Using open source intelligence tools we revealed the vast amount of unprotected smart devices throughout Germany, enabling strangers to spy on people's homes via web cameras, access private data, control services installed as part of home automation systems or disrupt Internet services by misusing them for DDOS attacks. Our project was the cover story of the weekend edition and an editorial focus for a week at www.sz.de/iot

PAGE 1

Unprotected and Dangerous

More and more German households use devices that can be operated remotely via the Internet. However, many of the webcams and hard drives are easily accessible from the outside, by strangers. Pictures from the nursery, bank statements, passwords – everything ends up online. Everyone can access them, without breaking the law. Findings of a month-long SZ investigation

Hunter is sitting at the kitchen table, there is coffee and coke. He is holding his smartphone in his hand, a few meters away from him gleams an iPad on the wall. Steven Hunter, father of two children and employed in the automotive industry, says he can control the whole world with these devices, provided that he has an internet access. He is talking about his world.

Hunter's world is a smart home, a house that is largely controlled by digital technology. Either automatically or, if the owner wants it, from his mobile phone. Hunter's house is set up near Aachen, a city not far from neighboring Belgium and the Netherlands. He paid 30,000 euros for the digital technology and its installation.

Hunter can, for example, turn the sockets on and off when his children are playing near them. He can program the light switches to regulate patio lighting in the summer and the Christmas tree in December. He can open and close his garage via the system, move the blinds up and down, check the room temperature and see which windows are open or closed. The technique, hidden in a gray box in the utility room, knows no limits, it is almost arbitrarily expandable. That may sound futuristic, but has already became an integral part of everyday life: By 2018 there will be around 720,000 smart homes throughout Germany.

There's just one problem. Steven Hunter is able to control his world – but everyone else can control Hunter's world, too. Because the central operation of his home automation is accessible to anyone who has a computer with an internet connection. Hunter's house is completely unprotected.

A team of Sueddeutsche Zeitung investigated cases like the one of Steven Hunter for several months. These cases don't only concern smart homes but also the most diverse devices, from vehicles to buildings which are connected to the Internet. They also include toasters, washing machines, rifles, cars, saunas, mailboxes, children's dolls, even sex toys ... the list could be continued indefinitely.

During their research SZ reporters found webcams showing sleeping babies. Pictures from the nursery accessible by anyone who can open up a browser. External hard drives containing secret documents or private photos, the most intimate details of a stranger's life. There are industrial plants, for example wastewater treatment plants whose technology is openly available, and shops like the thousand square meters large furniture stores whose heating can be turned up and down from the outside by everyone at will.

You do not have to be a hacker to do this. The Internet provides special search engines for smart devices, just like Google being a search engine for websites. For this research, the Sueddeutsche Zeitung used the search engine shodan, available at shodan.io. Upon request it spits out a random list of all the internet-connected, unprotected devices it finds. The list can be filtered, for example by countries.

This search works quite reliably because the devices, be it a webcam or an external hard drive, are usually always online. After all, many people want to control their home technology when they're out and about, too. Let's say someone sets up a webcam in his house and connects it with his WLAN so that the device is online and he thus can see what the webcam is currently filming. Many users in this situation would think that their connection is secure because they encrypted their WLAN. In fact they would have to secure the webcam itself, for example with its own password. Without this extra backup the webcam tears a gap in the originally secure network, and the pictures of the camera are now visible, theoretically for everyone online. During this research SZ reporters discovered thousands of such unprotected accesses, not just connected with webcams, but with various devices. Just like the controller from Hunter's smart home.

If anybody would have found the house of family Hunter with the help of shodan, they would have been able to view their control system in their own browser. This is the same browser with which you would otherwise read the news on sueddeutsche.de or spiegel.de. And you could easily open the garage of the Hunters. Whoever wants to know exactly where the house is situated either to break in or to steal the car has only to combine a little: shodan displays the approximate location of the house, references to the Hunter family's last name can be seen in the home control which is visible online (which is why we changed it in this text). The rest comes down to the phone book and Facebook.

