#05 OCTOBER 2019

PUBLISHED BY Secura

SecurAware

INSIGHT
Enhancing Security & Privacy of Medical Data

EVENT
Black Hat Sessions

REFERENCE CASE
Klaas van Houten, N.V. Nederlandse Gasunie

THE HACK
IoT Solar Inverters & Trickle-Down Vulnerabilities

RECENT HACKS
Huge VPN & Mailserver Vulnerabilities

NEWS HIGHLIGHTED
Launching Secura File Exchange

NEWS
Security Awareness: How to Change Behaviour?

INSIGHT
Taking a Closer Look at Pseudonymisation

ANTAL VAN KOLCK-LUIJT, SERVICE LINE MANAGER SECURITY ASSESSMENTS

Move Up, Shift Left and Go Beyond!

Dear reader,

In this issue we look back at a very successful Black Hat Sessions with the theme: Protecting your critical systems. Keynote speakers included Victor Gevers, the unsurpassed champion of Coordinated Vulnerability Disclosure, who inspired us to use our ethical hacking skills for a higher purpose. During the workshop ICS Hands-on-Hacking attendees could get their geek on by trying to hack a 'real' OT environment. Simultaneously, in the management track the Dutch Road and Transport Authority provided insight in their next steps for a certification scheme to ensure secure “IoT” cars on the road. A pilot in which Secura participated, I proudly add. These are just a few highlights, which together created an inspiring day. As Secura we already started to prepare the event for next year, where the theme will be around cloud. The term 'cloud' has become a description of many business models and technologies, and Secura closely follows the trends related to this.

We see a large integration between the traditional OT (operational technology) and IoT, partly driven by security. The need of organisations to assess their OT systems as well as production sites and plants is growing to balance availability and security. Read more about this in the interview with Klaas van Houten from the N.V. Nederlandse Gasunie in this SecurAware. Sensors integrate into more traditional environments to realise performance improvements and security/resilience by providing (near) real-time and valuable data. Especially when storing such data in the cloud, you have potential for a great, secure and efficient solution or possible catastrophe at your hands. This is a common trend for the whole industry: move up, to the cloud.

We also see a large trend called 'shift left'. Security is moving from a penetration test at the end to integration in the development process. In essence, security needs to be taken into account in the full development cycle (from left to right). From DevOps to DevSecOps by training developers in secure programming and integrating source code review tooling. SSDLC is on a path to become a house-hold term and for good reason. Bug remediations are most costly at the end of the cycle. The earlier in the process you can prevent or fix these corrections, the most cost-effective you are.

Hence maturity models like OWASP-SAMM (OWASP Software Assurance Maturity Model) are becoming increasingly popular. OWASP-SAMM supports you in performing a (self-)assessment of where you stand and provides you with a path and management tracker on how to improve. This open-source jewel is perfectly embedded with the ASVS (Application Security Verification Standard) and the OWASP testing guide. This has lead Secura to update our report format for security assessments to this standard, in order to clarify what our test coverage is, as well as what we do beyond this standard. Going beyond standards is where the unique value lies of a highly qualified and skilled ethical hacker.

Secura went above and beyond my own expectations. We have nearly doubled our team in two years, and serve hundreds of customers. While we aim to continue to deliver the best and newest services to you, we owe you a big thank you for inviting us to assess your security. Let's move up, shift left and go beyond together!

Antal van Kolck-Luijt
Service Line Manager Security Assessments

From BIG to BIO: Ready?

In 2020 the “Baseline Informatiebeveiliging Overheid (BIO)” will become effective. Are you ready? BIO compliance is not a tick in the box.

Speaking with our customers in the public sector, we see organisations struggling with addressing security in an integrated way. Focus is on BIO compliance, while organisations don't know their current state and what to do. Therefore Secura developed a BIO readiness check in order to assess the organisation's state according to BIO (and ISO27k) addressing all aspects of Organisation, People, Process and Technology. By using a more integrated method, you will get a clear maturity scoring and clear overview on what topics requires specific attention.

Call us to organise an initial conversation or workshop to gain insight into your BIO readiness, what requires attention and how to implement the BIO requirements. Would you like to read more explanation and details about the BIO, please download the full white paper on our website: https://www.secura.com/whitepapers

European Cyber Security Month (ECSM)
October 2019

https://cybersecuritymonth.eu

ECSM is the EU's annual awareness campaign that takes place each October across Europe. The aim is to raise awareness of cyber security threats, promote cyber security among citizens and organisations; and provide resources to protect themselves online, through education and sharing of good practices.

SecurAcademy Open Class Training Courses
October & November 2019

https://www.secura.com/securacademy

- 31 October & 1 November 2019: **Internal Pentest Training**
- 19 November 2019: **Hands-on Hacking**

Security of Healthcare Data Awareness Workshop
January 2020

https://www.secura.com/asclepios-awareness-workshop

This workshop, themed “Protecting vital assets, the art and science of working with medical data” will focus on the current limitations concerning the collection, storage and access to the sensitive patient's medical data and how ASCLEPIOS attempts to solve these (read about the project in this SecurAware). Register your interest on the website. Admission is free of charge.

Secura Backdoor Detector: The Rogue Asset Detection Tool

Data protection involves securing the network to ensure sensitive data remains inside of the network. To prevent data exfiltration, it is important to ensure the secure network does not contain any 'backdoors'. For that reason, it is important to regularly scan the network for unexpected connections!

Secura Backdoor Detector is a toolset that can continuously scan a network and detect connections towards another network (e.g. the internet). Main features are:

- Detect unintended (or malicious) backdoors
- Double check firewall settings
- Double check network segmentation
- One time check or continuous scanning
- Notification in case of an unexpected connection

Visit our website for more information. Secura developed a series of comprehensive tools, which may be of your interest too. See also the article about the new Secura File Exchange platform in this SecurAware.

COLOFON

Contributors
Daniël Dragičević
Floris Duvekot
Christiaan Hillen
Klaas van Houten
Robert Meppelink
Ralph Moonen
Maayke van Remmen
Razvan Venter
Jos Wetzels

Art director
Jacqueline Bayot/
Studio Novi

Contact
editorial@secura.com

Secura B.V.
Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)88 888 31 00
E info@secura.com
W secura.com

Follow us on

Razvan Venter

Enhancing the Security and Privacy of Medical Data

Beginning of 2019 Secura officially launched its contribution within the ASCLEPIOS project. ASCLEPIOS (Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare) aims to provide a novel platform for the secure and privacy enabled transfer and processing of sensitive healthcare data.

