SySS
THE PENTEST EXPERTS.

IT SECURITY KNOW-HOW

Alexander Straßheim, Sebastian Schreiber

IOT PENETRATION TEST

November 2017

Schaffhausenstraße 77, 72072 Tübingen, Germany

+49 (0)7071 - 40 78 56-0

info@syss.de

www.syss.de

This article is based on: A. Straßheim, S. Schreiber, "IoT-Penetrationstest", DuD – Datenschutz und Datensicherheit, 10/2017, pp. 623–627.

Introduction

It will not be long before all our household electronic devices can actually be linked with one another over the internet. Bluetooth, Wi-Fi and mobile communications are already available in nearly every household. The Internet of Things is becoming more and more important, and is gradually becoming part of our everyday life. Our household appliances will be able to both exchange and process information. Our lives will therefore become easier, faster, more comfortable, connectable and smarter. Analysts assume that more than 30 billion devices will be connected to the internet by 2020.

Developers of Internet of Things (IoT) devices are faced with a decision: Should they extend existing devices with older micro controllers and thus make an internet connection and Cloud-based applications possible, but accept possible security risks in doing so? Or should they use newly developed micro controllers that have been designed especially for IoT devices? This is because different requirements are placed on IoT devices. These requirements include low power consumption, high computing performance, different interfaces and also – with increasing importance – security.

Many IoT devices are powered by batteries. Great emphasis is placed here on a long operating time between the charging processes although low power consumption is also a desirable goal for the devices running off the mains. This enables the development engineers to keep the size of the overall device and the utilized components – cooling elements for example – small. Numerous sensors and input units, e.g. touch recognition and graphic displays, require enormous processing power. In addition to USB and Ethernet, many of the new IoT devices use radio connections. They mainly include Bluetooth Low Energy (BLW) and Wi-Fi. And last but not least, IoT devices will also maintain the personal privacy of the user while also providing protection against digital attacks, unauthorized access and data changes. Generally speaking, the security requirements relating to IoT devices are higher than those for devices not connected to the internet. Recently, it has been possible to read an increasing number of reports in which IoT devices have been misused for digital attacks. In 2016, for instance, hackers misused thousands of IoT devices for Distributed Denial-of-Service (DDoS) attacks and paralyzed large areas of the internet. Companies such as Amazon, Netflix, Spotify and Twitter, to name but a few of the large enterprises, were affected by these attacks [1]. For manufacturers and service providers, these kinds of attacks and outages not only mean an image loss, but also have immense commercial losses. IT security researchers presume that similar Distributed Denial-of-Service (DDoS) attacks using IoT devices will increase in future [2].

What is the Internet of Things?

Communication between electronic devices is now well-established albeit often in a simple form. When we, for example, order something over the internet, we can track our parcel using our smartphone and know where the shipment is at any particular time. If our printing cartridge is running low, the printer can automatically trigger the order for a replacement. Some human interaction is still required in the described cases. Thanks to the Internet of Things, this human effort will no longer be necessary. The IoT is not just being talked about, it has now become part of our everyday life. When looking specifically for a definition of the term, it can quickly be seen that there is more than one definition for the IoT [3]. Different institutions regard this term in different ways and one quickly stumbles from one keyword to the next. Terms such as IoT, Industry 4.0, M2M – the interlinking of machines and systems is referred to in many ways and in reality all mean the same: IoT means communication between smart devices without any human intervention. It must be assumed here that IoT

