to be executed in the context of a website, but just a small oversight in programming the output can make it possible, enabling a hacker to smuggle his code into the website. When another Internet user visits the hacked contact form, the data that the hacker has manipulated can be sent to his browser. That, for example, is how hackers carry out phishing attacks. Furthermore, we often come across SQL injection, local file inclusion and the far less frequent open redirect vulnerabilities.

How do website operators react when you approach them?
Sebastian Neef: That varies widely. At many companies our first problem is that we have no idea who to contact with our information. There is no contact address and the employees we contact do not see themselves as being responsible. Companies like Telekom or Google are another matter. Telekom has CERT which is indeed responsible for just such queries and responds very fast. As a rule, CERT sends us within a day an e-mail confirmation stating that the appropriate departments have been set to work on the issue or that the security breach has already been closed. But not every company can afford a CERT. Small firms can certainly not be expected to do so. Communication then becomes a somewhat more protracted business.

TELEKOM LAUNCHES BUG BOUNTY INITIATIVE

On October 28, 2013 Deutsche Telekom launched a bug bounty program. Third-party informants are requested to report security vulnerabilities in the telekom.de domain's Web portals confidentially. This initiative is based on a responsible disclosure policy. Telekom asks security researchers to report vulnerabilities confidentially and undertakes to close security breaches as quickly as possible within an appropriate time frame. Informants' commitment is rewarded. A single remote code execution vulnerability can lead to a reward of up to EUR 5,000 subject to the criticality of the system used.

For the conditions of participation and further information about Telekom's responsible disclosure policy visit **www.telekom.com/bug-bounty**

"I would like more companies to be transparent about how they are improving the security of their Internet services."

Sebastian Neef
Media informatics specialist and co-founder and operator of the security portal internetwache.org

What would you like website operators to do to improve security on the Internet?

Sebastian Neef: Companies should be transparent about the measures they undertake to improve the security of their Internet services. I would also like to see every company that has a website or an online service to operate a responsible disclosure program. Security researchers should be able to report vulnerabilities confidentially before a cybercriminal can exploit them. It would be good if companies were to reward the work that analysts undertake free of charge with a mention on their website or a modest cash reward for the vulnerability they have discovered.

That is not very widespread in Europe yet. American companies adopt an entirely different approach. Many of them run bug bounty programs and mention and commend informants in a Hall of Fame on their websites. In order to operate a program of this kind, you must, of course, be strong enough to own up to the fact that security vulnerabilities can happen. If more companies were ready to deal with this issue openly and actively, cybercriminals would stand significantly less of a chance to to get up to their dirty tricks.

WIDESPREAD SECURITY VULNERABILITIES

An **SQL injection vulnerability** enables a hacker to execute MySQL code in a system and possibly read, amend or delete data.

Local file inclusion vulnerabilities in script-based Web applications enable hackers to smuggle program code into the Web server and execute it.

An **open redirect vulnerability** enables attackers to manipulate the links on a website and redirect visitors to other destinations.

WLAN TO GO WITH BUILT-IN SECURITY

WLAN TO GO is set to become the world's largest HotSpot network. Deutsche Telekom ensures by means of a special router specification that customers can share the unused bandwidth of their DSL connection with others without the slightest security concerns. To participate in WLAN TO GO, customers need, in addition to their IP-based Telekom connection, a Speedport W724V router. The security experts at Deutsche Telekom's Group Information Security department drew up the security specifications required of the manufacturers of this router and checked that they were observed. The Speedport router transmits two separate WLAN signals and thereby sets up two totally separate networks. The first is encrypted and remains private, while the other appear on the HotSpot user's screen as a Telekom_FON access point. A HotSpot user who logs onto the FON network at his disposal has no opportunity to access the telephone subscriber's private WLAN network. Network devices from notebooks to storage are thus totally secure. And that applies in both directions: HotSpot users need to have no fear that the router's owner might be able to access their mobile terminal devices.

SECURITY ON THE INTERNET.

CONTACTS

Abuse Team
Deutsche Telekom AG
Group Information Security
Missbrauchs-Team
T-Online-Allee 1
64295 Darmstadt, Germany
E-mail: Abuse@telekom.de

Deutsche Telekom CERT
Deutsche Telekom AG
Group Information Security
Landgrabenweg 151
53227 Bonn, Germany
E-mail: CERT@telekom.de

Editorial Office
Deutsche Telekom AG
Group Information Security
Friedrich-Ebert-Allee 140
53113 Bonn, Germany
E-mail: CERT@telekom.de

LIFE IS FOR SHARING.