Not all devices and buildings are as vulnerable as the Hunter's one. Nuclear power plants or aircrafts can – if at all – only be cracked by professional hackers. And password-protected devices can be secure as well. But that is not the point of this research. This text is about the scores of unprotected devices that are already part of our everyday life. And in the near future, many products will only be provided with internet access. Not only because the new technology is convenient for the customers but also because it enables some manufacturers to collect usage data – for some inconspicuous market research.

The fact that those devices are unprotected is due to the manufacturers as well as to the customers. The users want a more comfortable life. A webcam in the nursery promises parents a relaxed evening in the city, an external hard drive at home which is accessible from the workplace makes everyday life easier. Hunter for instance says about his house: 'When we go out in the evening and start wondering if the iron is turned off, I just turn off the respective socket via my phone.' Taking care of security settings, setting passwords up and typing them again and again does not go together with the idea of a more comfortable life.

However, there are also low-cost manufacturers whose equipment can't be updated after a security vulnerability has been made public. Customers often have to deal with two manufacturers – the hardware producers who build the webcam as well as the software producers responsible for the operating system of the device. That makes things complicated. Whoever is liable for damages often remains unclear.

In homes or facilities the new technology is usually set up by installers and electricians. In their eyes the question of security is often limited to cleanly separate the wires behind the power outlet, though. Indeed, the security of digital, internet-enabled devices is complex. In Hunter's case, Siemens, the manufacturer of the most important parts of the smart home, writes the 'commissioning engineer' must 'create a suitable security concept in the process of planning.' Hunter's electrician neglected this.

Prior to starting this investigation, the team of reporters at the Sueddeutsche Zeitung had agreed on a codex. It states, among other things: 'If we land on a control surface, we do not press buttons or change settings.' This means: devices such as Hunter's home automation system were only operated after the persons concerned had given their explicit consent. The SZ team was thus able to turn off the light in Hunter's house from a computer in Munich while talking to the man on the phone. Most of the times, the last proof had to be made on the spot for ethical reasons, though.

So, a journey throughout Germany set in. It often led to people who just happened to be victims of unsecure technology without having bought a device themselves. In Cologne, for example, Claudia B. has worked for four and a half years as the head of a bakery store. The business belongs to the brand ‘Backwerk’, a franchise company. Its boss, whose name is Jan Kahrmann in this text, runs several branches in Cologne, one in Austria. Kahrmann has equipped its bakeries with safety technology, every square meter of the sales area is monitored. But the cameras sent all images into the web, easily to be seen by anybody, without Kahrmann’s and Claudia B’s knowledge. If you wanted to watch B. or one of her colleagues – either to stalk them or to break into their homes while they were at work – you could do that at any time.

During the research editors of the SZ in Munich could watch on their screen as two of their colleagues, who had traveled to Cologne, strolled through the local pastry shop; how the two waved in the security cameras that are installed over the counters with the lye pretzels and the fresh baguettes. Or to someone else, since no one knows who was watching at that moment.

When asked about the security flaw Kahrmann's technician commented: ‘That’s a big problem, we’re lacking an update.’ For a while the ‘Backwerk’ cameras indeed disappeared from the net. But in the end the problem outpaced the technician. After a few days everyone was again able to see Claudia B. at work, watch hundreds of customers doing their shopping. This is true as of today. Dusseldorf lawyer Udo Vetter, who specializes in internet law, calls this a scandal: ‘In addition to the violation of personal rights, this is also a violation against data protection law.’

The bakeries use the surveillance software ‘go1984’, manufactured by the logiware GmbH from Nordhorn in Lower Saxony, Germany. The SZ came across this software in many other cases as well. Upon a detailed request the company spokesman replied: ‘Thank you for your email whose unqualified content we do not want to comment on further.’

Legislators and consumer protection also hold back when it comes to the
Internet of Things. A seal of approval on the packaging that rates the security of such devices, does not exist. As a result a world has emerged in which commodities, but also buildings and industrial technology may be a threat to humans. The things that surround us develop a life of their own, they become the eyes and ears of our enemies.

