#02 FEBRUARY 2018

PUBLISHED BY Secura

SecurAware

INSIGHT
New OWASP Top 10

ADVICE
GDPR: Are you ready?

EVENT
BHS 2018

HACK
The state of Dutch SSL/TLS certificates

Reference Johannes Denissen, DAF Trucks
Trucks have become computers on wheels

REMCO HUISMAN, COMMERCIAL DIRECTOR

Take control of your digital security (before someone else does)

2017 was a productive year, in which we built a solid foundation for the continued growth of our company. We opened an office in Amsterdam, achieved certifications for both ISO27001 and 9001, changed our structure and incorporated our subsidiary ITSX. The latter was the rationale behind our major change last year: the rebranding into Secura. With the rebranding we want to emphasize our new position in the market: from a pentesting company to a full service organisation that can help you take control of your digital security, before someone else does.

'Take control of your digital security (before someone else does)!' is the new theme for the Black Hat Sessions (BHS) which will be held on the 14th of June at National Business Center (NBC), Nieuwegein Utrecht. BHS is our annual security conference where you will be informed on Digital Security: The latest trends, threats and the crucial solutions. Informative for decision makers, managers, CISOs and technical security experts.

The sixteenth edition of BHS will see an improved programme, a new venue (in Nieuwegein), more space and best of all, the Secura Grand Slam: a Capture-the-Flag (CTF) competition aimed at student teams from University or Higher Education.

Everybody knows the OWASP Top 10, but what many people do not know, is that it changes over time. All things considered, it would have been weird if the OWASP Top 10 had not changed. The world changes, IT technology changes, new vulnerabilities are found or introduced and last but not least, attack(er)s change. Regardless of how much has changed in the last 4 years, injection vulnerabilities like SQL injection are still firmly ranked at the number one position. A lot of companies ask us to perform 'penetration tests' against the OWASP Top 10. Rest assured, that we do not limit ourselves to the Top 10, as there are many more problems to be found. Cross Site Request Forgery (CSRF) for example, dropped out of the Top 10, so should companies stop testing for CSRF? We do not think so. I am sure that our contestants in the CTF at the Black Hats Sessions will target their attacks using one or more issues from the OWASP Top 10. It should be no surprise that we will hide a few of these vulnerabilities in our CTF.

I hope that you are not yet completely bored of GDPR, which I can imagine is hanging over everybody's head like the proverbial 'Sword of Damocles' as the deadline of May rapidly approaches. We recommend that you continue to work hard, with the aim of being compliant by May. However, should you require assistance, no worries, you know who to turn to ;-)

The fact that we have opened an office in Amsterdam has not come at detriment to our customers in Eindhoven. In this SecurAware we are proud to present Johan Denissen, Head of Information Security & Incident Response at DAF Trucks, who has the challenging task of keeping both the company and the connected trucks safe from digital security threats.

I will finish this column with the striking IT security news that hit the world earlier year: Meltdown and Spectre. Our technical director: Ralph Moonen, will give some background information regarding these two quite fundamental vulnerabilities. It makes you wonder what is next…. a security issue with SSL/TLS certificates perhaps?

So, take control of your digital security, before someone else does.

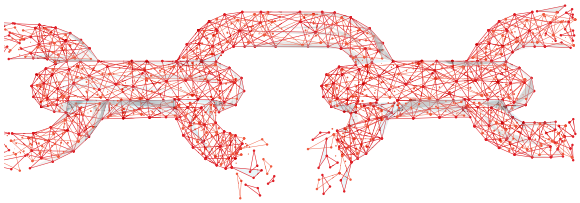
Have a safe year!

Remco Huisman
Commercial Director

Opening Amsterdam office

Our company is in a transition. This resulted in a new name and a complete portfolio to reflect our position as well as a clear vision on how to control all aspects of digital security. The open house party of 30 November last year was an excellent moment to inform and to connect in an informal setting. We proudly presented our story and ambitions but also gave some interactive demos on hacking with a drone, XSS but also the much discussed GDPR. This combined with bubbles and bites was a perfect way to catch-up and celebrate.

Thank you for helping us to celebrate this milestone.

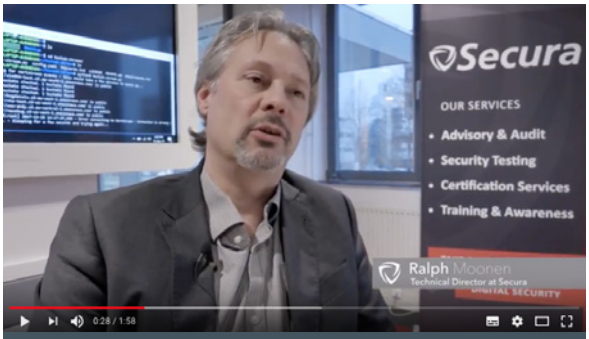


Secura Grand Slam
Student CTF

Organising a Capture The Flag (CTF) fulfills a long-cherished wish of Secura. The first episode of the Secura's CTF will be held at the Black Hat Sessions on June 14th 2018 at NBC Nieuwegein Utrecht. The registration is open only for students in the last 2 years of their study at a University or Higher Education. For more info: www.secura.com/ctf

Infosecurity Europe
05-07 June 2018, Olympia London
Secura booth X149
www.infosecurityeurope.com
Infosecurity Europe (Infosec) is the region's number one information security event featuring Europe's largest and most comprehensive conference programme and over 400 exhibitors showcasing the most relevant information security solutions and products to over 19,500 information security professionals. Join us at the Secura booth X149 (New Exhibitor Zone) on 5-7 June 2018 at Olympia London.