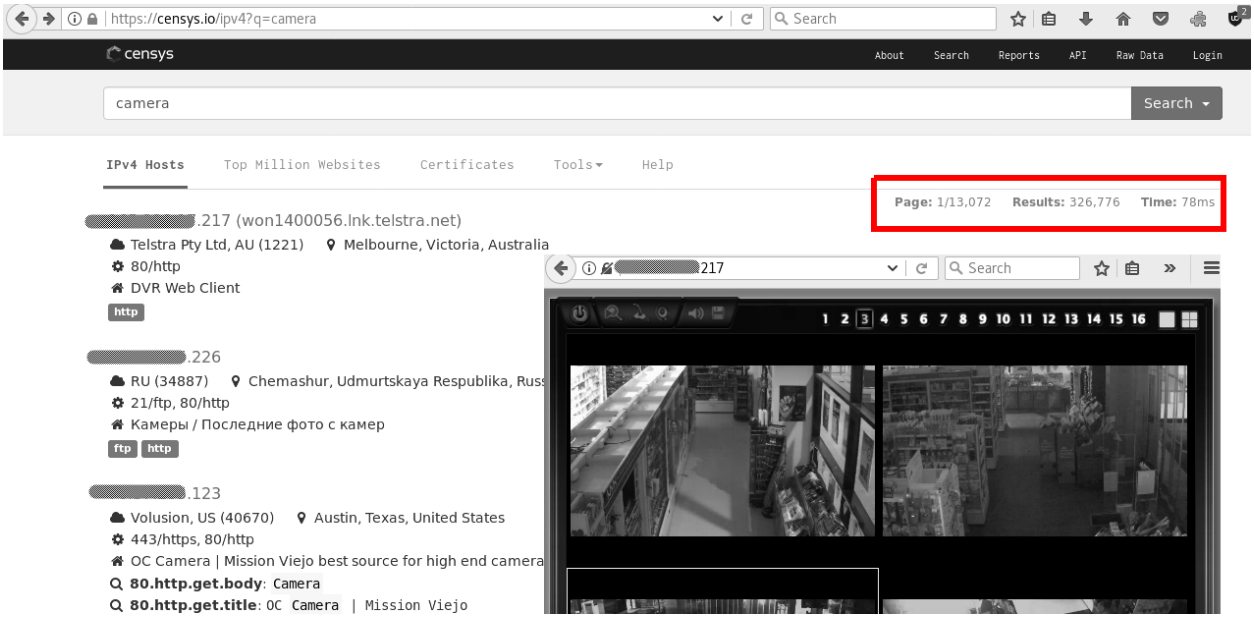

Figure 1: Censys: IoT search engine with potential hazards

devices often have an IP address and can be reached as a separate unit in the local network and over the internet as well. The Internet of Things is not just a technology, it also combines a whole range of different technologies. These devices are therefore able to acquire, evaluate and exchange data, and also use the data for further activities. This abundance of possibilities will accompany us in daily life and reduce our workload. However, this also means that there is a whole range of new digital attack scenarios associated with such refined technological developments.

Misjudged risks of the IoT

This article also deals with IoT devices in the literal sense, i.e. with “intelligent” devices that are connected to the internet and can also potentially be targeted “from the outside”, that is to say not just from within a closed company network. Although this produces new value-added networks, new digital risks are also created. Possible dangers arise at four different levels [4]. The first level is the hardware level. This relates to the IoT device interacting with its environment. The interaction usually takes place through sensors. It is therefore possible to manipulate certain kinds of signals in such a way that sensors are disturbed and malfunctions result [5]. It cannot be ruled out that attackers may be able to extract sensitive data from the device when accessing the hardware. Dangers at the second level, the network level, relate to the exchange of information between the components. The attackers may induce the utilized software to trigger undesirable activities. The dangers at the third level concern the back end or Cloud solution where the various services are to be found. In addition to the requirements, data can therefore also be stored which are needed for the IoT products to function. These products may contain vulnerabilities, e.g. on account of the use of outdated software through which the IoT device could be misused for malicious activities. The application level is the fourth level and relates to the vulnerabilities in the operation of a web-based application or a mobile device.

Hidden and apparent dangers

Owners of an IoT device can quickly become the victims of malware. This was recently the case when IP cameras were affected by a vulnerability in which the infection lasted less than two minutes [6]. Since the majority of devices susceptible to the malware "Mirai" used in this case did not have a non-volatile memory, the devices could be freed from the malware after interrupting the power supply. This is not a permanent solution, however, since these devices will be infected again within a short space of time. In principle, it makes sense to generally change the preset passwords of the devices.