What sounds like a thriller has long been commonplace. This normality is dangerous. The Federal Office for Information Security (BSI) notifies in writing most devices are ‘insufficiently protected against cyber attacks in their delivery condition and can thus be easily found by attackers.’ Often the affected people don’t notice that they have been attacked at all. The pervert who watches children over the unprotected webcam of their parents will hardly likely self-proclaim its security flaw. The intelligence service who makes a copy of an external hard drive of an officer of the German Federal military forces will leave no greeting card. And whoever intends to open Hunter’s garage to steal his Mercedes will barely trumpet his method.

In the end many devices designed to provide security make the lives of those involved more dangerous. The most important component in Hunter’s smart home is its alarm system. It was put in place to protect the house in the burglary-ridden region between the Netherlands, Germany and Belgium. Sensors in the door and window handles sound the alarm when they move unexpectedly. In case of danger the alarm is set off. Unless the burglar turns it off before breaking the door open. Up until a few days ago, anybody was in the position of doing just that.

Hunter has since reacted – and pulled the internet cable out of the wall in his utility room on the ground floor. His control system worth 30,000 euros is offline. His new alarm system is called Ricki. A German shepherd dog, ten months old and not connected to the Internet. At least not yet.

PAGE 2

Digital Tsunami

How criminals attack states and companies with botnets

Rob Graham, an information security expert from the US ordered a security camera for 55 dollars on Amazon. Barely delivered, he connects the camera to the Internet and starts a stopwatch. He doesn't have to wait too long. Mere 98 seconds later he realizes that the device is being attacked by a computer program from the Internet: the attacker uses Graham's camera over the net, without turning off its original function.

It is a particularly refined kind of an attack. This is not about spying on the owner of the camera but about assuming control over the alien device to launch a far bigger attack. Criminals start such attacks countless times every day; usually the devices are then considered part of a network of hijacked devices: This is called a 'botnet'. The operators of these networks consisting of thousands or millions of individual devices use this weapon to make websites like sueddeutsche.de collapse due to sheer overload.

Cybercriminals are taking advantage of the fact that internet-enabled devices – such as cameras, printers, routers, webcams – can access websites just like any normal Internet user. When many devices in a botnet are calling a specific webpage at the same time, the page becomes overloaded and crashes in the end. DDOS attacks is the term used for these cases. The abbreviation stands for Distributed Denial of Service which stands for a simultaneous attack by many devices at a common target.

Because more and more devices are located at home but should also be controllable on the road they are therefore unprotected connected to the Internet. As a result some botnets are huge and very powerful by now. The owners of the hijacked devices are often unaware of this. Jan-Peter Kleinhans, who is responsible for the Berlin thinktank 'Stiftung Neue Verantwortung' researching the Internet of Things says, 'If my router is infected and conducts a DDoS attack at three o'clock in the night, I wouldn't notice.'

The attacks do not have to be expensive, small botnets are available up from 30 euros on a day-to-day lease on digital black markets. Criminals use the networks in different ways. Some want to remove the website of a political opponent from the net, others want to force the stock market price of a company down by taking down its offer from the net. Many intelligence agencies also use the technology for their political goals.

The attacks are getting more aggressive. This fall a botnet of a never before known size called Mirai targeted a central part of the global Internet infrastructure. Many websites were no longer accessible, including Amazon and Paypal. The attack was mainly carried out with the aid of poorly protected, infected surveillance cameras and digital video recorders of a Chinese low-cost manufacturer. Another Mirai attack hit Internet service providers in Liberia. The attack was so massive that it was feared the whole country had to go offline.

Open House

Smarthomes are comfortable and energy-saving. But if unprotected, they attract burglars and voyeurs

Who likes to come home seeing two journalists standing in front of their house explaining why this specific house is so endangered? Sandra Wiesel (name changed) would rather prefer continuing her call on this autumn evening. But when she realizes what the surprise visit is all about, namely the safety of her family, she hangs up very quickly. Whether an internet affine teenager on Honolulu, a bored woman in Singapore or a burglar from Regensburg – everyone was able to control the house of the Wiesels in placid East Bavaria: open and close the garage door, turning blinds, lighting, temperature up and down. Even the fountain in the garden can be switched on and off. This confirms Sandra Wiesel's fears. She has always warned that her husband's hobby wouldn't lead to anything good. Despite the fact that he works in the field of digital technology.