Black Hat Sessions 2018
14 June 2018, NBC Nieuwegein NL
www.blackhatsessions.com
The Black Hat Sessions is Secura's annual security conference. It's a lively event in which you get informed about the latest trends, threats and solutions in the world of Digital Security. The informal atmosphere, the interaction with speakers and delegates and the diverse schedule have been appreciated for years by both IT Pros and management. Read more about BHS 2018 on page 14 of this SecurAware.



People behind Secura

Who are the passionate people behind Secura dedicated to fulfilling our mission of helping you take control of your digital security? And what makes Secura stand out from other companies in the sector? We proudly present 'Working at Secura – the movie'. Take a look at https://www.secura.com/workingatsecura for the 2-minute video and our story.

COLOFON

Contributing editors
Ben Brücker
Ester van Dael
Daniël Dragičević
Remco Huisman
Matthijs Koot
Ralph Moonen
Maayke van Remmen

Art director
Hannie van den Bergh / Studio-HB

Contact
editorial@secura.com

Secura B.V.
Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T + 31 (0)40 23 77 990
E sales@secura.com
W www.secura.com

Follow us on

Tom Tervoort, Security Analyst

THE TEN MOST CRITICAL WEB APPLICATION SECURITY RISKS

New OWASP

Since the previous version of the OWASP Top 10, which dates back to 2013, a lot has changed in the area of web applications. What do these developments mean for security? Do the same problems still exist or do we now have to deal with entirely new risks?

Over the past few years a couple of large trends have emerged with respect to web development. An example of this is that the majority of the application's logic has shifted from the back-end to the front-end. This trend manifests itself in the fact that more and more so-called single-page applications are being developed based on JavaScript frameworks. Previously, the web server would generate pages and serve them to the user, nowadays the server frequently offers an API which allows the front-end (from the browser or even from a mobile application) to communicate with the server and create the web page using this technique instead. On the other hand scalability has received more focus. The same is true for the new options that are offered to users by browsers, as well as improvement of the user experience on various devices. Do these types of changes influence the type of vulnerabilities found in web applications a lot?

A1:2017 - Injection

The most well known example is named SQL injection, with which an attacker is able to execute specific queries and by doing so is able to read or modify data that is present in the underlying database. Even though SQL injection has been a widespread and large problem for over 20 years, this risk still occurs, albeit at a less frequent rate during our investigations. Nowadays developers are well aware of the impact that this infamous risk causes and web frameworks are designed to prevent this risk by default.

On the contrary this does not hold for other types of injection vulnerabilities: An interesting example of this is NoSQL injection, which executes a similar attack against query languages of alternative, non-relational databases.

A2: 2017 – Broken Authentication

In general, it is a difficult task to prevent an attacker from hijacking user's accounts. New trends have emerged in this area as well, such as stateless session management, single sign-on and authentication methods that are a good fit for mobile applications. These trends also pose new risks; risks that developers may be less familiar with.

A3:2017 - Sensitive Data Exposure

The third risk is sensitive data exposure caused by, for example, the lack of encryption or (strong) user authentication. Nowadays, sensitive data is frequently disclosed by accident. On the upside, the use of encryption during transport by means of HTTPS has increased drastically.

A4:2017 – XML External Entities (XXE) [NEW]

The fourth risk on the list is a notable newcomer. This is an old issue that allows an attacker to read arbitrary files on the server, as well as on the network behind the firewall. This issue is caused by a feature that is offered in (old) software that reads XML messages.

OWASP Top 10 -2013		OWASP Top 10 -2017	
A1	Injection	A1:2017	Injection
A2	Broken Authentication and Session Management	A2:2017	Broken Authentication
A3	Cross-Site Scripting (XSS)	A3:2017	Sensitive Data Exposure [2013:A6]
A4	Insecure Direct Object References	A4:2017	XML External Entities (XXE) [NEW]
A5	Security Misconfiguration	A5:2017	Broken Access Control [2013:A4+A7]
A6	Sensitive Data Exposure	A6:2017	Security Misconfiguration [2013:A5]
A7	Missing Function Level Access Control	A7:2017	Cross-Site Scripting (XSS) [2013:A3]
A8	Cross-Site Request Forgery (CSRF)	A8:2017	Insecure Deserialization [NEW, Community]
A9	Using Components with Known Vulnerabilities	A9:2017	Using Components with Known Vulnerabilities
A10	Unvalidated Redirects and Forwards	A10:2017	Insufficient Logging&Monitoring [NEW, Community]

The risk has made it into the Top 10 because static source code analysis shows that it is very prevalent in practice. Hopefully its listing in the OWASP Top 10 will lead to more widespread knowledge about this obscure but dangerous vulnerability.