Healthcare Data Security Threats and Practical Limitations

The issues and limitations concerning the transfer, storage and usage of healthcare specific information have been of high interest for many years. Together with the continuous and high paced advances in the domain of cyber threats, the cybersecurity of this healthcare information becomes a clear point of concern. The issues are coming from multiple perspectives, which can equally lead to a compromise of highly sensitive, personal data. In the hand of malicious hackers, this data could subsequently become subject to ransomware scenarios, or even life endangering attacks.

Social Engineering

First of all, the healthcare domain is one of the most vulnerable to social engineering attacks. When it comes to personal health, patients are generally more than willing to share their sensitive information, in order to treat their medical issues. A simple phone call to a patient, while claiming to be a legitimate doctor for example, has a high chance of successfully extracting information which would otherwise be kept safely by the patients. At the same time, similar types of social engineering attacks could also target hospitals or clinics. By acting as a legitimate employee, easy access to internal databases of data can be granted. More details about these types of real-life social engineering scenarios can be found in a separate article on our website: https://www.secura.com/blog-social-engineering-in-a-healthcare-context

ASCLEPIOS

The ASCLEPIOS project is part of the European Union's Horizon 2020 program, funded under grant agreement No. 826093, and will span over 3 years, with the end in December 2021. ASCLEPIOS puts together 11 partners from the domains of healthcare, research, industry and services, all having the goal of developing a novel, privacy and security enhanced solution for medical data processing.

Legacy Technical Solutions

At the same time, the technical solutions which are deployed for collection, storing or transferring highly sensitive medical data are, in many of the cases, outdated. Cybersecurity in the medical devices and systems domain is a relatively new focus area, and important medical devices regulatory bodies (such as the FDA or the EU) are only now beginning to keep a close eye on the state of the art concerning existing security features. Considering this, many of the medical devices, systems, or transfer/storage platforms deployed in hospitals or wore by patients have technical limitations in terms of their security. Practical attacks on implanted medical devices have been demonstrated[1][2], attacks on hospitals' secure networks are common and the security of the data stored in the cloud relies solely on the measures implemented by the Cloud Service Provider (CSP) – which often has at most a self-declaration of security.

Where Security Succeeds, Trust Becomes an Issue

Finally, imagine the situation in which no external security incidents can come by attacking the medical devices, systems or cloud platforms. Would that mean the perfect world in which the data is fully protected? Unfortunately, no, since the cloud-stored data is encrypted with a key fully in the control of the CSP. Therefore, the CSP can at any moment decrypt and access the stored data, without leaving any trace which the patient or doctors could detect. Trust in the CSP becomes an issue, especially in the light of the many abuses against information privacy laws and regulations.[3]

Towards a Novel Solution in the Security and Privacy of Medical Data

The threats and practical limitations exposed above represented the incentives at the base of the ASCLEPIOS project. Under this project, the intention is to develop a platform based on which medical data can be securely collected from patients and stored in the cloud. To eliminate the issue of trust in the CSP, the keys used to encrypt the stored data will not be in the control of the provider, but will be generated by the patient him/herself. The patient will then upload to the cloud encrypted information, while the encryption key will be stored, in encrypted form, in a different trusted location. The encryption of the medical data in the cloud will follow the principles of Secure Searchable Encryption (SSE), thus allowing for the search in the encrypted data, without the need to decrypt it first.

In order to retrieve the encrypted medical data (by doctors or other legitimate users), the decryption key can be requested from the trusted location. Here use will be made of another novel concept, Attribute Based Encryption (ABE). Using ABE, the owner of the medical data will be empowered to decide who can access the encryption key, by defining a set of matching attributed. Examples of such attributes could be location, medical department, purpose of use, or the name of a specific doctor.

Finally, it is recognised that the research on medical data is a crucial element when it comes to the development of new treatments and solutions. Using the ASCLEPIOS platform, doctors which are allowed to get access to patients' data can make this data (in the encrypted form) available to external third parties, for research purposes. Operation on encrypted data are possible through the use of Functional Encryption. The diagram below provides a visual representation of the ASCLEPIOS concepts and involved stakeholders.

The Role of Secura

Secura will be, throughout the duration of the project, one of the main partners. Secura's expertise, covering domains such as security, privacy and awareness will enable a unique position within the project, both supporting the development of the platform, as well as actively disseminating the results and raising awareness on the topics.

From a technical point of view, Secura's experts will help in the development, design review, testing and finally validation of the proposed platform. At the same time, the GDPR compliance elements will be mainly supported by our involved project members. Finally, but equally important, Secura will actively hold security and privacy workshops, presenting the progress of the ASCLEPIOS developments, as well as raising awareness towards the criticality of securing medical data.

Next Steps

The project is getting close to the end of its first year, with the first set of deliverables already being published. The progress of the project can be followed on https://www.asclepios-project.eu/. In terms of results dissemination and general awareness, Secura fixed the date of the first thematic workshop on the **16th of January 2020, at our office location in Eindhoven**. Registrations to this workshop can now be made at https://www.secura.com/asclepios-awareness-workshop. The series of workshops will continue throughout the whole project's duration, with a target of two workshops per year.

1. https://www.csoonline.com/article/3222068/465000-abbott-pacemakers-vulnerable-to-hacking-need-a-firmware-fix.html
2. https://www.govtech.com/security/FDA-Warns-of-Insulin-Pump-Cybersecurity-Vulnerabilities.html
3. https://venturebeat.com/2019/07/23/5-data-privacy-startups-cashing-in-on-gdpr/

Christiaan Hillen

The Search for Additional Information:

Taking a Closer Look at Pseudonymisation

> According to the GDPR, pseudonymisation means 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information' (art. 4.2).

Through the definition of personal data (art. 4.1), we can learn what anonymous data is as well: any information not relating to an identified or identifiable natural person. That is, if we have data, but can no longer attribute it to a data subject, even with the use of additional information.

The distinction here is quite clear but subtle. It's about additional information. In the simplest form it means that data has been stripped of identifying marks, and a single identifying element is added. This can be used to refer to a separate lookup table wherein that row of the table will provide the personal data that belongs to the pseudonymous entry.

Likely Reasonable

Both pseudonymity and anonymity rely on what means are 'likely reasonable' to be used in order to re-identify an entry. Given enough data, no entry will ever be anonymous, and this is something that should be considered when working with large amounts of data.

As the Article 29 working party stated: 'Pseudonymisation is not a method of anonymisation. It merely reduces the linkability of a dataset with the original identity of a data subject.' Anonymisation on the other hand is the application of methods to 'achieve irreversible de-identification'. In simpler terms: we want to be able to reverse what we did, versus we do not want to be able to go back.

