iB

INFORMATIEBEVEILIGING

jaargang 19 - 2019

#2

Studenten treden in voetsporen cybercrimineel

TaHiTi: a threat hunting methodology

Ik swipe, dus ik ben

Achter Het Nieuws: Europe first

TSTC

ICT en Security Trainingen

Next Generation Cybersecurity Training

TSTC is een gerenommeerd IT opleidingsinstituut en erkend specialist in informatie beveiliging-, cybersecurity en privacy trainingen.

Top 10 Security trainingen

CEH • OSCP • CCSP • CCFP • CISSP • C|CISO • CRISC
Privacy CIPP/E-CIPM • CISM • ISO 27001/27005/31000

Nieuw in 2019

- Extreme Hacking NextGen tm
- Cybersecurity Compliance Officer
- Cybersecurity Specialist
- Certified Chief Innovation Officer
- Red team vs Blue team

Recognition for Best ATC's and CEI's

TSTC Accredited Training Center of the Year 2017

Circle of Excellence Instructor 2017

www.tstc.nl

WINNEN DOE JE SAMEN

Carnaval is weer achter de rug, maar tijd voor samen zijn en samen werken is nog niet voorbij. Misschien moeten we ook in ons vakgebied veel meer met elkaar optrekken en zaken samen oppakken. Hierbij een kort overzicht wat je dit keer van ons kunt verwachten in dit nummer.

De rubriek Achter Het Nieuws staat altijd achterin het blad, maar het onderwerp van deze keer is van voorpaginabelang. De discussie over het 5G-netwerk en mogelijke spionage door Huawei is slechts een symptoom van een grotere verschuiving die gaande is in de verhoudingen en vriendschappen tussen landen. In een tijd waarin internationale betrekkingen tekenen vertonen van wantrouwen in technologie producenten en gegevensuitwisseling, is de samenwerking van Nederlandse financiële instellingen op het gebied van Threat Hunting hoopgevend. Samenwerken en kennisuitwisseling is een belangrijke voorwaarde om ons vakgebied vooruit te helpen. De ontwikkeling van de TaHiTi-methode door samenwerkende 'concullegae' is een mooi statement van hoe het wél kan.

Indirect is samenwerken en kennisuitwisseling ook één van de adviezen in het artikel over PCI DSS. We hebben het dan over samenwerken binnen een breder securityprogramma in een organisatie. Er zit veel overlap tussen securitystandaarden en door die niet steeds als losstaande gebeurtenissen te zien en gebruik te maken van de kennis die al aanwezig is, kan men de scope van verschillende compliance projecten vereenvoudigen.

Maar we openen het magazine met een interview met Melanie Rieback, een grote voorvechter van openheid. Zij stelt dat de samenleving gevaar loopt als beveiligingsbedrijven hun klanten dom houden en kennis niet delen. Activist én ondernemer zijn: dat kan de wereld een stukje beter maken.

Via dit iB Magazine draagt het PvIB weer graag bij aan het verspreiden van kennis. Daarom hebben we ook een overzicht geplaatst van alle artikelen in 2018, die in iB Magazine zijn gepubliceerd: handig als je op zoek bent naar informatie over bepaalde onderwerpen.

Op naar meer samenwerking voor een veiligere wereld!

Fook Hwa Tan en Nicole van Deursen

In dit nummer

Melanie Rieback
(fotograaf Sebastiaan ter Burg)

INTERVIEW

MEDE-OPRICHTER RADICALLY OPEN SECURITY MELANIE RIEBACK OVER HAAR MISSIE VOOR HET LEVEN

Activist én ondernemer. Zo omschrijft Melanie Rieback, mede-oprichter en CEO van IT-beveiligings- en consultancybedrijf Radically Open Security, zichzelf. Geen alledaagse combinatie, beaamt ze. "Zeker niet in het conservatieve zuiden van Amerika waar ik ben opgegroeid." Maar het is volgens haar juist die combinatie van activist en ondernemer die maakt dat ze de boel kan opschudden. Dat ze de potentie heeft de wereld een stukje beter te maken.

We gaan terug naar 2014. Het is wat Melanie Rieback betreft tijd voor een, in haar woorden, "ethisch alternatief in de IT-beveiligingsmarkt." Ze geeft haar baan op bij ING, waar ze deel uitmaakt van het Computer Security Incident Response Team (CSIRT), en ze start Radically Open Security (ROS). Het eerste non-profit IT-beveiligings- en consultancybedrijf ter wereld.