A5:2017 – Broken Access Control

Risk number five is a classic issue that is still very widespread, even in modern web technologies that often employ sophisticated means of authentication. The absence of authorisation checks typically classes as a vulnerability that is difficult to test for with automatic testing software.

A6:2017 – Security Misconfiguration

Frequently software is configured in a default manner so that it is easy to deploy and use. This however does not guarantee that the configuration is also secure. Ensure that important security features are enabled, you do not make use of default passwords and have disabled debugging functionality within production environments.

A7:2017 – Cross-Site Scripting (XSS)

The seventh risk is cross-site scripting: the hijacking of another user's browser session by injecting scripts in a web page. This risk has seen a big decline since 2013: it dropped four places from number three in 2013 to number seven last year. This vulnerability can be disastrous nonetheless, however it is much more difficult to exploit nowadays due to the mitigations employed by web frameworks. These types of security measures are in practice however unfortunately often disabled when they get in the way of development. Furthermore, they do not offer exhaustive protection against all forms of cross-site scripting attacks.

> I do hope that we will one day learn to not include user input within instruction languages, causing injection vulnerabilities to be dethroned from the Top 10 of most critical web application security risks

A8: 2017 - Insecure Deserialization [NEW, Community]

Insecure deserialization is the possibility for an attacker to modify a transported programming language object, which allows the hijacking of the server.

A9: 2017 - Using Components with Known Vulnerabilities

Using components with known vulnerabilities is listed because it is relatively easy to use software that detects these vulnerabilities.

A10-2017 – Insufficient Logging & Monitoring [NEW, Community]

Insufficient logging and monitoring is also a newcomer in the Top 10 and relates to the fact that you assume that prevention by itself is sufficient. It is just as important that you are able to detect hacking attempts and respond to it in a just manner, as well as having a contingency plan in case things go south.

It would not come as a surprise if technology-specific issues such as external XML entities and insecure deserialization were to be gone in the next iteration of the Top 10. These types of risks are easily detected, mitigated and prevented. More fundamental issues such as broken authentication and using components with known vulnerabilities however are likely to be featured on the Top 10 for many years to come. The reason for this is that these are examples of risks that cannot simply be mitigated by implementing new or different technologies. They will pose a challenge for developers, just like they have been doing for the past ten to twenty years. I do hope that we will one day learn to not include user input within instruction languages, causing injection vulnerabilities to be dethroned from the Top 10 of most critical web application security risks.

OWASP offers a wealth of information that helps prevent such risks, but also to offer guidelines for testing existing applications through the OWASP Testing Guide (https://www.owasp.org/images/1/19/OTGv4.pdf).

Ralph Moonen, Technical Director & Tom Tervoort, Security Analyst

The state of Dutch SSL/TLS certificates

Transport Layer Security (TLS)[1], also known as Secure Sockets Layer (SSL), is the most important security mechanism in use on the internet currently. It is a technology that has evolved over the past few years and has known quite a few vulnerabilities.

Authentication of websites is performed using so-called X.509-certificates that contain public keys, which are used to prove that a communication partner knows a corresponding private key. If the public key is short or can be cracked, the private key can become known, after which an attacker can impersonate the site and place themselves in the middle between a victim and the website, decrypting communication. If the certificate is not valid, we cannot know with certainty the identity of the communication partner. It is therefore imperative that TLS certificates are valid and secure. Periodically, Secura investigates the state of the certificates used for TLS in use in the Netherlands. Specifically, we look at the most common cryptographic algorithm, RSA[2].

Gathering certificates

In order to investigate certificates, we performed a scan of most[3] IPv4 addresses that are routed into The Netherlands, according to RIPE. Using OpenSSL we extracted as many certificates as we could find. In total a little less than 500.000 certificates were downloaded and analysed for various aspects, such as issuer, expiration dates, algorithms supported, key lengths, and weak keys.

Some numbers!

The most used certificate issuers are:

1. `99194: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA`
2. `66075: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3`
3. `18047: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Organization Validation Secure Server CA`

> We have found that approximately half of the users of TLS do not use it properly

4. `16528: C=US, ST=Someprovince, L=Sometown, O=none, OU=none, CN=localhost/emailAddress=webmaster@localhost`
5. `16300: C=TW, ST=HsinChu, L=HuKou, O=DrayTek Corp., OU=DrayTek Support, CN=Vigor Router`

About half of all certificates given out by actual CA's, the rest is self-signed or issued by an unaccredited CA. This in itself means that *half of the certificates* cannot be trusted.

In order to be able to set an unforgeable signature, it is important to use a secure cryptographic hash function. We see the following distribution of hash functions:

- SHA-2-family: used by 77.7% of certificates
- SHA-1: 20.8%
- MD5: 1.5%

No attacks are known against any of the SHA-2 hash functions. However, SHA-1 is broken in theory and MD5 can be broken for the cost of about 50 cents of computing time per certificate.

Collisions

An RSA public key contains a term that consists of the product of two prime numbers. So its only factors are those two primes. Every number can be factorised into its prime factors. But generating a number **p*q** that is hard to factorise relies on generation of random numbers.

A common problem is that devices may generate their keys right after being booted for the first time, before the OS has been able to gather sufficient randomness. If two products **p*q** share a prime, you can even calculate their greatest common denominator (GCD) very easily using Euclid's algorithm: [https://en.wikipedia.org/wiki/Euclidean_algorithm].