So how likely is it that a dataset that was deemed properly pseudonymised, or even anonymised, is inadvertently re-identified? It turns out going back was still possible, even though you thought it was impossible. If identification is possible, anything you did with the data set was performed on personal data, even though you thought it was anonymous at the time. This means that all restrictions and obligations are in effect, such as the need for a DPIA, legal grounds for processing, and a notification to the data subjects if the data is processed illegitimately (such as with a 'data leak'). Pseudonymising data therefore should not be taken lightly.

What Is Identification

At its core identification is the possibility to single out an element from a group. This does not mean that the element is known by name or by social security number, just that the combination of attributes of this element result in a unique combination.

Often times when discussing with customers about a certain design, this issue is encountered. The obvious name and address are removed from a dataset, or something from a small input space is hashed to use as identifier, but singling out is still possible. This is in seeming contradiction to what we normally see as identification, which has to do with the information that is on our government-issued ID. No name equals no identity, right?

One possible and well-known mitigation in data sets is to use 'k-anonymity', wherein attribute values are generalised to the extent that each individual shares the same value. This is done in such a way that for each entity known to be in the database, there are k-1 other entries in the database that are indistinguishable from this entity, given a certain set of attributes.

Although this works in theory care must be taken to have a large value of k, as a 50/50 chance of being the right entry is not secure enough. Also in some cases even just being in the database somewhere, without actually knowing which entry a data subject is, can already be too much information. Think medical data sets or data sets on far-right/-left political views.

There are many more ways of pseudonymising data, and each solution needs to be tailored to the situation.

Combining Information

In pseudonymisation, as already described, a lookup table of sorts exists that allows re-identification of data, where this table is technically and organisationally protected. The question that then comes to mind, is whether such a table can be created from external means. What if a party with highly advanced profiles on its users, such as a personalised search engine, or any of the social media or communications platform, colluded with an attacker to re-identify the data set? These parties typically know what their users are interested in, what they are reading online, what they are searching for, what they buy.

One has yet to meet the first patient in this day and age, who has not done at least some basic online searches concerning his or her ailments and has kept a complete social media silence about this. Even just visiting a hospital whilst using a smartphone generates information about being at that hospital at a certain time. Now if the pseudonymised data on the patient population contains dates on which patients were at the hospital for their check-up, such data can be compared to what is known about the location of the smartphone. Just four spatiotemporal data points are needed to identify 95% of individuals.

In our everyday lives we leave a very large digital trail with everything we do. If a (malicious) party can get hold of this and compares that data to an anonymised data set, this data may turn out to be readily identifiable for that party.

Likely Reasonable, Continued

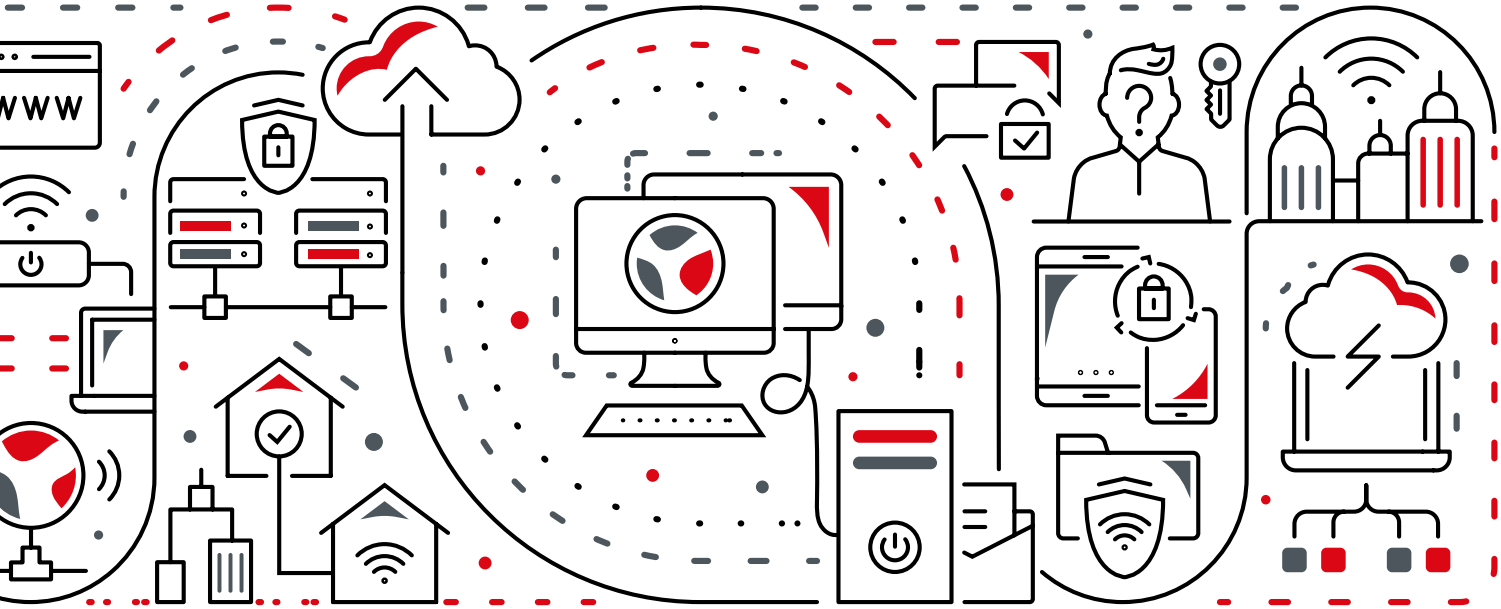
We trust parties with our data. Some parties we trust with just about every piece of data we have because we do not wat to miss out on social interactions and likes. Attackers typically do not have all this data at their disposal, so performing re-identification is difficult for them.

This is what pseudonymity is about, how much effort does it take the expected attacker to re-identify entries in the data. As absolute anonymity is not possible with any degree of realistic data, we resort to what is likely reasonable. Although attackers do have a lot of time on their hands, if they have to scrape the social media and gather terabytes of information to re-identify your pseudonymised table however, that may be considered an unreasonable amount of effort.

On the Side of Caution

Re-identification is a balancing act between usefulness to the users and effort for the attackers. The differences between personal data, pseudonymised data, and anonymised data are subtle. Err on the side of caution, ask yourself the difficult questions, and in case of doubt consult the experts.

