#01 OCTOBER 2017

EDITED BY Secura

SecurAware

Secura
Formerly known as Madison Gurkha

INSIGHT
New control set DigiD

EVENT
Report BHS15

ADVICE
Are you prepared for the GDPR?

HACK NEWS
Interesting Times

Interview Hans de Zwart (BoF)
The Future is False Positive

NEW NAME, NEW LOOK, SAME QUALITY

Secura: take control of your digital security!

As you open our new magazine you might not immediately recognise us, but you will have guessed by now that Madison Gurkha has changed its name! We are quite excited about this and want to tell you the background of this important change and how it will affect you.

Most likely you have worked with Madison Gurkha previously. Our company built a strong track record in ethical hacking, penetration testing and security training. We may have tested your infrastructure or applications, or provided training. These services are delivered by a strong and growing team of security experts. And with that expertise we can do more, which is why we recently launched services like Continuous Scanning and Red Teaming.

Earlier this year we added an Audit & Advisory service portfolio to the Madison Gurkha offering including ISO 27001, Privacy/GDPR and DigiD audits through integration of our former subsidiary ITSX. You can read more about it in our previous Update 29.

Recently, we opened a new office in Amsterdam to serve our clients in the West of the Netherlands better. We also received our ISO 9001 and ISO 27001 certifications.
As you can see, our company is in a transition!

And now, finishing of this important transformation, we have changed the name Madison Gurkha into Secura to emphasize that we reposition our business: from an ethical hacking company into a knowledge center for digital security with a wide range of services.

In order to highlight all the changes, our business has undergone a complete rebrand including a new corporate identity with a new look and feel that matches our future ambitions and plans. We really look forward to continue building on our strong brand to support you with the best and up to date knowledge to take care of your digital security needs.

We currently have four service lines within Secura:
- Advisory & Audit
- Testing Services
- Certification Services
- Training & Awareness

We will continue to grow the company: by hiring more experts, by investing in R&D and service development, by doing exciting projects (a lot of learning by doing!) and by focusing more on international projects.

Security is a hot topic. Recent hacks and ransomware attacks like WannaCry and (Not)Petya show that society is still vulnerable across many industries. There is a lot of work to be done and Secura has the ambition to become an internationally recognised thought leader on this subject.

Dirk Jan van den Heuvel
Managing Director

Infosecurity.nl, Data & Cloud Expo 2017
1 – 2 November, Jaarbeurs Utrecht

Infosecurity.nl is the foremost Dutch tradefair in IT security for both managers as well as professionals. We will be there so we can inform you, in an informal setting, of our ambitions and more importantly to discuss the latest trends in the area of digital security including the GDPR, Red Teaming and any security issues you would like to control. We welcome you at our new Secura booth: A042.

Opening of our Amsterdam Office 30 November, 15h – 18h, Amsterdam

We are very proud to announce the opening of our new office in Amsterdam. This office will make it easier to serve our clients in the Randstad, while reducing travel time for our consultants and our CO2 footprint.

Good reasons for us to celebrate this milestone with our customers and relations. On Thursday 30 November, 15h – 18h, we will host an open house party in our new Amsterdam office (building The Yard, Karspeldreef 8, Amsterdam). Between 16.00h and 16.30h the official opening ceremony takes place. You are most welcome to join us for drinks and some networking.

If you would like to come, please register through www.secura.com/opening or by sending an email to rsvp@secura.com

Article of the year

The Article "Apple vs FBI: de feiten op een rijtje" (in Dutch) written by our security consultant Matthijs Koot, that was published in IB Magazine 2016 #5, won the second price in the "PvIB Article of the year 2016 competition". Congratulations! The complete top 3:

1. Marijke Stokkel, Zo wordt het een succes.
2. Matthijs Koot, Apple versus FBI: De feiten op een rijtje.
3. Peter Kampman, Risicoanalyse: Privacy versus informatiebeveiliging.

Read more: https://www.pvib.nl/actueel/nieuws/artikel-van-het-jaar-2016

ISO 9001 and ISO 27001 Certified!

In taking control of your digital security, we maintain the highest levels of responsibility, care and customer service. To seal the establishment of our Quality Management System meeting the requirements of ISO, an external auditor from BSI has been performing an ISO 9001:2015 and ISO/IEC 27001:2013 audit. The result was a positive advice to certify Secura for both standards!

bsi. ISO 9001 Quality Management | ISO/IEC 27001 Information Security Management

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

Ester van Dael

The Future is False Positive

Hans de Zwart is CEO of Bits of Freedom, the civil rights organisation defending two fundamental rights regarding digital communication that are indispensable for your freedom: privacy and freedom of communication.

Bits of Freedom exists more than 15 years. What did you achieve the past years?