Thousands in Germany encounter this issue just like the Wiesels and the Hunters (see page 11). Houses controlled via the Internet and smartphones are the new standard. Sometimes the owner does the set up himself, sometimes electricians install these automation systems by default.

The advantages: the central control should save energy and electricity through intelligent planning while allowing residents flexibility at the same time. The neighbor wants to deliver a package, but you are out of the house? No problem, the front door can be opened on the go via the phone. In addition, the intelligent houses with their sophisticated alarm systems protect against burglary.

Those who build today also rely on digital technology to uphold the resale value of the house. Manufacturers like Bosch and Siemens have expanded their offer ranging from central controls up to digitally networked thermostats. The US group Nest serves as a model. It is part of Alphabet, the group which Google belongs to. Manufacturers make sure that products from different brands work together in one house by now, hence analysts expect that the demand will continue to grow. But the comfortable life in a networked house entails significant risks: With the smart home, the home is literally connected to the Internet. This is especially convenient for certain criminals: burglars.

Interconnected keyhole

Be it a bedroom or salesroom – wherever surveillance cameras are running, people find themselves quickly on the net again

A young woman, almost a girl, wrapped in her winter coat, stares at the slot machine. She presses a button. Again and again. It's half past eleven in a gaming hall north of Dortmund, the largest one in proximity, it's noon soon. Security cameras are attached to the ceiling above the woman. The operator of the arcade places value on watching his guests lose their money. But the cameras of this gaming hall stream live to the Internet, the surveillance images of billiard tables, currency exchange and slot machines are openly available for anyone interested in watching. 24 hours, seven days a week: Theoretically everyone with an internet connection around the world can look at the young woman being taken in by the slot machine, pushing the button, again and again.

When the SZ confronted the management with its findings a technician gets in touch with the reporters: 'Everything runs via logins, only three people know the passwords.' He is wrong. A password was not necessary, the monitoring system of the arcade was openly accessible.

This incident is not an isolated case. Hundreds of webcams in Germany are openly accessible just like those in Dortmund. It's quite obvious that their users or the people you can watch via the webcams don't know about this. If you click through the streams, you will see anything from babies in their cots to a sleeping dark-haired woman – the webcam is directly aimed at her body. Or you can follow the girl with blond braids lying on a brown leather couch and watching TV.

The security flaws provide strangers access to many places: bedrooms, living rooms, bathrooms, shops and businesses such as the arcade near Dortmund or a pharmacy in the German city Stade, an Asian restaurant in Hamburg or boutiques in North Rhine-Westphalia. Not only the customers are filmed, but often also the employees – without their knowledge. Their personal rights are permanently injured.

Who is to blame? Sometimes the manufacturers of the webcams or the developers of the software were sloppy, then again the technicians or the users simply configured the devices too carelessly.

PAGE 3

Closing the gap

How to protect your devices from unauthorized access

The vast majority of devices – be it a webcam, a hard drive or the controller for the temperature in the winter garden – come with standardized presets. Often passwords are also set by default. Those are mentioned in the operating instructions or can be guessed quickly. Hence hackers have a particularly easy game when the username for the baby monitor is ‘admin’ (stands for administrator) and the password ‘0000’.

That’s why these settings should be changed immediately after the purchase; a how to is part of the manual which can be found online via Google, if you can’t find it anymore. But you should make sure that the settings can be changed at all before buying any device; this is not the case with some devices. The Federal Office for Information Security (BSI) has asked all manufacturers to enable users to do this, though. But the market is very confusing. It is therefore advisable to pay attention to brand names and to prefer products from manufacturers that provide safety information about the devices as well as regular updates on their websites.

However, these updates must also be installed, only a few devices do it automatically. Once a vulnerability of a device becomes known, professional manufacturers ideally try to provide their customers with an update as quickly as possible. As long as the update is not installed, the device remains vulnerable: The public security flaw can then be exploited by any attacker. The BSI also recommends disabling the UPnP function of the router. UPnP stands for ‘Universal Plug and Play’ and is a standard setting allowing devices to communicate with another within a network. UPnP makes life easier for users, but unfortunately also for attackers. Through the router – the device via which all the other devices at home get access to the Internet – the UPnP can be switched off.