ROS is een sociale onderneming. "Honderd procent van de winst die we tot nu toe hebben gemaakt, is naar de Stichting NLnet gegaan", legt Rieback uit. Zij zet zich al jaren in voor het verbeteren van het internet voor iedereen, voor open source en voor digitale burgerrechten. De Amerikaanse heeft het idee om op deze manier een bedrijf te starten zoals Regina Coeli, het gerenommeerde taleninstituut in Vught, dat op dezelfde wijze als fiscaal fondswervende instelling opereert voor de kerk.

'We creëren bij onze klanten een hacker mindset'

Transparantie en openheid

Rieback predikt transparantie en openheid, omdat digitale veiligheid volgens haar voor iedereen haalbaar moet zijn. Het gedrag van veel grote IT-consultants en -beveiligingsbedrijven noemt ze "maatschappelijk schadelijk, omdat ze de IT-security tot een black box maken. Ze houden hun klanten bewust dom en daardoor lopen de klanten van hun klanten, wij burgers, gevaar."

Ze baseert zich op enkele ervaringen die ze in het verleden had met IT-security consultants. Ze stond toen aan de klantzijde en ze stuitte op een muur van geslotenheid. Kennis werd niet met haar gedeeld, terwijl ze daar naar eigen zeggen wel om vroeg. "Dat moest en kon anders."

Peek-over-our-shoulder

En dus ontwikkelde Rieback met haar collega-hackers binnen Radically Open Security de 'peek-over-our-shoulder'-aanpak. Dit houdt in dat klanten gewoon mogen meekijken wanneer zij en haar collega's, ethisch hackers uit bijvoorbeeld Australië, Amerika, Nederland en Duitsland, de zwakke punten van hun computersystemen blootleggen.

"Elke pentest die je bij ons koopt, is in feite een gratis training. We brengen zo niet alleen onze kennis over. We doen meer. We zorgen voor een verandering in denken. We creëren bij onze klanten een hacker mindset." En dat laatste is volgens haar een voorwaarde om je te kunnen wapenen tegen kwaadwillenden.

De open en transparante manier van werken betekent ook dat Rieback en haar inmiddels veertig freelance collega-hackers open source omarmen en promoten. Alle tools die ROS maakt en gebruikt, zijn met andere woorden voor iedereen gratis beschikbaar.

Samenwerken, Rieback hamert erop. "Cybercriminelen doen het. En dus moeten wij het als IT-professionals ook doen."

Dat zij en haar collega's zich door hun open manier van werken wel eens overbodig kunnen maken bij klanten, gelooft Rieback niet. Dat blijkt volgens haar in elk geval niet uit het hoge percentage herhalingsklanten dat haar bedrijf heeft.

Geeks als ambassadeurs

Klanten waarvoor Rieback graag werkt, zijn boven alles nieuwsgierige klanten. Nieuwsgierigheid die binnen de bijna honderd bedrijven en (overheids)organisaties waarvoor ROS inmiddels werkt vaak in eerste instantie aanwezig is bij de 'geeks' binnen die bedrijven en organisaties. "Zij zijn onze ambassadeurs", legt ze uit. "Ze hebben over ons gehoord via de hacker community of tijdens een keynote of andersoortige lezing van mij. En ze pleiten er vervolgens binnen hun eigen organisaties voor om voor ons te kiezen als het gaat om IT-beveiliging." Ze moeten hiertoe volgens Rieback binnen hun eigen organisaties vaak het gevecht aan met "de interne bureaucratische cultuur." Met succes, want geld uitgeven aan reclame heeft Radically Open Security volgens haar nog nooit gedaan. En toch groeit het aantal klanten gestaag.

Heeft ze haar eigen verwachtingen met Radically Open Security overtroffen? "Ik zie dat onze aanpak andere IT-bedrijven beïnvloedt, maar ook daarbuiten hebben we een positieve maatschappelijke impact. Dat vind ik als sociaal ondernemer nog veel belangrijker. Dus ja, het succes van ROS heeft mijn verwachtingen overtroffen."