Some years ago, the scientists behind [https://factorable.net/] showed that many public keys in certificates share the same primes, due to bad random number generators, and can be cracked. Cracked keys means an attacker can impersonate this web site, and decrypt intercepted traffic. We thought it would be interesting to revisit this research and apply it to the Dutch IP space. Therefore we extracted the public keys from all Dutch certificates, and ran fastGCD. After an hour or crunching numbers, our laptop spat out no less than 53 broken certificates.

A closer look at these certificates show something interesting: all 53 are device certificates, apparently devices with weak cryptographic random number generators. If they had cryptographic random number generators that functioned correctly, we would certainly not find any collisions at all in a small data set of ~500.000. However we found 53, which is statistically very close to impossible unless the devices suffer from grave weaknesses in their PRNG's.

Conclusion

If you use TLS, you must use good practices. We have found that approximately half of TLS users do not use it properly. A very small, but very significant percentage of public 1024-bit RSA keys can be cracked, showing that devices do not all have secure certificates. We do not know yet exactly which devices are affected and are contacting the vendors at this time.

We will publish an update and whitepaper when we have researched this issue a bit more and received response from vendors and affected Dutch organisations.

---

1. https://en.wikipedia.org/wiki/Transport_Layer_Security
2. https://en.wikipedia.org/wiki/RSA_(cryptosystem)
3. We excluded the large DSL and Fiber home ranges of KPN, Ziggo and others because they relate to private individuals.

I deal with a wide range of topics, from IT forensics to privacy, testing, e-discovery, monitoring and product security

Johannes Denissen, DAF Trucks

How would you describe in a few words DAF Trucks?

DAF Trucks is a leader in the design, manufacture and customer support of high-quality premium trucks. DAF is a wholly-owned subsidiary PACCAR Inc., an American Fortune 500 company. DAF manufactures its trucks in facilities in the Netherlands, Belgium, United Kingdom and Brazil. DAF products are sold and serviced by a network of over one thousand independent dealer locations throughout Europe, the Middle East, South America, Australia, New Zealand, and Asia. Under the name Paccar Financial, DAF also provides financial services for financing trucks and trailers, including repair and maintenance and insurance options.

You are Manager Information Security at DAF. What does this function mean?

I am the head of information security and incident response for DAF worldwide and for PACCAR Financial in Europe. This means I am accountable for establishing effective information security governance aligned with the organizational risk appetite. Also I am accountable for organizing an effective response in case of security incidents. This means that I deal with a lot of topics, IT Forensics, product security, e-discovery, monitoring, awareness, manufacturing networks, cloud, legislation like privacy, etcetera.

How is digital security set up within the organisation?

Today we operate using the think-build-run organizational model. Meaning there are three professional groups involved:

- **Information Security Management**
  They look at all the new company initiatives, and determine the cyber threats associated and consequently propose measures to combat these threats;
- **Solution Center**
  If technical measures are desired to combat new threats, this group figures out the nitty-gritty details of how to best do this and deliver the technical solution turnkey;
- **Security Operations**
  They manage the various security systems that our Solution Center delivers. Like firewalls, IDS's, IP's, DLP, malware protection tools, etcetera. They investigate the events of interest reported by our Security Operations Center (SOC). And also they are part of our core team to respond to security incidents.

How many people are concerned with digital security within the organisation?

I am not allowed to tell you how many people are concerned with digital security within our organization as this is considered confidential information. What I can tell you is that this year the team will grow with 4 FTE.

What do you feel proud of?

What I am most proud of is that we always gained executive support for information security and we did not need a breakpoint like an incident to get there. Information security is seen as a business enabler.

What are the main challenges in the field of digital security for DAF?

There are many security challenges ahead of us. The most important ones that come to my mind are:

- Properly securing our smart factories, because the increased connectivity of smart machinery in our production facilities will make them vulnerable to cyber-attacks;
- Adequately securing our connected trucks, as truck connectivity makes our trucks too vulnerable to cyber-attacks.

> DAF is member of ACEA Cyber Security Taskforce and the Auto ISAC

Could you tell us more about the initiatives of DAF with relation to connected vehicles (and autonomous driving)?

The idea is that all the DAF trucks will be connected. It helps our customers to manage their fleets better and also reduces the downtime of their trucks. And it must be done responsibly, or it becomes the "Internet of very dangerous things". Trucks have become computer networks on wheels, with all their problems that come with that, like the use of cryptographic protocols, software updates, cyber physical vulnerabilities, patching, cyber-attacks, etcetera.

DAF is developing 'platoon driving' as a project currently and participates in a UK truck platooning trial [http://www.daf.com/en/news-and-media/articles/global/2017/q3/30-08-2017-daf-trucks-participates-in-uk-truck-platooning-trial].

How is DAF dealing with security in this matter?

There are various working groups analyzing everything from the hardware to the communication protocols, performing penetration tests, risk analyses, privacy analyses and safety workgroups. We take it very seriously and we work with various partners, including Secura. But DAF does not isolate itself, we are also a member of ACEA Taskforce Cyber together with other automotive vendors. It is a trend in many sectors to establish Information Sharing and Analysis Centers (ISAC's) where private companies and the governments share (confidential) information on cyber security issues. Through our parent company PACCAR, DAF is also a member of the Auto ISAC [https://www.automotiveisac.com/].