I think the biggest achievement is that we had net neutrality as the first country in Europe and the second country in the world: by law it is regulated that Internet providers treat all internet traffic in the same way, which will also be included in European legislation. Additionally, we eliminated a number of download prohibitions and upload filters from bills. Another important achievement is that we organise the Big Brother Awards for 12 years already, and the event keeps growing. The Dutch government is one of the first governments in Europe to explicitly make a statement regarding encryption: the cabinet does not wish to weaken encryption despite terroristic threats. I think that the internet culture in the Netherlands, to which we contribute, played a role in this decision.

What did you not achieve yet and what would you like to bring to the attention?

In my opinion that would be the stopping of mass surveillance. Just before the elections, the 'sleepnetwet' was passed by the Tweede Kamer. This is a law regulating the power of secret services. One of the authorisations in that law is the 'sleepnet authorisation', which gives them permission to monitor people on a large scale at random – so without having any prior suspicions. There is a trend that because surveillance of the entire population has become affordable, it is also happening. That is very worrisome.

> There is a trend that because surveillance of the entire population has become affordable, it is also happening. That is very worrisome.

The 'sleepnetwet' now has to be passed by the Eerste Kamer. There are a lot of problematic aspects of this law, that probably are unacceptable from a human rights perspective as well. Thus we are exploring if, in case the law is passed, we can appeal it through a judge.

What do you consider other worrisome developments regarding privacy?

Another problematic development is related to the dominant online business model at the moment: 'surveillance capitalism'. A company collects as much data as possible from people, analysis this data, and tries to create models using data scientists and machine learning algorithms. With these models companies try to predict behaviour. In the last phase this predicted behaviour is sold at 'prediction markets'.

The most famous example of this is the way Google handles ads. But of course there are many other instances, and because making behavioural predictions is driven by data, there is a tendency to store more and more of our information. The question is: when does prediction of behaviour change into creating or manipulating behaviour?

> The question is: when does prediction of behaviour change into creating or manipulating behaviour?

Regarding a number of the latest elections, for instance concerning Trump, there has been a lot of discussion to what extent social media played a role in his election. In the end it seemed not too bad, but you can imagine that Google, if they wished to do so, could influence the elections by choosing which information they do or do not show. And the number of domains where Google can influence our behaviour is growing. Because we all use e-commerce, Google can track all the movements of the civilian. Companies thus sometimes know more about us than we know about us, and than governments often know about us. And because these companies aren't under some sort of democratic control, it appeared to be very hard to hold them accountable, which I think is very troubling.

What does Bits of Freedom think of the GDPR and why?

We are moderately positive about it. There are a couple of matters that are just not sufficiently taken care of, in our opinion. For instance what is and is not allowed regarding profiling and that there is too much freedom once you have consent of the consumer. This is one of the most lobbied for legislative procedures ever. There is a lot of pressure from companies to take out certain details, and unfortunately those companies managed to do so. Having said all this, the GDPR definitely is a step forward, because of all the individual rights you gain as a citizen.

In the US they have 'the 'California Effect'. California has such a big internal market in the US, that when California passes a new bill, it is often easier for companies to comply to those rules than to stop doing business with companies in that state, and often it is then cheaper to comply to the Californian rules for all of the US. A famous example of this is when California got new legislation for car emissions. The response was that cars with less emissions were put on the market throughout all of the US. I hope that the GDPR will cause a 'California Effect': that Europe will manage to regulate companies such as Google in such a way that it improves for the whole world.

Will the GDPR lead to more of a 'tick box culture' in companies? Or do you think companies will also still actually make an effort for information security and prevention of data leakage?

I have a somewhat cynical perspective on companies, because in many cases it is simply rational for a company to stay only just within the limits of the law. What you do see, is that that should be done with a certain societal legitimacy, just like in the food industry where more and more companies have organic products because customers deem that important. It then becomes irrelevant whether the company considers that actually important themselves. I hope that we are moving to a society where there is such a level of knowledge of the workings of our digital world and who are winners and losers in that world, that companies will be kept on track by their customers. There also exist companies that consider privacy a unique competitive advantage: if two companies provide the same service, but one of them also provides privacy protection, I think most people prefer the company with privacy protection. I think this provides a lot of opportunities.

Of course it is the case that to a certain extent there will be a tick box culture within companies, but at the same time a tick box culture isn't necessarily bad. As long as you really go through all the steps, checklists and ticks make sure that at least there will be more attention for a certain subject, which makes people more aware and hopefully motivates them to make responsible choices.

This is a shortened version of the interview. If you're curious to read the full version, please see the extended interview on our website (in Dutch): https://www.secura.com/interview-hansdezwart.

CV

Hans de Zwart is the Executive Director of the Dutch digital civil rights organisation Bits of Freedom, fighting for freedom of communication and privacy on the internet. In the past he was Shell's Senior Innovation Adviser for Global HR and Learning Technologies, before that a Moodle consultant for Stoas Learning and he started his career as a Physical Education teacher at a high school in Amsterdam. He operates on the intersection between technology (which he prefers to be "open") and society, often viewing issues through a civil rights lens. He knows that technology is always political and believes in the power of design.