In November 2016 customers of Deutsche Telekom were the victims of a botnet attack and in the course of which would have almost been part of an even larger botnet. An attempt was made to attack the router over port 7547 and to link this with the Mirai botnet. Maintenance servers were able to contact the router via this remote maintenance port and notify the server that a software update is available. An attempt was made in this way to bring additional malware into the device. Fortunately though, the attack did not function perfectly with the result that the around 900,000 attacked routers of Telekom could not be misused for an even larger botnet, but only that some routers simply failed [7]. Nevertheless, Deutsche Telekom suffered enormous financial losses for which the responsible 29-year-old British hacker received a suspended prison sentence of one year and eight months from Cologne District Court at the end of July 2017. This attack highlights the fact that many attacks are not apparent to the individual user.

Many IoT systems can be found using the search engines Shodan and Censys. Even private cameras, weather stations and installations of public utility companies can be controlled.

Figure 1 shows the search engine Censys with a search request for IP cameras. Inadequately protected cameras can provide a detailed insight into the private sphere. However, not only can IP cameras be explored, but also critical equipment control systems. This represents an immense security risk. If these systems get into the wrong hands, the consequences can be serious. With regard to IT security in particular, operators of critical infrastructures must be aware of the risks associated with interlinking devices.

The Wikileaks press release entitled "Vault 7: CIA Hacking Tools Revealed" describes the nightmare of security experts: In this way networked automobiles will be used as a potential murder weapon [8]. The following sentence in particular stood out in the leaked documents of the CIA: "In October 2014 the CIA also wanted to infect a vehicle control system used in modern automobiles and trucks". The purpose of this control was not specified, but it would allow the CIA to carry out assassinations that could almost not be perceived as such [9]. In the document quoted by Wikileaks as the source, there are also considerations by the CIA regarding attack targets with IoT devices. However, the documents do not show whether the secret service has in fact already managed to manipulate a networked vehicle and infiltrate the control system. The fact that this is possible was demonstrated by the security experts Charlie Miller and Chris Valasek when they hacked the Cherokee Jeep from Chrysler in 2015. The attacks on the entertainment system in the vehicle are also interesting. It was possible, for example, to monitor the vehicle location without having to attach a separate transmitter for this purpose. Even the microphones in the vehicle could be tapped to follow the conversations between the passengers. At present, automobile owners can hardly protect themselves against attacks or improve the IT security of their automobiles. However, it is recommended that diagnostics systems running over ODBII be unplugged if possible because the connector plugs operated over ODBII constitute a gateway for attacks against the vehicle.