Sandra Kagie is freelance tekstschrijver/journalist. In het verleden is zij als eindredacteur nauw betrokken geweest bij iB-magazine. Ze is te bereiken via info@sanscriptoducties.nl.

Hoe collega's en concurrenten over haar denken, maakt haar niet uit: "Het is niet mijn missie hen op te voeden. Ik wil anderen inspireren. Van toegevoegde waarde zijn voor onze klanten en in bredere zin maatschappelijke waarde toevoegen in de vorm van een veiligere wereld voor iedereen."

Groei geen drijfveer

Groei ziet Rieback hierbij allerminst als doel voor Radically Open Security. Het is voor haar geen drijfveer. Integendeel, groei vormt volgens haar "een bedreiging voor de kwaliteit, integriteit en ethiek op basis waarvan zij klanten wil bijstaan." Investeerders worden door haar dan ook steevast buiten de deur gehouden. "Investeerders zijn uit op return-on-investment. Dat maakt dat je als bedrijf andere beslissingen gaat nemen. En daar gaat het mis."
De tijd is volgens de Amerikaanse rijp voor een radicaal andere manier van (economisch) denken. Ze verwijst naar de opkomst van het gedachtegoed van post-growth economen. "Een beweging die moet leiden tot een nieuwe manier van denken en daarmee tot een samenleving die niet langer gebaseerd is op exponentiële groei", legt ze uit.
Rieback ziet, in navolging van econoom en nobelprijswinnaar Muhammad Yunus, 'non-dividend businesses' als de bedrijven die de wereldproblemen kunnen oplossen. "Non-dividend businesses of sociale ondernemingen hebben niet winst als drijfveer, maar een positieve maatschappelijke impact. We pakken een maatschappelijk probleem bij de kop en stellen ons ten doel de pijn die dit probleem veroorzaakt op te lossen. In het geval van Radically Open Security is het doel een veiligere wereld voor iedereen."