Bjorn van der Schaaf

New control set DigiD

The DigiD assessment scheme was introduced in 2012 by Logius for systems and applications that use the Dutch national authentication mechanism. The assessment scheme contained a number of controls based on the ICT-security guidelines published by the Dutch National Cyber Security Centre (NCSC).

The NCSC has updated their guidelines in the mean time and this has lead to the situation that the DigiD controls were not in sync with the NCSC guidelines. Additionally, assessors have been critical about the actual controls selected and the varying level of technical detail, auditability and sensibility of the controls.

Therefore Logius has introduced a new set of controls that will go into effect as of 21 november 2017, and be applicable to all DigiD-connected applications. The professional organisaiton of IT-auditors in the Netherlands, the NOREA, has issued an updated audit guide for their members who perform such DigiD assessments.

Just as in the first version of the control set, the second version is based on the NCSC guidelines. However the actual selection differs somewhat. Some subjects get a little more attention, others less. This is motivated by a change in risk areas and a wish to lighten the burden of the audits.

The new control set focuses more on themes such as:

- Logging and monitoring
- Secure programming
- Incident detection and response

On the surface, the controls look quite different than previously; this is due to the new numbering scheme that the NCSC has introduced, and the categorizing of controls along so-called 'domains':

- Policy (B)
- Execution: Access control (U/TV)
- Execution: Web application (U/WA)
- Execution: Platform & Webserver (U/PW)
- Execution: Network (U/NW)
- Management / 'Control' (C)

What has changed?

The new control set has 20 controls divided over the six domains, while the old set had 28 controls. Some controls have been completely dropped, other have been combined. In general, the abstraction level of the controls has been made more consistent.

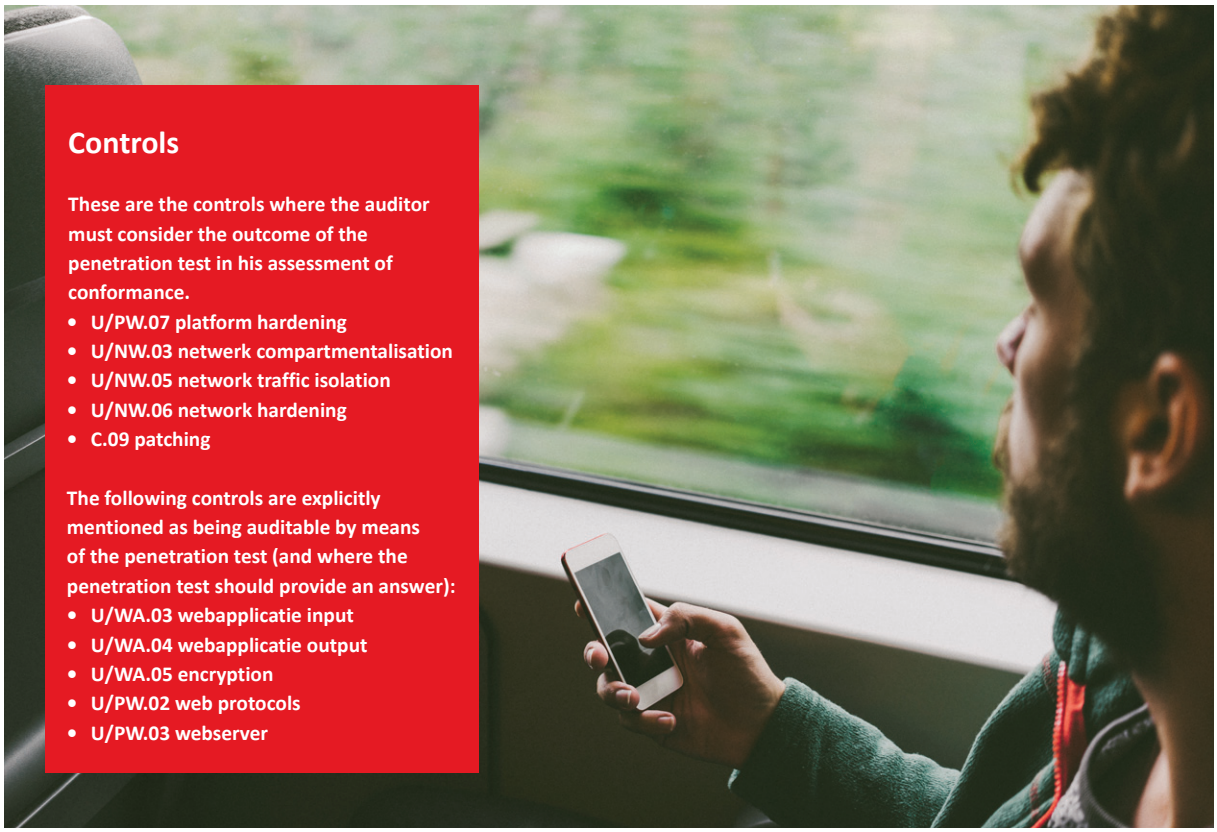
Because some controls have been combined, and new ones based on the new NCSC guidelines, the individual controls cover more ground than the old controls. In fact, when relating the new 20 controls, they can be related to 38 old controls from the NCSC guidelines instead of 28!