> Trucks have become computers on wheels, with all their problems of patching, updates, cryptographic protocols, internet connections ed.

What measures will be taken to control the security risks?

Perhaps the best measure that we have in place to control the digital security risk is that IT risk management is a recurring agenda item for the risk council. The risk council exists of top-level executives who periodically talk about the biggest IT risks and their mitigation options.

Another important measure that we have taken is that we annually invite one of the best Red Teams (ex NSA hackers) in the world for a full week and ask them to gain unauthorized access to our systems while we watch them do it. With what we learn we from them we improve our monitoring and threat hunting.

And of course, we also learn a lot from many of the security tests that Secura is performing on many of our projects and platforms.

What do you think of the GDPR and why? What is the impact for your organisation?

GDPR compliance is a must do. It does not help DAF to build trucks faster, cheaper or better. The only business case for doing GDPR is avoiding the significant fines for non-compliance.

For the information security organization, GDPR introduces the need to produce and maintain a wide range of documentation.

In what way does Secura support DAF Trucks?

Secura has a leading role at DAF within the connected truck program. Secura performs risk analyses, penetration tests and also provides consulting for the new design of secure hardware modules for the connected truck program.

DAF Trucks

DAF Trucks is a leader in the design, manufacture and customer support of high-quality premium trucks and a wholly-owned subsidiary of PACCAR Inc.. Johannes Denissen is Head of Information Security and Incident Response for DAF worldwide and for PACCAR Financial Europe.

Ralph Moonen, Technical Director

Meltdown, Spectre and 'Cozy Bear'

Since our last SecurAware, many interesting hacks and vulnerabilities have surfaced. Obviously the Meltdown and Spectre bugs are important, because we will suffer from these for a long time to come. Also notable is the revelation that the Dutch AIVD was able to hack and track the Russian hacking group 'Cozy Bear' for a long time. This is also notable because it is very uncommon for such an intelligence position to become known publicly so soon after it existed.

As for Meltdown and Spectre, it is clear that not all is known yet. Vendors have released BIOS patches, and retracted them again. Intel has provided microcode updates but they are reported to be crashing servers.

A little background

Side channels attacks are well known and have been used to break all kinds of security measures. They rely on physical characteristics of systems changing, depending on what they're doing. You can measure and sometimes manipulate these characteristics and by analyzing them, that they should be keeping a secret. For instance, by measuring the power consumption of a chip, it is sometimes possible to extract the encryption key it is processing at that time. Or, by measuring the radio frequency emanations of a CPU, you can statistically deduce the plaintext of a communication. In the current case, it is a timing attack. Measure the time it takes to retrieve a byte from memory and you can tell if it was in the cache, or if it was retrieved from actual RAM. How can we tell the value of the byte from this? Well, we can't, not directly. But we can indirectly. CPU's use a trick to speed things up: when they encounter a branch in the executed code, they execute BOTH possibilities, and only choose which value to return, after evaluating the branch condition. Timing cache hits in memory then reveals the value of the memory location! For a very readable and detailed write-up of these techniques, I refer to Bert Hubert's piece [https://ds9a.nl/articles/posts/spectre-meltdown/].

> We are confident that the vendors will release more stable patches soon

To patch or not to patch?

So, as for the question, can you afford to not patch? Exploitation of these bugs rely on being able to execute code on the target machine. But Javascript in a browser window is also code execution and there are so many scenarios for an attacker to attain code execution that we can answer that question pretty easily with a resounding 'no, you must patch the OS'. And doubly so in shared (cloud) environments! In fact, it is for exactly these kinds of attacks that we advise against running any kind of security critical applications in the cloud. But two side notes are relevant: there is a performance hit (the cache exists for efficiency reasons, and removing the use of cache also removes efficiency). And also, Microsoft has introduced a new mechanism to determine if the anti-virus software plays well with the patches. A new registry key is introduced signaling the AV-vendors compatibility with the patches. Read up on this issue here [https://doublepulsar.com/important-information-about-microsoft-meltdown-cpu-security-fixes-antivirus-vendors-and-you-a852ba0292ec].

More stable patches soon

Nevertheless, you simply cannot fully patch a microcode vulnerability in the OS layer. There will always remain avenues of attack. Therefore hardware vendors have released BIOS patches, and Intel has released microcode patches. Unfortunately, it turns out that these patches have unwanted side effects in some cases, including crashing and rebooting servers. Even when using a test-server, it still remains risky to apply these patches in production systems, and it is therefore that we advise against applying these BIOS and microcode patches if availability is important for your business. We are confident that the vendors will release more stable patches soon. We will keep you updated in blog articles on our website.