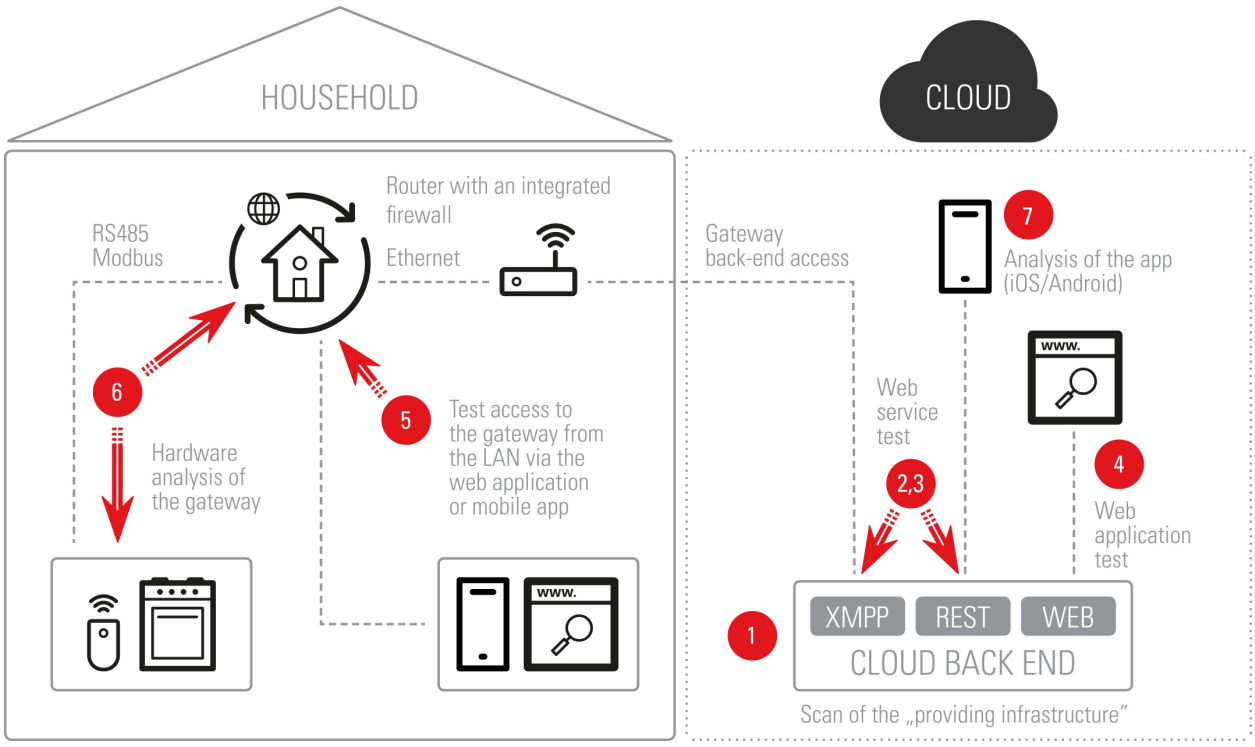

Figure 2: Components of the Internet of Things

However, the attackers do not always need highly complex knowledge of the possible attack vectors. For example, a Smart Lock user was quite astonished when a neighbor suddenly entered the apartment without needing a key. With Smart Lock the house door can be controlled, for example, using a smartphone app. If the smartphone (or tablet) is now in the house and a language assistant is also active, a tilted window is all that is needed to open the door. The neighbor was therefore able to unlock the front door by calling out "Hey Siri, unlock the front door". [10] Only the instruction is required here, the language assistant is not able to differentiate between persons on the basis of their voice.

Test plan and simulated attacks

Smart Home manufacturers are aiming for easy handling of the devices, even without any IT knowledge and at the press of a button. It will also be possible to control the IoT devices from anywhere. This often means that security suffers. The operating instructions do not point out that the settings needed for the devices will open up gaps in the firewall which is supposed to protect us against attackers from the internet, or that sensitive data can be transmitted unencrypted over the internet.

Figure 2 shows the typical setup of IoT hardware. The numbered arrows shown designate the tests that are also anchored in the project plan of a penetration test (cf. Figure 3).

The exact choice of tests and tools is made to match the IoT device and its requirements because a penetration tester will make the most of his test time to acquire as many findings as possible. It is also important to accurately document the findings and test results obtained for the customer, and be able to make recommendations for the rectification of vulnerabilities so that the customer can raise the level of IT security in a sustained

manner. Market launch can begin once the security of the device has been taken to a level which is sufficient based on the examples given above or other comparable specifications.

Various services normally run at the back end (1). Depending on the configuration, these services can show vulnerabilities or be based on outdated software. If vulnerabilities are present, there is also a risk of a possible privilege escalation of the attacker that leads to compromising of the system. As a result, this IoT device can be misused for malicious activities.

The interaction between IoT devices usually takes place in different directions. Thus, the devices are often used via web applications or mobile apps for smartphones and tablets.

The underlying web service and the data traffic to the back end (2,3), but also the application (4, 5, 7) itself may therefore be vulnerable and show up vulnerabilities. Principally, there is a danger that an attacker can make the software execute undesirable activities through corresponding manipulation of the data traffic. If the IoT device is unable to check the legitimacy of a query, the IoT device is under the control of the attacker as a result.