The owner of the DigiD connection will need more attention for several subjects in order to pass the audit. Where relevant, additional measures must be implemented at vendors (software, hosting, application, SaaS, etc.).

1. Logging and monitoring coupled with incident detection and response

Controls dealing with implementation and use of IDS/IPS systems get more focus in the new situation. Logging and monitoring are connected to this. Questions organisations should ask themselves are: will data traffic anomalies be detected? What if logging patterns start to change? How much time does it take to detect that and what are you going to do? Does logging and monitoring cover the full stack (network, OS, and application)?

> Simply sitting back and waiting for the result of the penetration test is not a guarantee for a successful audit



Controls

These are the controls where the auditor must consider the outcome of the penetration test in his assessment of conformance.

- **U/PW.07 platform hardening**
- **U/NW.03 netwerk compartmentalisation**
- **U/NW.05 network traffic isolation**
- **U/NW.06 network hardening**
- **C.09 patching**

The following controls are explicitly mentioned as being auditable by means of the penetration test (and where the penetration test should provide an answer):

- **U/WA.03 webapplicatie input**
- **U/WA.04 webapplicatie output**
- **U/WA.05 encryption**
- **U/PW.02 web protocols**
- **U/PW.03 webserver**

2. Secure Programming

Important controls deal with with input and output validation of the application. Building a secure application will need to have controls in the secure programming realm, and attention is necessary for development, test and production environments. Controls that protect against the OWASP top 10 classes of vulnerabilities must at least be in place. Source code reviews can be used for this but that is not mandatory. By adopting secure software development frameworks and automated testing it can also be assessed by the organisation that they comply. Simply sitting back and waiting for the result of the penetration test is not a guarantee for a successful audit.

So should be throw all documentation from previous years away? Absolutely not! Documents and evidence from previous years can be changed to follow the new numbering with relative ease. However it will be necessary to perform a self-assessment or gap-analysis to find out what documentation is missing with regard to the previous version.

The role of the penetration test

The penetration test in mentioned in several ways in the standard:

- From a process standpoint
- The results of the tests
- Coverage of the controls.

From a process standpoint, the management controls state that the DigiD web application, the server, and also other servers in the same DMZ as a the DigiD application, must be tested periodically (at least yearly), AND when there is a specific reason to do so (usually interpreted as a major change being implemented). The NOREA guide also states that the penetration test should take place in the time frame of the audit. Secondly, test results (findings) must lead to actions and these actions must be monitored to ensure progress. The penetration test is mentioned in several controls as a means to (partially) cover these controls.

Conclusion

The new standard v2.0 does not deviate hugely from the previous norm, as a first glance at the numbering system might imply. But it's also not simply a case of renumbering the old norms. The focus on a number of domains and the rewritten NCSC controls do mean that organisations are advised to:

- Study the formulations of the new controls and the new guidelines from the NOREA.
- Give attention to the domains dealing with secure programming, loggin and monitoring and incident detection/response.
- Map existing documents, processes and evidence to the new control set.
- Perform a gap analysis to the new control set well before the actual audit is performed.
- Implement additional measures based on the gap analysis.
- Make sure that penetration tests, TPM-reports, ISAE3402-reports etc. are in line with the new control set.

To read more: www.secura.com/DigiD-audit

Sources

1. https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
2. https://www.logius.nl/fileadmin/logius/ns/diensten/digid/assessments/120221_norm_ict-beveiligingsassessments_digid.pdf
3. https://www.norea.nl/download/?id=2562

Matthijs Koot | Senior security consultant, Secura

WPAD
still standing its (quicksand)ground

During penetration tests performed at internal networks, one objective is to obtain credentials and gain foothold in an authenticated environment. A range of theoretical attack paths to obtain credentials can be dreamt up for any environment, but not all paths are equally likely to be traversed successfully.

One attack path that we find to (still) often yield success is the abuse of Web Proxy Auto-Discovery (WPAD), a feature that is enabled by default on Windows and Internet Explorer systems.

A specification of WPAD was drafted in the previous millennium by a consortium that had usability in mind: to help computers find an internet connection when connected to a network, without the need to configure a proxy server. The draft specification expired in 1999 [https://tools.ietf.org/html/draft-ietf-wrec-wpad-01] and never reached the status of Internet Standard --- but WPAD is still present and found in today's networks.

Vulnerable client

WPAD depends on DHCP or DNS, and on Windows systems can additionally fall back on LLMNR or NetBIOS (NBT-NS). If the DHCP server does not provide a WPAD url (something like "http://example.com:80/wpad.dat", where example.com is an internal system), DNS is used as fallback mechanism. On Windows, Link-Local Multicast Name Resolution (LLMNR) and NetBIOS are also used as fallback mechanisms. A computer that has WPAD enabled --- again, this is the default setting in Windows --- but does not get a WPAD url via DHCP, periodically sends out a discovery request using fallback mechanisms. When DNS-, LLMNR- and NetBIOS-responses are unauthenticated, and they often are, an attacker can send a fake response and make the vulnerable client send all HTTP traffic through an attacker-controlled proxy server. The WPAD process takes place without human interaction and if the attack is performed with due diligence, it does not disrupt the user's communication.