Ralph Moonen



VPN and Mailserver Vulnerabilities Are Huge Cybersecurity Risks

It is not often that new critical vulnerabilities are exposed in widely used internet services such as email servers or VPN servers. In our daily work, we use these types of services as we do a highway or car. It gets us from A to B without much trouble or hassle and yes, accidents happen but rarely does a complete highway fail, or do all cars from a particular manufacturer crash simultaneously. Yet this is what has happened in the past few weeks, when vulnerabilities in the PulseVPN and Exim mail server were disclosed that are so critical, attackers are able to take over the system completely. There was no need to already know a username or password, and the attacks are not always easy to detect and certainly not easy to prevent (other than patching).

CVE-2019-11510: Door Wide Open to Corporate Networks

Let's take a closer look at the risks from the PulseVPN vulnerability, also known as CVE-2019-11510. This vulnerability allows an attacker to simply request a file from the VPN server (that runs on a Linux operating system). Such a file could be, for instance, the password file from the OS. Fortunately, the web server process has no access rights to the actual OS passwords because they are stored in a file called /etc/shadow which is protected. However, the web server process on the appliance is also used to manage VPN users and passwords. For those users, it must have some access rights. As it turns out, it is indeed possible to download the database of VPN users. Worse: their passwords are stored in plaintext. And even worse: the sessions of logged in users can be hijacked because the session identifiers are also in a readable database.

This vulnerability therefore means that an attacker can hop on the VPN service, masquerading as a legitimate user (by either using their password, or their sessions identifier). Once on the VPN, the attacker can do what a normal VPN user could do: access the corporate email server, CRM server, SAP system, Oracle system, file shares, Sharepoint servers, whatever normal corporate users do. Obviously, there might by additional access controls in place, such as an extra username and password for Windows authentication or Single Sign On (SSO), but in our experience, VPN users often have pretty much the same view of the network as an internal user, who is physically on the network at the corporate premises. For an attacker, this is a big advantage because they no longer need to breach firewalls, implant malware, APT's or place rogue devices. They can immediately start penetrating into the internal network.

So we have established that this vulnerability sets the door wide open to corporate networks. Therefore our security specialist Matthijs Koot decided to investigate how many Dutch organisations were vulnerable to this attack, despite the patch being available already for many months. During the first scan, well over 500 Dutch organisations were vulnerable. We were astounded by the names on the list: banks, government, aerospace, defense contractors, oil and gas, publishers, entertainment, ISP's, and even a few security companies! We immediately contacted the Dutch NCSC and provided them with the list.

More background information on this can be found on https://www.secura.com/news-kwetsbare-pulse-connect-secure-ssl-vpns-in-nederlandse-ip-adresruimte

But even now, many organisations have not yet patched their systems. Mistakenly, many organisations think that their problems are completely solved when they are patched. However, this vulnerability has been exploited in the wild for several weeks before it gained attention. In that time, it is very likely that **every single vulnerable server in the world** was attacked and exploited. Yes, that means that over one hundred thousand servers were compromised. Why are we so certain about this? Well, if we could run a script in a few days to check all Dutch servers, you must assume that a nation state actor such as China, Russia, the UK or the US, were way ahead of us. These countries have dedicated programs for scanning the whole internet for such vulnerabilities. It is therefore a safe bet to assume that not one, but several countries' cyber intelligence units have already compromised these servers and harvested usernames and passwords. And in some cases it would be obvious for them to compromise the target's internal network through the VPN access while they're at it.

Another consequence is a little more subtle, but the effect can also be huge. Many of the VPN servers use wildcard certificates for their SSL/TLS connections. This means that the certificate can be used on any host in the domain: *.victim.com would therefore include www.victim.com, mail.vicitim.com etc. A large subset of the VPN servers do not come equipped with a so-called 'secure element' on which the private SSL/TLS keys are stored. This 'secure element' usually takes the form of a dedicated chip that is used to store keys in a way that they cannot be extracted from it (like a smartcard). Instead they reside on the file system, as files, similar to the usernames and passwords. This file is usually protected so that only privileged accounts can read it.

CVE-2019-11539: Attackers Can Chain Two Vulnerabilities

However, there is another vulnerability, called CVE-2019-11539, whereby an authenticated administrator can execute commands on the operating system after logging in. Attackers can chain these two vulnerabilities now: first extract the administrator password with the first file read vulnerability, and then log in and abuse the second vulnerability. The attacker can then gain remote code execution and ultimately get at the SSL/TLS keys. This means that you should consider the certificate also compromised on all these VPN servers. In short, it is therefore not sufficient just to patch. If you are running a PulseVPN server, you should:

1. Patch
2. Audit all logs for exploiting of the arbitrary file read vulnerability
3. Audit all logs for in-session changes in IP addresses (indicating hijacked sessions)
4. Revoke the certificate of the VPN server and generate a new one
5. Disable all VPN user accounts until passwords have been changed
6. Inform all users that those passwords have been compromised, so that they can change all instances they used that password

Exim Mail Server Software Need Urgent Patching!

Just recently, a vulnerability with a similar impact was disclosed for Exim mail server software. The exploit for this has not yet been published but enough details are known to make it entirely possible for a nation state actor to create an exploit in one or two weeks. Again, this vulnerability will be widespread, and impact many high-profile companies and organisations. If you have not yet patched, you should do so immediately, and you should also consider the email server compromised (and therefore also all mail handled by it). Any SSL/TLS certificates for those vulnerable Exim servers should also be revoked. We will probably never find out, but my guess is that these vulnerabilities will continue to have consequences for many years to come.

Maayke van Remmen & Daniël Dragičević

The greatest challenge for our IT Security is the ***balance between availability and security*** of the gas transmission network

Interview with Klaas van Houten, Operational Security Lead & ICT Security Architect at N.V. Nederlandse Gasunie.

The N.V. Nederlandse Gasunie (Gasunie) ensures that gas transport throughout the entire Dutch national transport network happens safely, uninterrupted, affordable and is as sustainable as possible. So that everyone has access to gas anytime, anywhere.

What is the prime task of Gasunie?

Gasunie is the owner and maintainer of the national infrastructure for large-scale transport and storage of gas in the Netherlands and northern Germany. At the moment, mainly natural gas is being transported and green gas. With the energy transition, this will increasingly move to sustainable gas such as hydrogen. In addition, we participate in the construction and management of networks for heating and CO2.

You are Operational Security Lead at Gasunie. What does this job require?

I deal with daily security issues, such as handling security incidents, answering IT security questions, supervising security investigations and handling change requests. I also fulfill the role of IT Security Architect at Gasunie. This involves reviewing designs and advising various delivery managers on innovation, translating functional wishes into possible solutions and drawing up an annual roadmap.