Also, neither production nor any possible implementation faults in the hardware (6) should be ignored. The worst case scenario for the manufacturer involves attacks in which the attackers acquire unauthorized access rights for the device and assign the device their own code for execution purposes. Even the sensors installed in the device can be attacked and manipulated. The consequences are incorrect measurements and function faults. Thus, not only can signals between the sensor and gateway be attacked, but also between the gateway and the back end. This would mean that the IoT device performs undesirable activities.

Measures & conception

Attacks such as those in 2016 where an enormous number of vulnerable IoT devices were misused for the DDoS attacks highlight the need for action when IoT security solutions are involved. The manufacturers are often not aware that, besides the functionality of the devices, security is also extremely important. An analysis of different devices shows that in some cases products only contain limited security mechanisms or have no security mechanisms at all. Attackers normally need just a single gap to compromise a vulnerable system [11]. It is vitally important that manufacturers develop acute awareness of security issues. Only when this prerequisite has been created can concrete measures be implemented as the next step.

IT security should be an established part of the planning and development phase. Appropriate architectures and suitable security-related design decisions must be included at a very early stage of the development process in order to minimize possible follow-up costs.

Areas of attack can be minimized, for example, by deciding before the development process which components will be needed for the actual operation of the device. Cost pressure during development and production is a crucial factor. If a manufacturer offers several equipment variants, it is highly unlikely that a separate circuit board will be developed and populated for each variant. All expansion modules involve additional costs. For example, plug connections are very expensive, not to mention the associated expenditure involved in manufacturing, assembly and maintenance [12]. The manufacturer's main objective is usually to produce large numbers of standardized components in order to save costs. The equipment variants often differ in the firmware which leaves some of the functions unused in the lower cost variants.

Sub-project	Module	Time needed (in man-days)
Kick-off workshop (by phone)	KICKOFF	
1) Analysis of Cloud systems (infrastructure test) Everyone involved in the solution and server systems reachable over the internet are subjected to a security analysis. To this end the penetration tester uses both different security scanners (e.g. Nessus, MaxPatrol, Saint) as well as vulnerability scanners / exploit collections (e.g. Metasploit Framework). In addition for the security tests, software tools developed in-house are used in the appropriate context, for example Active Directory Scanner, ShCoLo, FirePeek/FirePoke, Windows File System Scanner, Windows Registry Scanner and Wolpertinger. Manual and semi-manual tests are also part of this test.	INTERNET	0.5
2) and 3) Testing the web service for a) app and b) gateway The focal point of these tests is a security analysis of the customer's web service communicating over XMPP as shown in the documents provided. The main test objects are: 1) Vulnerabilities in the transportation security and man-in-the-middle manipulation of legitimate queries, in particular testing for susceptibility to a downgrade attack. 2) Input filtering (e.g. to SQL or XPath injection) 3) Authorization (privilege escalation, access to external data,...) 4) XML parser (external entities, XML bomb, ...) Two methods are used: **1) Direct analysis of the API** The customer provides an interface definition. Vulnerabilities are identified by direct accesses to the web service. A separate client is written to this end as appropriate. **2) Traffic interception** Communication between the client and the web service is established by using an attack proxy and manipulation is therefore made possible.	WEBSERVICE	1.5
4) Analysis of the web application: On the one hand, the existence of web vulnerabilities (e.g. the OWASP Top 10) is tested from the perspective of an unannounced attacker as well as from an announced user. On the other hand, evidence of safe encrypted data transmission is provided. In this case use is made of browser extensions, special attack proxies and manual test methods. The efforts required are shown in our calculation basis for web application testing (see next section). **Evaluation of the application:** Protection needed: High (exposed on the internet) Complexity: Low – medium (few functionalities, no rights and roll concept)	WEBAPP	2
5) Analysis of the web application at the gateway: On the one hand, the existence of web vulnerabilities (e.g. the OWASP Top 10) is tested from the perspective of an unannounced attacker as well as from an announced user. On the other hand, evidence of safe encrypted data transmission is provided. In this case use is made of browser extensions, special attack proxies and manual test methods. The efforts required are shown in our calculation basis for web application testing. **Evaluation of the application:** Protection needed: Medium Complexity: Low	WEBAPP/ WEBSERVICE	2