Authentication

When the user opens a website in their browser, the attacker's proxy can inject HTML code that fetches an image over an SMB url pointing to the attacker's proxy. If the user is NTLM-authenticated,

> Employees, including users, sysops and developers, should always feel encouraged, never blamed, for reporting on unusual activity!

the browser will send an SMB request accompanied by an authentication token, which the attacker then possesses. This is all without human interaction, too. Alternatively, the attacker can inject a fake login prompt. If a network is set up such that users are, under normal circumstances, sometimes prompted for their credentials --- for instance to log on to an intranet site even though they already entered those to access their system --- they might very well supply their credentials. If the user is already authenticated to a non-HTTPS intranet site, such as through NTLM authentication, existing authentication tokens can be readily observed by the attacker and, depending on circumstances that exceed the scope of this explanation, be directly re-used by the attacker, or be cracked (for instance using hashcat).

Update mechanisms

If the client system is power-on but not in active use by the user, authentication tokens can still be observed if the client runs auto-updating software, for instance anti-virus, that gets updates from an internal server over an authenticated (but unencrypted) HTTP-connection. Update mechanisms should be configured to use non-user accounts (i.e., a computer account or service account) that have long and random passwords, and that have the least viable privileges on internal systems. In practice, this is not always the case; an attacker may then, depending on circumstances, use this information to obtain a foothold.

Don’t use WPAD

Abusing WPAD has always been relatively trivial from a technical standpoint; and the open source tool Responder, created by SpiderLabs and now maintained by lgandx, makes it a breeze. The fact that WPAD is often deployed in insecure way is well-known for years; and more issues surround it, including that under certain circumstances, WPAD discovery requests can end up on the public internet [http://www.computerworld.com/article/3074509/security/top-level-domain-expansion-is-a-security-risk-for-business-computers.html]. It is left as exercise to the reader to think about the potential implications.

Our advice: don’t use WPAD. If that is not an option, make sure client systems only accept WPAD responses via an authenticated transport means, such as DHCP Authentication, DNSSEC, or signed NetBIOS. Make sure that users are never prompted for credentials when browsing intranet sites under normal circumstances, make sure auto-updates are done using properly (low-)privileged non-user accounts, enforce HTTPS on intranet sites, and promote security awareness. Also make sure the IT helpdesk has the right resources and attitude to help users recognise and report unusual activity, specifically including unexpected login prompts. Employees, including users, sysops and developers, should always feel encouraged, never blamed, for reporting on unusual activity!

Internships and IoT lab

As of 4 September 2017, Secura has entered into a co-operation with the Leiden University of Applied Sciences (UAS, or Hogeschool Leiden). The UAS, together with the Haagse Hogeschool and the department of Cyber Security & Resilience of TNO have recently started the IoT Lab at the HSD Campus in The Hague. The IoT lab is meant to allow students to perform research into IoT security and forensics.

Hans Henseler, lector Digital Forensics & E-Discovery at the UAS reached out to Secura and asked us to become sponsor of the lab, enabling students to perform a research internship for us at the lab.

Of course we were very enthousiastic about the plans and the possibilities of the lab. Ralph Moonen, technical director at Secura, comments: “It is vital that students practice their skills in an environment that is not only academic but also stimulates creativity. As a security company we fully support such initiatives and the interns that will be performing the research.”

Secura now sponsors the lab, and a student performing research into the security of automotive tracking dongles (Josefien Hupkes) has started her internship. In the coming time, additional interns might also begin research for Secura in the IoT Lab so we hope to grow and support internships at Secura in this way.

At this moment in time, the lab is still in the process of acquiring all the necessary equipment and software. In its final form it will host a small data centre, hardware analysis tools, soldering stations, and a multitude of software tools for digital forensics. We look forward to working with the IoT lab, and wish Josefien a succesfull internship!

Dirk Jan van den Heuvel

Are you prepared for the GDPR?

In our modern world, we use devices connected to the internet in our free time and in business. Smart phones, tablets and computers are connected and become more and more connected to other devices making it easier to do business, making our lives more comfortable and enabling government agencies to better interact with citizens. Doing business is built on trust. Trust in receiving the products and services in time and with the expected quality.

In order to obtain the services and products people will have to register and provide personal data. Customers/citizens do so on the basis of trust. They would like their data to be handled carefully and only used for the purpose they provided their data. The higher this trust is, the more likely it becomes that customers/citizens turn to your organisation. The commercial power and attractiveness of doing business with your organisation is built on this trust. Data protection today is an important customer value. Organisations that prove they have a high level of data protection and continuously work to improve their protection level have a substantial competitive advantage.