How is information security structured within the organisation?

The IT Security Manager designs the IT security policy and the security measures. The Operational Security team is responsible for day-to-day affairs, handles IT Security incidents, assesses changes and advises the organisation. Ultimately, the team managers of the various support groups are responsible for applying the correct IT security measures to guarantee confidentiality, integrity and availability as agreed. Within the different support groups, a number of employees focus on IT security. These employees act as the point of contact for the support group and the Operational Security team.

Which standards and frameworks apply to the energy sector?

There are many standard frameworks for the sector. For IT security Management we have been using an ISO27001 certified ISMS (Information Security Management System) for the past 5 years. In addition, our measures are largely based on the ISO27002 standard. For projects we use a 'secure scorecard' based on our measures, that prescribes which security measures must be taken depending on the CIA rating.

How does Gasunie cooperate with other organisations in the energy sector to bring IT security to a higher level?

Gasunie cooperates with various other companies within and outside the energy sector. For example, we contribute to the Energy-ISAC (Information Sharing and Analysis Center), an initiative of the NCSC (National Cyber Security Center), part of the Ministry of Security and Justice. We also contribute to sector-specific working groups.

What added value do you see in these partnerships?

Especially being able to hold consultations with other parties in the same sector is of great added value for us. This applies at the moment of acute situations in which action must be taken swiftly and correctly, but also for questions concerning the security aspects of design and implementation. It is interesting and educational to see how other companies deal with the same issues and to see how we can learn from each other. In addition, warning each other of threats has a reinforcing effect on security.

What are the biggest challenges for Gasunie concerning digital security? And what do you do to keep the risks under control?

The largest challenge is balancing IT security on the one hand and the availability of the gas transmission network on the other. This is especially true for security patching, which is implemented by us through a standard process. However, a critical patch is not concerned with a standard process. To keep this under control, we regularly perform risk analyses. Based on this analysis, together with the various support groups we determine per environment what needs to be done to mitigate the risk to an acceptable level.

Furthermore, we – just like many others – have to deal with the digital transformation. The challenge here is to get and keep all employees aware about information security. Clicking on a link or scanning a QR code is done in no time and this can have major consequences in our sector. We keep our people informed and aware through an awareness program that requires compulsory security training. Part of that entails conducting phishing campaigns and we provide hacking demos to demonstrate how simple it is to become a victim of digital attacks, and we show how you can protect yourself against these.

I am happy and proud to see that IT security receives a lot of attention within the support groups. This helps especially in situations that deserve attention, to act well and adequately.

What are your experiences with Secura?

Since the cooperation that started about a year and a half ago, Secura has carried out various projects for Gasunie. The open attitude, willingness to include those involved in what they are researching and the professional and independent advice ensure a pleasant cooperation. “There is a great deal of flexibility and I am glad that people think about how projects can be executed according to our best interests”.

THE N.V. NEDERLANDSE GASUNIE AND SECURA

Secura supports Gasunie in conducting security investigations in both the IT and OT landscape and assists with the implementation of the internal ISO audit.

Gasunie recently had one of the projects carried out by means of an attack tree session (Threat Modeling). Different groups were brought together in order to find out what the greatest threat currently is. From that point of view, Secura experts considered together with Gasunie what is necessary to actually handle this threat. The insights from this session provide an excellent overview of the chain and the weakest links in the process.

© Gasunie

Maayke van Remmen

Black Hat Sessions 2019: Thank You!

Proudly we look back at the seventeenth edition of Secura's annual security conference the Black Hat Sessions "Protecting your Critical Systems" in June 2019. Over 300 participants came together to network and to be informed about security issues in critical sectors. Thank you to everyone who participated and contributed to this beautiful edition!

Between the keynotes by Victor Gevers (Founder of GDI Foundation and Chairman of Global CERT), Jos Wetzels (Principal Security Consultant at Secura) and Elsine van Os (Clinical Psychologist and Intelligence and Security Expert), we offered a large number of lectures given by promiment Dutch and international speakers in multiple technical and non-technical track. Ali Abbasi (Ruhr University), Jeroen van der Ham (NCSC - University of Twente - EEMCS/DACS), Robin Massink (Alliander) and Marina Krotofil (BASF) presented their in-depth technical approach and current researches and innovative solutions to the unsolved problems facing the industry. During the managerial track of the Black Hat Sessions our speakers Geert Pater (RDW), Max Geerling (Dutch Payments Association), Ben Kokx (Phillips), Anderson Domingues (LyondellBasell), Paul Wijninga (Agentschap Telecom), Wouter Wissink (Chubb) and Liesbeth Holterman (Cyberveilig Nederland) addressed how they deal with security and how to increase cyber resilience within their business.

For the most important lessons learned, new insights and a comprehensive report of the sessions, please visit secura.com/recap-blackhatsessions-2019

BHS

Growing awareness of blended threats is crucial - behavioural, physical and technical; thinking broader

Elsine van Os - CEO and founder of Signpost Six

The pros don't bother with vulnerabilities; they use features to compromise the ICS: Insecure by design, legacy and lifespan, porous boundaries and visibility and control

Jos Wetzels, Principal Security Consultant at Secura

Cars with current technology of today's age are capable of learning while driving. This means that the complete lifecycle of such cars have to be monitored on the basis of safety and security

Geert Pater, Manager Vehicle Standards Development at RDW

SAVE THE DATE: 11 JUNE 2020

Black Hat Sessions 2020: Cloud Security

On June 11th 2020 we will celebrate the 18th edition of Black Hat Sessions. On request of many participants of Black Hat Sessions 2019 and previous editions, the theme of next year's edition will be around the theme “Cloud Security”. With practically every business running on some kind of a cloud network and database, securing the cloud has never been more important. Secura follows the trends related to this important topic with big interest. The coming months, we will prepare an high quality speaker programme with technical and non-technical sessions, as well as interactive workshops, demos and fun things to do.

The BHS is aimed at a broad audience: decision makers, managers, CISOs and technical security experts. We look forward to see you there. Save the date and keep an eye out for up-to-date information at www.blackhatsessions.com

Jos Wetzels & Ralph Moonen

IoT Solar Inverters & Trickle-Down Vulnerabilities

Nowadays almost all solar inverters have an internet connection via Wi-Fi or cable. The main benefit of this connection is that the user can monitor the device from anywhere. The downside is that the inverter becomes a target for attackers. In this article, Jos Wetzels describes insecure Wi-Fi modules in Solar inverters and how these vulnerabilities end up in very different products with very different, and potentially dangerous, impacts.