Sub-project	Module	Time needed (in man-days)
6) Hardware analysis of the gateway: The penetration tester will analyze the utilized product hardware. In addition to others, the following aspects are examined: – Hardware inventory (identification of utilized components and the available interfaces, e.g. JTAG, serial Console/UART) – Hardware debugging via the identified interfaces (e.g. memory dumps) – Identification and analysis of the operating system, the utilized applications, service configurations and the file system – Analysis of extraction possibilities for the utilized memory components used (e.g. Flash/SPI) Possible tools for this test phase are Bus Pirate, JTAGulator, Minicom / Screen, flashrom or Logic Analyzer. – Search for deposited credentials	PRODUCT	2
Documentation including executive summary, assessment of the vulnerabilities; two-stage quality assurance	DOCU	2.5
Total number of man-days:		10.5

Figure 3: Test modules

The basic functional components should be examined in regard to their security during the concept phase of an IoT device. In particular, communication between the involved interfaces and their protection is a neuralgic point. For example, attention should be paid here to the fact that signals and queries could be manipulated or that they might originate from a source other than the device.

It should be ensured wherever possible that unauthorized data are rejected.

Market launch

It is important that the product is subjected to security testing by an independent service provider before it is launched on the market. The objective of security testing is to detect possible vulnerabilities and show how they can be rectified. Leading security organizations have specified how a security test and the documentation are to be designed. If a security test has not been performed prior to market launch, it should definitely be carried out afterwards. Even if the latest security precautions were taken during the development phase, there is ultimately no absolute guarantee that the end product will be free of security problems. New security gaps are always being discovered and published. If the manufacturer wants to gain the trust of customers, it is important to deal with detected vulnerabilities in an open manner. If known gaps are closed and security updates are made available, it is less likely that attackers can misuse a known vulnerability and be successful.

For example, Somfy, a company which develops and markets drive and control technology for roller shutters, sun protection systems and garage and yard doors, also underwent a security test. The product TaHoma® Connect was tested. In this way it was possible to identify several vulnerabilities before launching the product on the market. These vulnerabilities were then rectified before the actual product launch took place. After the IoT security test for TaHoma® Connect, Somfy was issued with a certificate attesting to a high degree of data security.

Summary

There is still insufficient awareness of the potential dangers for Internet of Things devices. Manufacturers do not disclose all the risks which the customer is taking when using IoT devices. Neither the operating instructions nor the packaging normally mention any hidden functions, services and possibly available sensors. As far as the customer is concerned, an IoT device is a black box whose exact functions and security are a mystery to him or her. In principal, IoT devices should be isolated in a separate network because they constitute a danger for the local network where private documents, videos and images are located and this danger cannot be estimated.

Arne Schönbohm, Head of the Federal Office for Security in Information Technology, suggests introducing a Best Before date for IT. Manufacturers of software and hardware will therefore guarantee their perfect condition and will be liable in the event of defects. Manufacturers would thus be obligated to ensure the security of supplied products for a certain length of time. It will be made clear to the customers in this way that the product being used has an expiry date and that, after this date, ensuring security is the responsibility of the customer [13]. This raises the question of how to install security updates and who will be responsible in this case. Should the household, i.e. the user of such an IoT device, personally install the security update? Should the manufacturer or the salesperson perform this task?

Whereas this proposal might be desirable, it will be very difficult to implement in practice because the market is global and not transparent.

The importance of IoT security has increased following the IoT bot net Mirai and the Chrysler hack. Manufacturers of renowned products now assign higher priority to the security of their devices because not only does a successful attack have an immense economic impact, but also damage caused to the company's image is also considerable.