Privacy & Data Protection

It is therefore that privacy is an important aspect in todays connected world. Privacy is interpreted in many different ways. For instance:

- "the right to be let alone"
- protection of personal data
- the right to self-determination over one's personal data
- a basic human right: article 8.1 of the European Convention of Human Rights states that "Everyone has the right to respect for his private and family life, his home and his correspondence".

In many countries, there are laws and regulations in place to protect privacy. But they differ from country to country hampering the exchange of personal data between public and private sectors, associations and enterprises. If it comes to the digital world, the topic needs to be handled on a supra-national level. Therefore, the European Union has adopted the General Data Protection Regulation (the GDPR), which entered into force on May 24th 2016. and will be enforced from May 25th 2018 onwards.

The GDPR regulates how businesses, government institutions and other organisations in private and semi-public sectors should handle personal data in order to protect the privacy of individuals living in the EU. Emphasizing the importance of compliance, the penalty for violations of the GDPR can run up to 4% of global revenue (or of € 20 million).

A high-level overview of the GDPR

It is useful to understand what the terms "personal data" and "processing" mean.

According to article 4 subsection 1 personal data is: 'any information relating to an identified or identifiable natural person ("the Data Subject")'. This means that a photo, name, email address, telephone number, GPS location, IP address, bank account number or a social security number is personal data. The definition is quite broad leading to the effect that the impact of compliance to the GDPR on your organisation could be substantial.

Controller and Processor

The GDPR distinguishes between a Controller (the party who collects personal data), a Processor (who process data on request of a controller).

Special categories of personal data

Special care should be taken when processing of certain special categories of personal data, as described in article 9. These special categories are: data: ["revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"]. Processing data within one or more of these categories is strictly prohibited, unless one or more of the legal grounds for processing such data (article 6.2a-j, 6.3, 6.4) are applicable.

Principles

The processing of personal data needs to meet six important principles:

- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountability

Impact

By working accordingly to these principles both the controller and the processor need to provide the following rights of a person when processing personal data:

- Provide the data subject with transparent information, communication and modalities for the exercise of his/her rights (art 12)
- Provide information as to where the personal data are collected (art. 13)
- Provide extra information if the personal data has not been obtained from the data subject (art 14)
- The right of access to the personal data by the data subject (art. 15)
- The right of rectification and erasure of the personal data of the data subject (art. 16, 17)
- The right to restriction of processing (art 18)
- The right to notification regarding rectification or erasure of personal data or restriction of processing (art 19)
- The right to data portability (art 20)
- The right to object and automated decision-making, including profiling (art 21, 22)

Risk Management & Impact Assessments

In order to prove that the level of protection is continuously monitored and improved organisations need to conduct regular Data Protection Impact Assessments (DPIA) or Privacy Impact Assessments (PIA) if the activities are considered 'high-risk'. They should also perform these assessments to 3rd parties (processors) involved in the processing of personal data conducting Due Diligence into processors suitability and ensuring the GDPR compliance. It is therefore that the organisation needs to have clear Processing agreements (laid down in either contract or other legal act) in place with 3rd parties that handle these personal data in compliance with the GDPR. If personal data is transferred outside the European Union the joint controller(s) and/or processor(s) outside the European Union must ensure compliance to the GDPR and appoint a representative located within the European Union.

> "Towards the future, the GDPR leads to a different way of designing and developing processes and systems: Data should be protected by design and by default!

Incident Reporting

In case of a data breach or incidents there needs to be an incident policy and clearly described procedures. All incidents should be registered and analyzed to improve the processes involved. Data breaches need to be reported within 72 hours to the regulating authority. If there is a serious risk at hand that data subjects might be harmed in their interests the data subjects involved should be informed as well.

Conclusion

The impact of the GDPR is high for organisations handling (large quantities of) personal data. Most organisations, processes and systems today have not been designed to protect these data sufficiently and to ensure that these can only be accessed by authorised people. This means quite some changes need to be made. Towards the future, the GDPR leads to a different way of designing and developing these processes and systems: Data should be protected by design and by default (GDPR Article 25)! Secura is a professional partner who can support your organisation to comply with the GDPR. Please contact us for our GDPR service offerings as shown in the figure above. Professional compliance mitigates the risk of a data breach incident and generates customer value!

To read more: www.secura.com/en-privacy

Ralph Moonen

Interesting Times

As the story goes, there is an ancient Chinese curse: “May you live in interesting times”. The story, it turns out, is just a story. There is no credible source for it being a curse. However it very well could be, and the times we live in are certainly interesting. Just in the past few months, we have seen Bluetooth being cursed with a handful of major vulnerabilities, Equifax being hacked due to presence of vulnerabilities that border on the negligent, and the September windows patch containing no less than 38 fixes for zero-day vulnerabilities.