This story started when we were alerted to a lot of open wireless access points (AP), all with similar SSIDs starting with a prefix string of 'AP_'. After connecting to an open AP, it turned out to belong to the Wi-Fi kit of an Omnik solar inverter and allowed anyone connected to it to log in (using default credentials). It also allowed any other networks the kit was hooked up to, to be accessed. Omnik is a Chinese-German manufacturer of photovoltaic (PV) inverters and accessories popular in the Netherlands, Germany and Belgium.

After connecting to the AP it is possible to go to the exposed web interface, called "IGEN-WIFI". Further research showed that the connectivity kits were in fact not manufactured by Omnik but instead by a company called SolarMAN/iGEN which sells their kits to other vendors such as Omnik, Hosola, Ginlong, Kstar, Power-One and others. That's interesting because it means whatever vulnerabilities we discover apply to multiple different vendors.

What Can an Attacker Do?

So what can an attacker do with access to the WiFi access point here? Well, first of all it allows us to interact with the PV inverters via various interfaces. Secondly the Wi-Fi kit needs to be able to connect to the internet in order to communicate with the SolarMAN cloud backend which ingests the inverter data and makes it available to users via a mobile app. As such the kit is connected to an internal network either via Ethernet cable or a Wi-Fi AP which means that the kit's own AP now acts as a point of entry into your private network(!).

Hi-Flying

The kits actually use a WiFi-module manufactured by Hi-Flying. The module exposes various services, including the module's AT interface, that provides access to sensitive functionality such as:

- Upgrading firmware
- Getting/Setting Wi-Fi configuration data (including keys)
- Getting/Setting service (eg. web server) credentials
- Getting/Setting 'user' configuration (device-specific info)
- Setting GPIO pin status
- Navigating to URLs in a proxy-like fashion

The only protection for this service is a 'password' which doubles as the network discovery string. The password is hardcoded in the firmware and cannot be changed and since it is part of the discovery protocol it cannot be considered confidential. By default this password is 'HF-A11ASSISTHREAD'. This same connection string is used in many other products also, including smart lightbulbs and LED-strips.

As it turns out, the issues with this interface have been independently discovered by multiple parties looking at different IoT products over the past few years such as WiFi Lightbulbs and LED controllers.

About Those Inverters

Using the AT command interface, an attacker can download a new firmware image to the connected inverters over the serial connection. And given that there's no firmware authentication mechanism on the inverter we can make arbitrary modifications, ranging from bricking them to more sophisticated actions.

Affecting Electrical Grid Stability

Solar inverters exist to convert the variable direct current (DC) output of photovoltaic systems into a utility frequency alternating current (AC) that can be fed into a commercial electrical grid or a local 'off-grid' electrical network. The power thus generated can be either fed directly into the utility grid, or can be used to supply households with power.

A balance between power supply and demand is crucial to the proper functioning of the grid in order to prevent instability. An attacker with sufficient control over an inverter's functionality (such as by means of downloading modified firmware) could manipulate it to potentially affect grid stability. An attacker could seek to manipulate inverter power output (and potentially affect the battery management system) or to cause a drop in overall supply.

Of course the complexity of such attacks is not to be underestimated. In addition to the defensive presence of grid protection systems and operator intervention, such an attack would require scale and coordination. Regardless, even in the absence of real-world demonstrations of feasibility on representative testbeds, the hardening of connected systems underpinning various Distributed Energy Resources (DER) such as solar, wind, biomass and small hydro is of crucial importance to overall grid hardening efforts.

Affecting Inverter Safety

Another potentially malicious scenario would involve an attacker modifying the inverter firmware in order to adversely impact safety, such as by causing a fire. Whether it is possible or not to reliably cause an inverter fire purely through software means remains to be demonstrated and as such caution is required in judging the realism of this scenario, but given the typical degree of inverter firmware control over internal fans, voltage adjustment temperature monitors, etc. a scenario like that is not outside the realm of possibilities.

Conclusion

While the potential impact of the discussed vulnerabilities on connected solar inverters and serial converters is worrying, they are not the real issue in this story. It is (or ought to be) common knowledge that most connected embedded systems (whether consumer or industrial IoT) are typically woefully insecure.

In my opinion the most troubling aspect here is the illustration of the detrimental effects of supply chain opacity on vulnerability management. The complicated supply chains in connected embedded systems involve many players across many tiers supplying and integrating different hardware and software components. This leads to the same product ending up with multiple different OEMs who do minimal customisation before passing it on to another layer of resellers who basically slap a new logo on it. A vulnerability in any component at any level can 'trickle down' an increasingly opaque supply chain to end up in ICS equipment, a POS terminal or internet-connected dolls alike, and the further up the supply chain vulnerabilities originate, the wider the range of products they tend to end up in and the harder it is to track and mitigate them without active collaboration of all parties involved.

In summary, what's needed is a more holistic approach to IoT security covering all relevant aspects of the product lifecycle and ensuring the products meet a common minimum baseline.

Note: Secura and the Dutch NCSC notified affected vendors of the vulnerabilities on various occasions and also notified China-CERT. No response from any vendor was received. [This article is an excerpt of a full-length article at https://www.secura.com/blog-iot-solar-inverter-and-trickle-down-vulnerabilities that includes all technical information and links to sources.]

Robert Meppelink

Launching Secura File Exchange

Sending or receiving large or sensitive files over the internet is a task many of us struggle with on a daily basis in our operations. Often, users resort to the tools that they know, such as e-mail, WeTransfer, Dropbox or OneDrive. In corporate environments, Managed File Transfer (MFT) solutions are often used. However, these tools are not all suitable for sensitive information or for communication with external users or customers. Many lack basic and advanced security features.

This is why Secura has developed a secure and easy way to transfer files between users on the internet, suitable for high-secure applications and when dealing with personal data that falls under the GDPR or other privacy regulations. In this article we analyse the problem, look at the weaknesses of existing solutions and present the case for Secura File Exchange (SFE).

The Problem

We are all accustomed to sending e-mail attachments. However e-mail is not a suitable medium for many types of data such as large files, personal data, sensitive financial information or company confidential information. There are several main reasons for this, the most obvious being that e-mail can only transfer files as attachments to a certain limit (usually around 12MB). Sending or requesting a PDF scan of a document from a customer or relation can already easily surpass this limit.