Cozy Bear

The other piece of notable news was the Dutch AIVD hack of Cozy Bear. Normally, intelligence agencies are extremely careful not to make their intelligence position and capabilities known. In this case, a journalist was able to report in detail on this hack. Obviously, he was fed this information, and it was probably not by the AIVD since they have now had their capabilities exposed. So probably some US party disclosed these details intentionally, to this journalist, at this specific time. It is speculation, but one can imagine that the US wants to send a clear signal to Russia: "We have strong allies, and you are not the only ones that can hack!" But we also have a referendum on intelligence agency capabilities coming up soon, and some parties might want to make our AIVD look very strong and capable. We might never know the real reason but it is slightly worrying that this level of hacking activity is now considered normal in the world.

Your privacy is important to us

We are pleased to share our knowledge with you. We do this by offering our newsletter SecurAware (three times a year), organising the annual security conference Black Hat Sessions (BHS) and through our updates and blog posts.

Would you like to keep up to date and receive interesting offers such as a special rate for attending the BHS (see page 14). Please subscribe for the next SecurAware by post and/or digitally: www.secura.com/subscribe.

Your privacy is of the utmost important to us. If you no longer appreciate to receive our newsletter please unsubscribe at www.secura.com/unsubscribe. We will respect your privacy and remove your data from our mailing list.

Do you have a question or are there any changes in your e-mail and/or postal address? Please send an email to marketing@secura.com.

Subscribe now at www.secura.com/subscribe and we will keep you up to date!

Ruud Kerssens, Manager Service Line Advisory & Audit

GDPR: Ready?

The General Data Protection Regulation (GDPR, or AVG for Belgium and The Netherlands) is still a board-level issue. After more than two years respite, the GDPR will become effective as of 25 May 2018. Are you ready?

For some time now, legal advisors have supported their clients to become 'compliant'. Although they were able to clarify and interpret the regulation, their focus was mainly on determining the effect and impact for their client in terms of which processing activities were in scope and which legal requirements needed to be addressed. By now many corporate GDPR compliance projects are almost completed, but do they ensure privacy compliance?

Impact

With the introduction of the data breach notification rules in the Netherlands (2016) and the finalisation of the GDPR (April 2016), privacy compliance has become a board-level issue mainly due to the fines that can be given. The maximum fine can run up to 4% of global revenue (or € 20 million). This could create major impact, obviously. Furthermore data breaches could have a large impact on the reputation of the company. It is useful to understand what the GDPR exactly means and to be aware of the impact of non-compliance. Please see our previous SecurAware for further clarification about the impact of the GDPR.

We must not forget that the original intent of the GDPR was to set rules on how to process personal data, instead of just restricting the use of personal data. The GDPR sets an EU-wide standard in addition to separate laws and regulation per EU country (that are harmonized to a certain extent). Therefore this is the perfect time to raise the level of control regarding the processing of personal data and that is certainly a positive effect of the GDPR. But management should be attentive to their GDPR compliance status, whether the impact is positive or negative.

Recent developments

In 2016 and 2017 the WP29 (Article 29 Data Protection Working Party) - where the national supervisors discuss the impact of the GDPR – published guidelines and opinions. As the GDPR allows national authorities to add national rules for certain rule settings (Article 87), additional local regulations are implemented, including in The Netherlands. The draft version of the Dutch "Uitvoeringswet Algemene Verordening Gegevensbescherming" (UAVG) describes the intended additions for the Netherlands. But other countries are also working on additional rules, e.g. Belgium and Germany. Pending some important guidelines concerning profiling, data breach notification and binding corporate rules, you should at least pay attention to the following already adopted guidelines:

Determining lead supervisory authority

It is important to know the lead supervisory authority of your organisation because of the local adjustments to the GDPR that are implemented by governments and the identification of the organisation you need to communicate with as Supervisory authority.

Remarks:

1. If processing takes place in foreign countries this is not by definition 'cross border processing'. Supervisory authorities will decide and take into account: the context of the processing, the type of data and the purpose of the processing E.g. analysis of special categories of data;.
2. The main establishment of the organisation is the starting point for identifying the relevant supervisory authority. Critical parameters are the central administration location and/or the location where the decisions on the purposes and means of the processing of personal data are taken;
3. The guideline explains the key concepts on how to identify the leading supervisor authority and describes its role.

Data protection officers (DPO)

This guideline was re-adopted on 5th April 2017. According to the GDPR the DPO should facilitate the organisation in complying with the provisions of the GDPR.

Remarks:

1. A DPO can be mandatory. Be aware that these criteria apply to both controllers and processors!
   a. A public authority or body is involved;
   b. The core activity is monitoring subjects on a large scale;
   c. The processing is on a large scale and with special categories of data or criminal related data;

2. Designation of a single DPO for several organisations is allowed with some additional requirements (especially availability and accessibility);
3. The guideline provides criteria for the DPO's experience and skills;
4. The guideline provides a description of the position and tasks of the DPO in the organisation.

Data protection impact assessments (DPIA)

This guideline was revised and re-adopted on 4th October 2017. Article 35 of the GDPR introduces the DPIA as a process to describe the (intended) processing and to determine necessity, risks and measures.

Remarks:

1. The data processing controller is responsible for the execution of the DPIA;
2. Mandatory for new - and sometimes required for existing - processing operations that involve "probable high risk to the rights and freedoms of individuals";
3. The DPIA should be carried out "prior to the processing";
4. A single DPIA could be used to assess multiple processing operations that are similar in some terms;
5. DPIA's should be continuously reviewed and regularly re-assessed. Carrying out a DPIA is a continuous process, not a one-time exercise;
   If the identified risks cannot be sufficiently addressed by the data controller the supervisory authority must be consulted;
6. An acceptable DPIA should comply with the criteria in the Annex 2 of the guideline.