References

[1] B. Chacos, "Major DDoS attack on dyn DNS knocks spotify, twitter, github, PayPal, and more offline. PCWorld", 21-Oct-2016. [Online]. `http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-online.html`. [Accessed: 11-Jul-2017]. (Cited on Page 1)

[2] M. Orcutt, "Lebensgefährliches Internet der Dinge? Technology Review", 7-Dec-2017. [Online]. `https://www.heise.de/tr/artikel/Lebensgefaehrliches-Internet-der-Dinge-3562468.html`. [Accessed: 11-Jul-2017]. (Cited on Page 1)

[3] F. Lindner, "IoT Definitionen: Was ist eigentlich das Internet der Dinge?" [Online]. https://www.expertenderit.de/blog/iot-definitionen-was-ist-eigentlich-das-internet-der-dinge. [Accessed: 11-Jul-2017]. (Cited on Page 1)

[4] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review", in 2012 international conference on computer science and electronics engineering, 2012, vol. 3, pp. 648–651. [Auch online]. https://www.researchgate.net/publication/254029342_Security_in_the_Internet_of_Things_A_Review. [Accessed: 11-Jul-2017]. (Cited on Page 2)

[5] Y. Son et al., "Rocking drones with intentional sound noise on gyroscopic sensors", in: Proceedings of the 24th USENIX conference on security symposium, 2015, pp. 881–896. [Auch online]. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-son.pdf. [Accessed: 11-Jul-2017] (Cited on Page 2)

[6] H. Gierow, "Mirai-IoT-Botnet: IP-Kamera nach 98 Sekunden mit Malware infiziert", golem.de, 21-Nov-2016. [Online]. https://www.golem.de/news/mirai-iot-botnet-ip-kamera-nach-98-sekunden-mit-malware-in-fiziert-1611-124602.html. [Accessed: 11-Jul-2017] (Cited on Page 3)

[7] "Telekommunikation: BSI: Bei Angriff auf Telekom 'noch einmal Glück gehabt'", Die Welt, 29-Nov-2016. [Online]. https://www.welt.de/newsticker/dpa_nt/afxline/topthemen/article159833020/Bei-Angriff-auf-Telekom-noch-einmal-Glueck-gehabt.html [Accessed: 11-Jul-2017]. (Cited on Page 3)

[8] F. Greis, "Vault 7: CIA hacking tools revealed" [Online]. https://www.wikileaks.org/ciav7p1/. [Accessed: 11-Jul-2017]. (Cited on Page 3)

[9] "Vault 7: Was macht die CIA mit gehackten Autos?", golem.de, 9-Mar-2017. [Online]. https://www.golem.de/news/vault-7-was-macht-die-cia-mit-gehackten-autos-1703-126639.html. [Accessed: 11-Jul-2017]. (Cited on Page 3)

[10] C. Wisniewski, "Siri opens 'smart' lock to let neighbor walk into a locked house", 22-Sep-2016. [Online]. https://nakedsecurity.sophos.com/2016/09/22/siri-opens-smart-lock-to-let-neighbor-walk-into-a-locked-house/. [Accessed: 11-Jul-2017]. (Cited on Page 4)

[11] S. Schreiber, "Der Penetrationstest als Instrument der Internen Revision", in A. Sowa, P. Duscha, and S. Schreiber, IT-Revision, IT-Audit und IT-Compliance. Wiesbaden: Springer Fachmedien Wiesbaden, 2015, S. 151–183. (Cited on Page 5)

[12] M. Dölle, J. v. Malottki, "Digitaler D-Day – Installationswege und versteckte Funktionen gefährden Privatsphäre und Sicherheit", c't, 31-Mar-2017. [Online]. https://www.heise.de/ct/ausgabe/2017-8-Installationswege-und-versteckte-Funktionen-gefaehrden-Privatsphaere-und-Sicherheit-3665522.html. [Accessed: 11-Jul-2017]. (Cited on Page 5)

[13] "BSI-Chef: IT-Mindesthaltbarkeitsdatum würde wichtige Signale setzen", 21-May-2017. [Online]. http://winfuture.de/news,97748.html. (Cited on Page 8)

THE PENTEST EXPERTS

SySS GmbH 72072 Tübingen Germany +49 (0)7071 - 40 78 56-0 info@syss.de

WWW.SYSS.DE