A further technical reason for e-mail not being a suitable is the fact that even in 2019, it is not guaranteed that an e-mail is sent securely over the internet with encrypted transport. While websites can easily be identified as using encrypted transport (the URL starts with HTTPS:// and therefore uses TLS security), this is not the case with e-mail. There is no way for a user to know or check how the e-mail is transported, and since regulations such as the GDPR and local regulations like the Dutch AVG require protection when sending personal information, you should not be using e-mail for any personal information. Does your HR department still send out salary statements or contracts by e-mail, or ask for copies of passports or other ID-cards by e-mail? If so, this is a violation of the regulations and could potentially lead to fines.

Exacerbating this problem, is the fact that any time you send an attachment by e-mail, you are effectively creating multiple (maybe five, six or more) copies of that attachment, all of which are no longer under your control (the sender), or the recipient, increasing the risk of leaking information. There will potentially be a copy of this data in:

- Your outbox
- The sending mail server
- The receiving mail server
- The E-discovery archive (if present)
- The inbox of the recipient
- All the backups of the above mentioned systems

Furthermore, there is the ease with which mistakes can be made when addressing e-mails. A very large number of data leaks are caused by simple typos in e-mail addresses[1], made worse by e-mail clients that provide type-ahead functionality (e.g. start typing "John…' and the e-mail client will automatically fill that up to the most used e-mail address starting with "John).

Add to all this the fact that e-mail is weakly authenticated (both for access controls to the mailboxes, as well as for the actual content of the e-mail) and it can be concluded that e-mail is simply no longer fit (if it ever was) for the professional communication of files between businesses and consumers, and between businesses and other business partners.

File Sharing Platforms

These limitations and risks have led to the growth of a large number of solutions for sharing (large) files, but most solutions are lacking in other ways and are focused on consumer-to-consumer type transfers and not on professional use. Users are keen to resort to solutions they know from personal use, because they are easy, such as WeTransfer or Google Drive™. Alas, in the free and personal versions of these services, there are no confidentiality guarantees whatsoever, and in fact Google states in their use policy that Google is allowed to use any data shared through Google Drive[2].

WeTransfer and many others do not offer authentication options beyond a simple password. None offer audit trails and logging capabilities. Further, since passwords are often weak, re-used and transported over insecure channels themselves, such file sharing platforms and cloud drives are also not fit for professional communication of files.

Professional MFT Solutions

There are quite a few solutions for the problems as described above. MFT products, such as Accellion, Axway and MOVEit neatly fill the most common requirements and sometimes offer advanced features such as integrity checks, Google Authenticator or even virtual keyboards to prevent keyloggers from seeing passwords being typed into the application. Other MFT environments are based on integration with existing environments such as TIBCO or Oracle, or are network share or folder based solutions for internal Windows domains.

However, most MFT solutions fail badly when it comes to overall security posture. Security starts with secure sign-up and enrolment. Therefore sending e-mails with plaintext login credentials (even if it is only once at the start of enrolment) completely breaks the security chain of multi-factor authentication. In addition, requiring a minimum password length of eight characters is insufficient for the present day where passwords hßashes of eight and even nine or more characters can be brute-forced or cracked. Also, the MD5 hash algorithm used for integrity checks has been fully broken for over a decade, yet is still used in some major MFT platforms, where it is described as 'secure'.

	E-mail	File Sharing platforms	MFT solutions
Large files	✗	✓	✓
Confidentiality	✗	✗	✓
Control data storage	✗	✗	✓ / ✗
Overall security posture	✗	✗	✗
Ease of use	✓	✓	✓ / ✗

Secura's MFT Solution

Secura performs several hundreds of application security tests every year. During these tests we get the opportunity to hack applications and systems, and give our customers advice on how to improve the security of the systems. It is therefore no surprise that Secura knows how to build a high quality, secure application. We know very well that all security measures are a trade-off with usability, and that compromises sometimes must be made to ensure that the security is not circumvented by users who feel burdened by these measures.

This is why we designed Secura File Exchange (SFE). SFE is the only MFT solution in the world built by a specialist security company, with security as the central pillar of development. We have built this product from scratch, and integrated many state-of-the-art security features including secure enrolment, secure hashing algorithms (SHA256), audit trails and many options for multi-factor authentication. SFE supports SMS text messages, Yubikeys and TOTP as second factors and will integrate many more in the very near future. But above all, we have made it very simple to use, both by recipients and senders of files, and admins. We also understand that there might be reasons that you need to keep the files in your own possession and not uploaded to someone else's cloud. This is why we offer our MFT solution in multiple deployment models: on premise and as a hosted dedicated service.

More information relating to SFE is available through the Secura website: https://www.secura.com/sfe

1. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2018
2. Google Drive Terms of Service, effective date: January 22, 2019

Floris Duvekot

Security Awareness:
How to Change Behaviour?
The Methodology of SAFE

In the previous edition of the SecurAware, WDO Delta elaborated about their first experience with Secura's new Security Awareness program called 'SAFE'. SAFE stands for Security Awareness For Everyone (SAFE) and aims to increase the level of security awareness within organisations. SAFE has been developed to help our clients with an integrated Security Awareness Program.

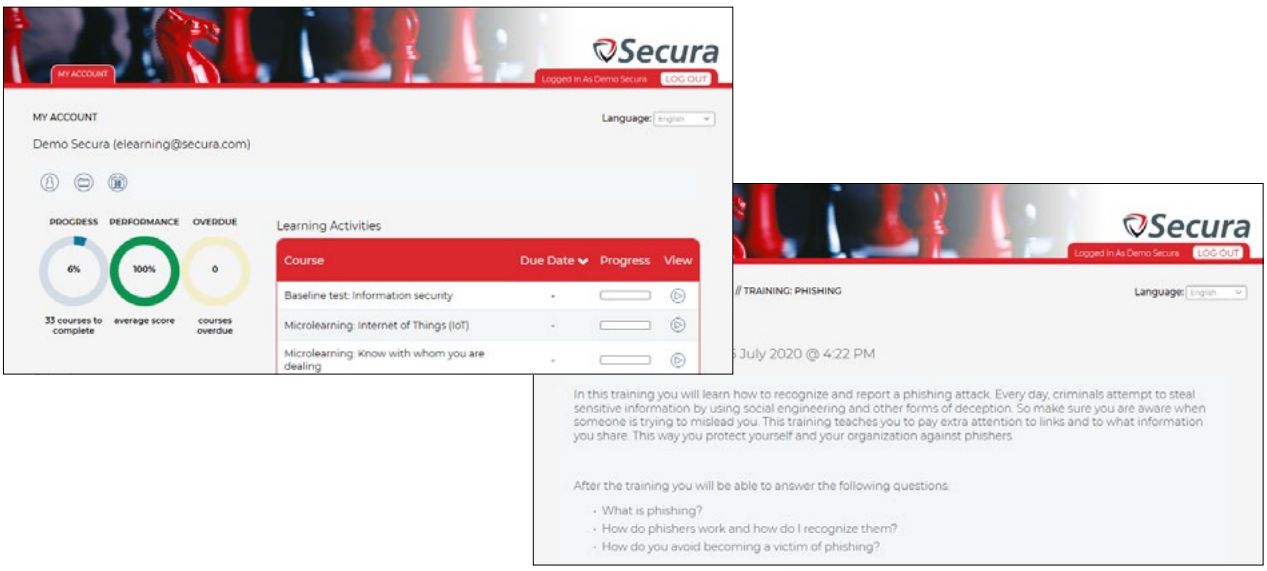
The methodology of SAFE is based on **assess and address**. This concretely means that the program is an orchestrated mix of assessing and training people's awareness and behaviour. We focus on the employee within the context of the **organisation, people, processes and technology** applicable to their daily work.