National Identification number (Burger Service Nummer, or BSN)

Because of the UAVG we understand that the implementation of the GDPR in the Netherlands is supposed to adhere to the former interpretation and regulation in the WBP as much as possible. The requirements regarding a special category of data, namely so-called "sensitive data", are nearly equal to those in the WBP. While the BSN is not a special category of data (Article 9 GDPR) the use of the BSN is restricted (Article 46 UAVG). The processing of BSN's is only allowed if the processing is laid down in the law or in general administrative regulation (known in Dutch as an "Algemene maatregel van bestuur" or AMVB). One example is the recently implemented Dutch law on personal data use in healthcare, including additional stipulations (in the "Besluit elektronische gegevensverwerking door zorgaanbieders"). It tells us that organisation processing a BSN for healthcare institutions, need to show their compliance (not certification) with NEN 7510, 7512 en 7513: the healthcare information security standards in the Netherlands including privacy rules.

> "As part of the accountability requirement of the GDPR it is important to address and audit controls in the check part of the PDCA process

GDPR compliance: are you in control and accountable?

The implementation of controls and processes to comply with the GDPR, appear to have a lot of impact. Most effort is invested in projects to become compliant. At this point the challenge is to get continuous control with a Plan Do Check Act (PDCA) process. Because the GDPR is a moving target, referring to WP29 publishing guidelines, opinions etc. and the implementation of the GDPR in local regulation, it is essential to continuously monitor developments around the GDPR.

Concerning the coming deadline of May 25th 2018, we advise to check your status and level of control with assessments or even audits to identify the last remaining actions. As part of the accountability requirement of the GDPR it is important to address and audit controls in the 'check' part of the PDCA cycle.

This could be a periodical privacy audit or a verification of any performed PIA's, as they are the essential identification process for determining the impact of processing of personal data. Be aware for recent developments like guidelines of the WP29 and the finalizing of the "Uitvoeringswet AVG" as they contain important clarifications of the GDPR.

25 May 2018 is just the beginning.

BHS 2018

Take control of your digital security (before someone else does)!

Secura might have changed its name, but the Black Hat Sessions are returning as usual in 2018! On June 14th we will organise the sixteenth edition.

Black Hat Sessions (BHS) is Secura's annual security conference in which you get informed about the latest trends, threats and solutions in the world of Digital Security. Informative for decision makers, managers, CISOs and for technical security experts. The sixteenth edition of BHS will see an improved programme, a new venue, more space, and a Capture-the-Flag (CTF) competition aimed at student teams from University or Higher Education.

The theme for our 2018 edition is 'Take control of your digital security (before someone else does)!'. Although the year is still young, the Spectre and Meltdown vulnerabilities are hot on the heels of the major revelations in 2017. We are sure there is much more to come. Let's not forget the GDPR coming into effect in May. In our BHS 2018 programme we will be bringing national and international speakers together to present their research, or to provide valuable insights into relevant and actual topics. Some of the topics that will be covered in the programme include: GDPR, Red Teaming, Hardware Hacking, Privacy, IoT & cloud security… All you need to know to take control of your digital security (before someone else does).

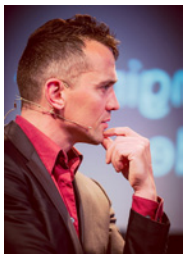
This year we will have multiple tracks besides the keynotes. These multiple tracks will be repeated twice so that missing a talk before lunch can be compensated after lunch. Of the four tracks, two will be really technical, and two managerial. Please note! There is a maximum number of participants per session. We would like to create an informal setting and promote interaction.

New edition, new venue

Our new edition will offer more and content of a higher quality in an improved venue. In the coming weeks we will be providing more information on the exact program and speakers. Keep an eye on the website www.blackhatsessions.com for the most up to date information.

REGISTER NOW AT WWW.BLACKHATSESSIONS.COM

Host



The BHS will be hosted by Chris van 't Hof, internetsociologist, presentor & author of the book Helpful hackers. Chris van 't Hof is an independent researcher, writer and presenter in information technology. With his background in both electrical engineering and sociology, he analyses the interaction between human and electronic networks. His eight book came out in March 2016: "Helpful Hackers. How the Dutch do Responsible Disclosure." His company Tek Tok organises conferences, workshops and IT security training. He also has his own talk show: Hack Talk.

Keynote Speakers

Adam Laurie (Aperture Labs Ltd.)
We are proud to have Adam Laurie (RFIDIOt, Aperture labs) to give a keynote. Adam Laurie is a security consultant working the in the field of electronic communications, and a Director of Aperture Labs Ltd. who specialise in reverse engineering of secure embedded systems.

Ralph Moonen (Secura)
Ralph Moonen, Technical Director at Secura, will present recent research that Secura performed regarding several topics, including the security of SSL certificates in the Netherlands, and the security of 4G voice communication (Voice-over-LTE, or VoLTE). We have discovered weaknesses in certain widely used devices and 4G-networks and will provide you with new insights into the risks.