If this seems like a lot, well, it is. And while all these vulnerabilities were disclosed using Responsible Disclosure practices, we are left with the feeling that there are so many other vulnerabilities out there, waiting to, or actively being exploited by whoever finds them, or buys them from or through companies such as Zerodium or Absolute Zero-Day.

Let's take a closer look at these examples and try to find out what they actually mean and how much risk to users and companies is involved.

Blueborne

Blueborne is the name that security researchers Armis gave to the collection of seven vulnerabilities they discovered in Bluetooth implementations over a wide range of devices including Android, iPhone and Linux. Billions of devices are at risk. At the time of writing this article, there was no public exploit available yet but as you read this, there might well already be an exploit module for Metasploit available. Using this exploit it is possible to remotely take over a phone or IoT device, by just having Bluetooth turned on (no connection or pairing necessary).

Vendors have been rushing to make patches available but millions of devices are not easily patched, because they lack remote secure firmware updates. Cars are especially at risk, because often the entertainment system runs Linux under the hood, has Bluetooth enabled, and to make matters worse, is often connected to the CAN-Bus. The CAN-Bus is your in-car network that controls everything from braking to headlights, locks, and park-assist. For a demonstration of what that can mean I recommend looking back at the Jeep hack that Charlie Miller demonstrated some years back when he remotely took over a car and made it do strange things like suddenly turning left.

What this means is that car manufacturers are going to have to fix the problem by updating the firmware next time the car is in for maintenance. But not all cars receive maintenance from the official dealer (who of course is the only party that can update the firmware due to security restrictions). It remains to be seen which manufacturers are impacted and how they will deal with it but one thing is clear: this is not the last time that vulnerabilities on this scale will be discovered.

And not just cars, but all kind of medical devices (insulin pumps), consumer electronics (home automation, alarm systems) and trackers use Bluetooth while not being easily updatable. Interesting times indeed…..

Equifax

Equifax is a credit rating company. They keep credit scores for citizens and while this is not very common in Europe, in the rest of the world it is. As a consumer (or company), your ability to get loans and mortgages is not so much controlled by your bank, but by this independent third party that keeps tabs on your monthly credit card payments. This information is sensitive, and must be correct or else you could have a big problem when trying to buy a house or a car. In fact, Equifax collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide.

When Equifax was hacked, personal data of 143 million people was exfiltrated. According to the company, the breach lasted from mid-May through July 2017. The criminals got people's names, Social Security numbers, birth dates, addresses and driver's license numbers. They also stole credit card numbers of about 209.000 people and documents with personal identifying information of many others.

> By the time you read this article, there is a large probability that a major ransomware attack based on these vulnerabilities will have happened or is about to happen

A breach like this will obviously lead to repercussions for Equifax and already law suits and class action suits are being prepared. The breach itself, Equifax reported, was caused by a missing patch in Apache Struts (CVE-2017-9805). It is interesting to note that at the time of the breach, although a patch was available, the vulnerability had not yet been published nor was exploit code available publicly. Were this to happen in a post-GDPR Europe, the company would have a serious fine to pay to regulators. Interesting times indeed…..

Windows 0-days

Windows patches are rolled out in batches, each second (and sometimes fourth) Tuesday of the month as you probably know. The September patch batch was exceptionally interesting as it contained no less than 81 patches for vulnerabilities that have a CVE entry. This security update fixes 27 critical and 54 important vulnerabilities, of which 39 vulnerabilities could lead to Remote Code Execution. Remote Code Execution (or RCE) is what allows a criminal to take over a system remotely, without being authenticated.

Affected components include Internet Explorer, Edge, .NET Framework, Skype for Business, Exchange Server, Office, and of course Flash (i.e. all the usual suspects). Of these, four of the patched vulnerabilities are publicly known and have associated exploit code in the wild. The rest will no doubt follow soon.

The recent ransomware attacks WannaCry and (not)Petya have shown again that although patches are available, many customers fail to install them for a wide variety of reasons, leading to major disruptions of businesses (Maersk lost up to a quarter of a billion Euro due to Petya).

I'm certain attackers are reverse engineering the Microsoft patches as I write this article, to create exploit code for the remaining 35 vulnerabilities that are not yet publicly known. By the time you read this article, there is a large probability that a large ransomware attack based on these vulnerabilities will have happened or is about to happen. Interesting times indeed…..

Anniversary edition
Black Hat Sessions

While the program commission is currently making the initial preparations for next year's Black Hat Sessions, we would like to briefly report about the latest edition of 29 June 2017.

In this special fifteenth anniversary edition: It's all about the Data" we presented a number of national and international prominent speakers to cover part of this broad spectrum, ranging from privacy to crime, from business to in-depth high tech.

The ethics of privacy

Rachel Marbus, Privacy Officer at KPN, believes that we are hyper focused on data protection and as a result are losing the bigger picture. Instead we should look at the constitutional right to privacy versus our moral values. Rachel defined three ways towards ethical thinking: deontological, teleological and consequential. Next to that she presented a quadrant related towards decision making within privacy issues. It contains four assumptions based on whether a situation is legally allowed and/or morally OK. She finished her lecture by asking us to stop focusing at the details and zoom out. Are you doing the right thing and what are you actually protecting?