A more complex but relatively secure solution is to pool your devices in one
VPN. The abbreviation VPN stands for Virtual Private Network, thus for a private network that extends to the public Internet. With the help of a VPN it is still possible to remotely control your smart home or webcam at home. But only with a device, for example a mobile phone, which is logged in the same VPN as the smart home. In addition, both devices must be connected to the VPN. As soon as this connection is established the devices connected to it are invisible for the other users on the Internet and thus protected. A prerequisite is, however, that the VPN is neatly set up. Since this is not always easy, you should get help from an expert, if necessary.

Wrecked in the web

An officer of the Federal Navy secures secret data and documents on an unprotected hard drive – everyone can access them

The hard disk manufacturer Western Digital is promoting his external disk ‘MyCloud’ as follows: ‘Access and share your favorite photos and videos from any place with an internet connection via your computer, tablet or smartphone.’ The device is a mass product that allows people to back up their data and enjoy being able to access it easily on the go.

One of Western Digital's customers works in the German Ministry of Defense. The captain mounted the disk in his apartment. He saves his complete life on it, the private as well as the official one. The hard drive serves as backup to his computer. There are bank statements, contacts, photos, detailed information about family members, account information, email passwords, a CV together with a picture of his child. Among the official documents are scanned troop badges, transfer notifications, fleet lists, the names of several German soldiers, detailed information about crews of German naval boats, telephone numbers, bills, certificates of service, a document for the secretaries of state and a detailed, scanned calendar that informs about appointments in the Ministry of Defense.

None of this should be public. All of it is publicly available.

The SZ calls the officer and informs him about the data gap. He says he is aware that the hard drive can also be reached from the outside – 'but only with a password'. As soon as he realizes that this is not the case, he unplugs the hard drive while still on the phone. The captain doesn't want to share details about the configuration of his device but obviously the man has made a mistake. Western Digital notifies on request that it's impossible to analyze the problem without further details.

The hard drive of the officer would have been a direct hit for terrorists and intelligence agencies, for criminals stealing identities, plundering accounts or seeking to spy on family members of the man. As part of the investigation hundreds of such hard drives were discovered, including small ones for private use such as the officer's but also entire servers. On many of them sensitive data is stored: business secrets, passwords, photos of affairs – there is nothing that is not saved.

Disposal facility without rinser

Almost all industrial plants are connected to the Internet today – many of them flawed. Their technique is openly available to the public.

He is a foreman in the field of wastewater supply, wearing his blue overall. The man sits in front of the screen and opens his eyes widely: 'That's impossible.' Next to him, his boss looks just as incredulously on the laptop. It shows a computer program with which one can remotely control a wastewater treatment plant. The men know the surface all too well: It's their job to look after this specific industrial plant. But the laptop, on which the control system of the wastewater treatment plant can be seen now in real time, belongs to journalists, who are paying these men a visit. The computer is not registered in their employer's network either, an association of water and wastewater utilities in Thuringia – the laptop is just connected to the Internet. Still, everyone can read the water level of the sewage treatment plant as well as the fault messages. 'That's bad', says the boss who is responsible for 24 sewage treatment plants. Two years ago, the disposal facilities were upgraded; now the technicians can remotely check if the machine is properly running, that simplifies their work enormously.

To be clear: the sewage treatment plant can't be controlled via the Internet, neither by an employee or an intruder from the outside. Only the status of the facility can be read online. However, the manufacturer of the used technology explains on request that he cannot rule out that some of his plants 'can also be externally controlled'. Again another company is responsible for the data link of the plant: It is unclear who is responsible for the error.

During their research SZ reporters will not only find sewage systems but also heating and ventilation systems, pumps, air conditioning systems of entire furniture stores and a fully automated community center openly accessible on the net.

Not every discovered system can be remotely controlled, many such as the wastewater treatment plant in Thuringia, merely indicate whether the system is working or whether a technician should have a look. What an attacker can do with the information depends on its intent. Clearly, security flaws also exist in more critical systems than sewage treatment plants. The manufacturer applies a similar technology like the one used in Thuringia in drinking water treatment plants.