Michel van Leeuwen (NCSC)
Michel van Leeuwen is Head of the Cybersecurity Policy Department (National Coordinator for Security and Counterterrorism), Ministry Security and Justice in the Netherlands. Michel van Leeuwen will give a keynote speech 'Cybersecurity, Next Steps in Policy in the Netherlands and EU'.

Side Track (management)
Security Compliance & Certification

How to measure the security of your software? How to benchmark the security of your organisation? This all depends on clear frameworks, guidelines and standards. In this track, new developments will be discussed such as the Guideline for Cloud Service Providers by the European Banking Authority, the Baseline Security Assessment Scheme (BSPA) of AIVD and the Meta-Security Scheme by the European Cyber Security Organisation (ECSO). **Miranda Chilvers-van der Kruk** (DNB) will present the scope of the EBA guideline and the relevance, important for cloud-service providers. The session will be closed with an interactive panel discussion between all experts and interested parties.

Side Track (management)
GDPR – Privacy by Design and Accountability

GDRP is alive now! GDPR is effective in all European Countries since May 25 2018. How do we guarantee privacy compliance in our processes? Challenges in getting processes work properly and identify privacy security issues, address them and implement the necessary controls in an adequate way. In this management stream we cover two important aspects that appear to be question marks for organisations which are eager to stay in control: **Fabian van den Broek** (Open University and Radboud University) will speak about Privacy by Design. **Wolter Karsenberg RD** (member of the Knowledge Group Privacy Audits of the NOREA) will speak about Accountable Privacy. We will finish the session with an interactive debate.

Register now

Relations of Secura will only pay 240 euro until April 20th 2018. To do this, use the code Secura#18 in your online registration.

BHS

Thursday 14th of June 2018
09:30 – 17:00
National Business Center (NBC) - Nieuwegein Utrecht (NL) NEW VENUE!

Price EURO 320
Student fee EURO 65

INFORMATION AND REGISTRATION
www.blackhatsessions.com

Side Track (technical)
Red Teaming

This track will focus on Red Teaming. From OSINT to Purple Teams and data exfiltration. We will present our latest insights and share techniques for blue teams also. Instead of just testing your applications, why not test your whole organisation? **Leen van der Plas** from (SoSecure) will speak about predicitive threat modelling and the physical side of Red Teaming.

Side Track (technical)
IoT -SCADA embedded

This technical track will cover topics including hardware security and vulnerabilities in SCADA/ICS networks. And we might just even throw in a technical talk about blockchain security ;-) If you are interested in new technologies that are going to impact our lives and want to learn about their vulnerabilities, this is the track to go to.

SecurAcademy

When it comes to training and awareness, Secura has a solid track record. Secura's experts are pleased to share their knowledge with you. The following practical training courses are planned and open to join.

MANAGEMENT

8 May
GDPR live (Executive Overview)

In this 1-day course you will receive an overview of the GDPR and you will be updated about recent developments, guidelines and best practices. You will get a thorough understanding of the GDPR regulation, the impact and how to ensure compliance.

14-18 May
Certified ISO 27.001 Lead Implementer training (incl. Exam)

Master the implementation and management of Information Security Management Systems (ISMS) based on ISO/IEC 27001. After mastering all the necessary concepts of ISMS, you can sit for the exam on day 5. The 'PECB Certified ISO/IEC 27001 Lead Implementer' 3-hour exam fully meets the requirements of the PECB Examination and Certification Programme (ECP).

27-29 June
Masterclass GDPR Live (incl. DPIA and workshop)

As of May, GDPR will be a fact within Europe. But how to approach it? The first day of this masterclass will give you an overview of the status of the GDPR, recent development, guidelines and best practices. The second day you will learn how to perform a Data Protection Impact Assessment (DPIA). In the last day, we focus on Privacy by Design and Privacy by Default. This gives you all the essentials to act as a GDPR professional.

TECHNICAL

10 April
Secure Programming Training

Train your developers to improve security at the creation stage. Learn how to find and exploit common vulnerabilities in web applications, such as Cross Site Scripting and SQL Injection, as well as steps to mitigate these issues in code.

19 April
Masterclass OSINT Information Gathering

Open Source Intelligence (OSINT) is critical for Red Teaming. Improve your OSINT skills by learning how to improve internet searches and create a clear overview of your findings by the OSINT guru Arno Reuser. You have nothing to hide. This course is intended for white/blue team members and intel-lovers.

3 May
Hands-on Hacking Workshop

A fun and practical 1-day course to gain insight how hackers can break into your organization. First, you will see how an attacker will become the Domain Administrator of an organisation after compromising the laptop of an employee. Afterwards, in a practical session, you will be able to setup a Raspberry Pi as an attack platform to gain this first foothold in an organisation.

3-4 July
Mobile Application Hacking Training

Combining the fast world of security and mobile apps, this course teaches you how to assess mobile app security by our own Secura experts. Armed with in depth information about the Android and iOS environment, your developers or pentesters will learn to identify security flaws in iOS & Android apps.

www.secura.com/securAcademy

TAKE CONTROL OF YOUR DIGITAL SECURITY