The end goal of SAFE is:

To reach individual behavioural change addressing the organisation's security

We have combined research and theories related to organisational learning, organisational behaviour and security awareness and translated these into program elements that either assesses, confronts, explains and trains your employees to learn and change their behaviour while creating a secure work environment at the same time.

The full program starts with a combination of behavioural assessments, site assessments and small technical assessments to determine the level of security awareness within the organisation as well as the weaknesses in the context of the employee. This is followed by training through classroom training, workshops, eLearning and relevant exercises. It confronts employees with their behaviour based on the results measured. The constant variety of components and challenges changes knowledge, attitude and behaviour. The yearly effect measurement shows the improvements and areas that continuously require attention.



Measure to Know

The first step is to determine the level of security awareness in your organisation. To measure the level of security awareness we have developed a method that measures the knowledge, attitude and behaviour of employees based on objective criteria. These criteria are the most important components to perform reliable and repeatable research into behaviour of employees and are derived from several categories such as: physical behaviour, digital security, workplace, incident management and other categories based on the ISO 27001 standard and NIST Cyber Security Framework.

The methods to measure behaviour of employees are a phishing attack, an employee survey and a security site assessment, with three main questions:

Baseline measurement: Are your employees secure aware and do they behave accordingly?

- How do your employees react when receiving a phishing email? Do they click or not, and do they report it?
- What do your employees think about information security in your organisation?
- What does Secura observe from a security perspective during a site visit at your offices?

Stage of Competence

In the results of the baseline measurement, we determine the stage of competence related to security awareness. The stages of competence within learning tells your organisation how employees perceive and react to security related tasks and is useful to propose a follow – up strategy to stimulate learning on security awareness topics.

1. The first stage of competence is called 'unconscious incompetence' where employees are perceived not to understand or how to do something within security awareness and does not necessarily recognise the deficit.
2. The second stage is called 'conscious incompetence', that relates to individuals who do not understand or know how to do act securely, but do recognise the deficit as well as the value of a new skill in addressing the deficit. When the results of Secura's measurement state that employees fall within the unconscious incompetence stage or the conscious incompetence stage, employees need to learn what to do in a normative setting is. You cannot do something without knowing how to act securely so we adjust our learning strategy for these employees.
3. The third and the fourth stage, 'conscious competence' and 'unconscious competence', both correlate to a level of understanding how to do act securely but differ in the way of actually thinking about that skill to act securely.
4. In the best case, employees act without concentrating/thinking about their actual behaviour (unconscious competence). They just do it as working secure has become a work habit. That is the end phase that Secura aims to achieve and therefore we must change habits and behaviour to reach that goal.

This baseline measurement tells us how the various components within the SAFE package should be used and implemented within your organisation, specific teams or employees.

Follow-Up Strategy

In our follow-up strategy we will confront your organisation with the results of the baseline measurement in roadshows, a management presentation or during another organisation event. This second intervention is our first direct contact with employees and gives us a chance to create a sense of urgency about the topic of information security.

For example, with our hack demo we show your employees how we crack a password within ten minutes and learn employees how they can create a strong password. The SAFE program manager of Secura will make sure that our advice aligns with the password policy of your organisation.

After this intervention we follow up with a mixture of blended learning by enrolling employees in e-learning courses and starting an offline communication campaign that supports the training courses as they keep reminding employees about the subject of the e-learning course.

When planning the e-learning courses, micro learnings and supporting videos and posters we follow the 'forgetting curve' of Hermann Ebbinghaus who found that new learned knowledge is easily forgotten by people. By sending reminders and using a mixture of communication tools we keep training employees about the relevant topics. Communication and customizing our training methods within the SAFE program is the key of a successful awareness program. Last but not least: we give dedicated attention to make security a topic to take serious while applying fun into the program. This can be addressed with employee attentions, a team game, a cyber security escape room, a crisis simulation, advanced social engineering or training your employees to think like a hacker or performing open source intelligence research themselves.

Security Awareness is more than organizing security training or eLearning in your organisation. Security Awareness requires an integrated approach, a dedicated program in assessing and addressing security awareness. Not only focus on the individual, but also on the context in which your employees are working.

For more information about our SAFE program, please visit: https://www.secura.com/security-awareness-for-everyone-safe

SecurAcademy

GET UP TO SPEED ON DIGITAL SECURITY

When it comes to training and awareness, Secura has a solid track record.
Based on our knowledge and experience we have developed various training courses and workshops which can help you to be and stay 'in control' of your digital security.

TRAINING COURSES & WORKSHOPS

SECURITY ORGANISATION

- **ISO 27001 Overview** (1 day)
- **ISO 27001 Lead Implementer** (5 days)
- **ISO 27001 Lead Auditor** (5 days)
- **GDPR Privacy Training** (1 day)

SECURITY BY DESIGN

- **Threat Modeling Training** (1 day)
- **Secure Programming Training** (1 day)

SECURITY TESTING

- **Hacker Mindset Training Course** (0.5 day)
- **Hands-on Hacking Training Course** (1 day)
- **Internal Pen Test Training** (2 days)
- **Mobile Application Hacking Training** (2 days)
- **ICS Security Training** (2 days)

ONLINE WEBINARS

Would you like to expand your knowledge through online webinars with industry-leading experts? Sign up for a live session or watch the recordings.

For registration and recordings: **SECURA.COM/WEBINARS**

Would you like to enquire about the possibility of hosting an interactive, tailor-made session at your company? Or do you want to join us in an open class course?

Contact us today to find out how we can help you expand your digital security knowledge!

T | +31 (0)88 888 31 00 **E |** info@secura.com

For more information and registration for open class courses:

SECURA.COM/SECURACADEMY

Secura