Losing yourself in a cloud of things

The "Internet of Things" is growing and we can't stop it. We've barely seen the tip of the iceberg when it comes to Internet-enabled devices which make us ask: "What is this ridiculous nonsense?" As the security-unconscious masses buy into the promise of personalised everything, everywhere, there are three important aspects that we need to consider. We need to think about identity management of every device (who are we sharing our data with?), control of the data flow (how do I control who is accessing my data?), and device ownership (who can configure it?). Michael, security consultant at Secura, presented future use-cases and drew parallels with existing technological solutions.

Plan to throw the first one away

In The Mythical Man-Month, Fred Brooks famously advised, "The management question, therefore, is not whether to build a pilot system and throw it away. You will do that. Hence, plan to throw one away; you will, anyhow." His advice sparked the evolution of rapid prototyping and agile development. However, companies still find themselves taking prototypes into production -- and having to re-engineer at great cost later, especially once security flaws rear their heads. In the project presented by Meredith Patterson they included planned prototyping and then reimplemented from scratch in functional languages according to language-theoretic security principles. This reduced technical debt and lead to more reliable software.

Physical pentesting

Besides being a professional digital pentester, Walter is also known as the fasted Dutch lockpicker. During his lecture Walter gave us a look inside the world physical pentesting. Instead of approaching data via IT as a hacker, he presented different ways to get physical access to a location where servers are stored. More looking at security from the mindset of a burglar, assuming the fact that

Keynote -Bill Cheswick (Ches) joined us from the U.S. to provide a keynote for this special edition

Keynote - Brigadier General Hans Folmer, Commandant General of the Dutch Armed Forces Cyber Command (DCC)

when somebody has access to a server your data is lost. Walter concluded that risk management should therefore consider all risks not just IT.

New sheriffs in town

As a police officer, John gave us insight on the way the Dutch police is working on a "no more ransomware" platform. In association with a broad range of partners they are investigating ransomware on a daily basis. Besides they have built over fifty tools in order to facilitate keys for locked computers. To launch the platform they confiscated ransomware servers and even controlled their domain. This made it possible to redirect infected computers to their platform. John concluded that it is time to get smart and work together. To act fast because it is a time sensitive problem.

A century of data stealing

25 years before the Edward Snowden revelations, in 1988, Scottish investigative journalist Duncan Campbell uncovered and reported the world's first mass surveillance system targeting international communications - covername ECHELON. In his talk Duncan gave a historical overview of data stealing in the previous century. Via examples he demonstrated how government agencies are often years or decades ahead of commercially known ways to conduct mass surveillance or steal data. It was hoped that technical solutions, especially cryptography, would contribute to ensure security and privacy. However, what is happening now is that encryption schemes are broken on a massive scale, such as the BULLRUN programme.

> "Thank you to everybody for this successful edition with more than 400 participants, inspiring talks, good conversations and a very positive atmosphere

The future is false positive

Hans de Zwart, Executive Director Bits of Freedom discussed three things in relation to false positives. He showed some worrying (and occasionally wryly funny) recent examples of false positives like a person with Parkinson's disease suspected of being a bus bomber. He identified some of the causes of this problem: fear as a motivator for policy making, our changing attitude towards risk and, most importantly, a drastic increase in the number of decisions made by machine learning algorithms. Finally, he explored a few of the practical strategies that we could implement in trying to decrease the number of false positives and minimise their damage. Secura had an extensive interview with Hans de Zwart. See page 4 of this SecurAware.

Hack for safety - TIBER & MGs RED teaming approach

TIBER (Threat Intelligence Based Ethical Red teaming) tests the cyber resilience of the Dutch core financial institutions against advanced attackers. Rogier Besemer, Program manager TIBER at the Nederlandsche Bank presented in this presentation the TIBER background, goal and the expected results. What makes a Red Teaming exercise truly worthwhile? Ralph Moonen, Technical Director at Secura, presented his point of view and share his experiences in recent projects. Due to the confidentiality of the information there is no presentation recording available.

Would you like to get more explanation and inspiration after reading the summaries, please go to www.blackhatsessions.com for the full presentation recordings (including the two keynotes). Hope to see you next year (again)! Keep an eye on our website to stay on top of the up-to-date information.

Secura

The digitalisation of our society is moving forward fast. This increased pace of digitalisation, combined with the rise of new technologies increases our digital security risks. Cybercrime is on the rise and cyber legislation is globally intensified. Identifying and mitigating digital security risks is therefore becoming progressively more complex.

Secura is your independent, specialised advisor taking care of all your digital security needs.

TAKE CONTROL OF YOUR DIGITAL SECURITY

Interested?

Would you like to learn more about our services? Please do not hesitate to contact us. We would be happy to become acquainted and to discuss digital security in more detail with you. **www.secura.com**