Missie voor het leven

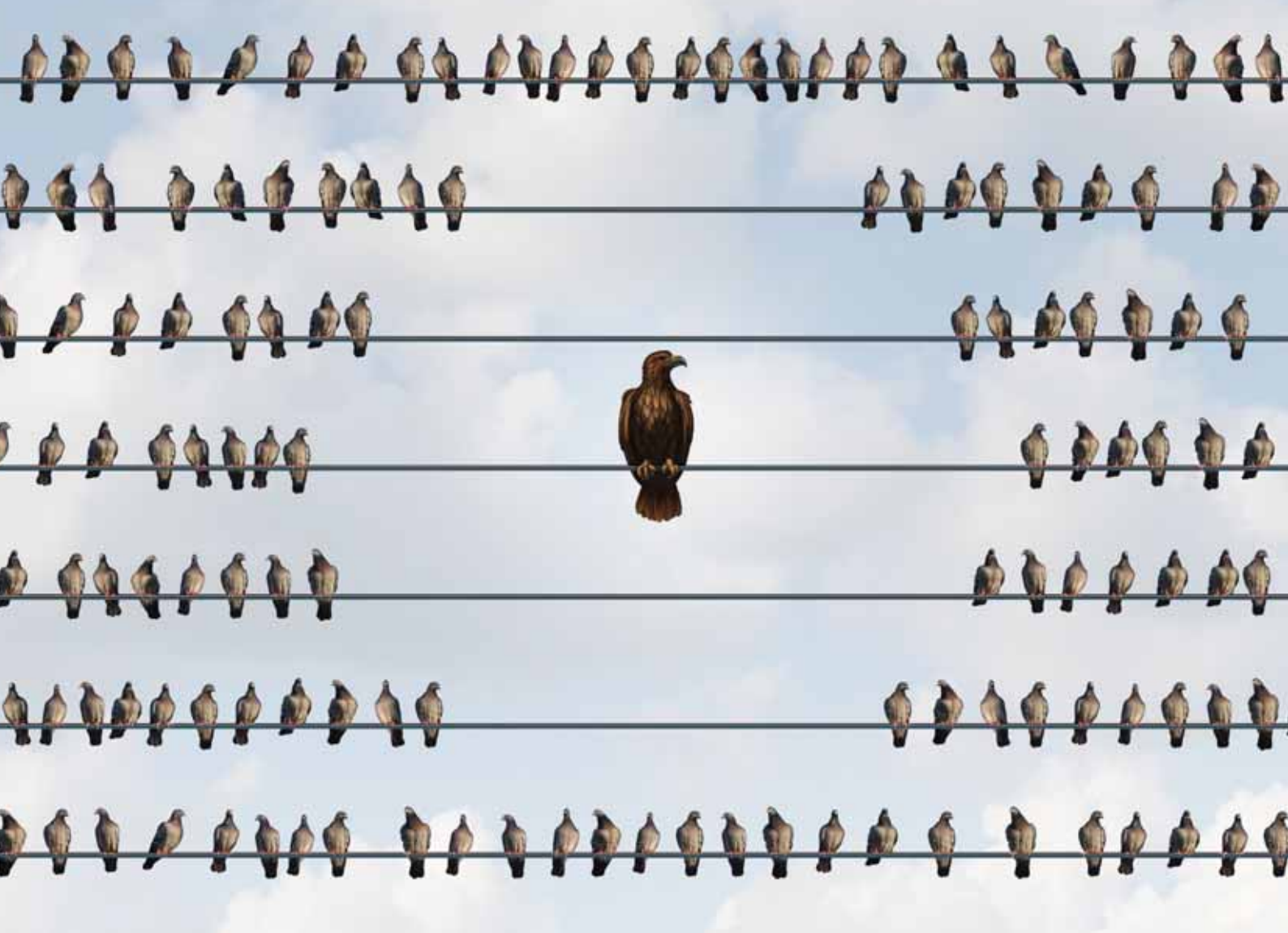
Met haar tweede bedrijf, Nonprofit Ventures, dat ze zo'n jaar geleden is gestart, wil Rieback nieuwe start-ups van sociaal ondernemers ondersteunen. Ze noemt het bedrijf een "non-profit start-up incubator." Ze wil met dit bedrijf bouwen aan een community van non-profit ondernemingen. In haar woorden "een missie voor het leven. Het gaat misschien in kleine stapjes, maar de kleine stapjes tellen wel op. Niet groeien, maar inspireren en daardoor verspreiden. Daar gaat het om."
Het verspreiden van haar boodschap om als bedrijf maatschappelijke impact na te streven in plaats van winst, doet Rieback niet alleen door het geven van lezingen, maar bijvoorbeeld ook door het geven van colleges aan jonge, startende ondernemers. Dit onder meer tijdens de startupbootcamps van ACE, het Amsterdam Center for Entrepreneurship.

Dat ze door dit soort activiteiten veel minder dan enkele jaren geleden bezig is als ethisch hacker, neemt ze voor lief. "Ik vind het soms jammer. Maar op deze manier, door anderen te inspireren, heb ik meer positieve impact."

RACHEL MARBUS

Mijn naam is Rachel Marbus en ik ben op dit moment functionaris gegevensbescherming bij KPN. Ik ben ooit bij de redactie van PvIB binnengerold nadat ik de vraag kreeg waarom ik als privacy officer toch zo actief was op social media en of ik daar niet eens een column over wilde schrijven. Dat was een match made in heaven. Vanaf dat moment ben ik met heel veel plezier vaste columnist geworden en niet lang daarna lid van de redactie. Saillant detail: ik was op dat moment nog helemaal geen lid van het PvIB. Dat heb ik uiteraard snel opgelost, noblesse oblige. Toen er een bestuursfunctie vrijkwam, hoefde ik niet lang na te denken. Na een pittig gesprek bleek dat de andere leden van het bestuur het wel zagen zitten met mij. Dat is alweer 8 jaar geleden. Binnen het bestuur ben ik actief voor eventuele juridische vragen, maar ook voor pers en PR. Voor mij is het lidmaatschap van PvIB altijd van onschatbare waarde geweest voor mijn vakgebied. Een privacyspecialist kan niet goed functioneren zonder ook op zijn minst een beetje verstand te hebben van informatiebeveiliging. En daarnaast zijn mensen binnen ons werkveld ook gewoon super gezellig(e nerds) en voelde ik me vanaf het eerste moment thuis binnen deze prachtige vereniging. Het meest recent opvallende nieuws is voor mij het onderzoek van een Australische onderzoeksgroep naar de identificeerbaarheid van personen aan de hand van hun swipegedrag. Ik vond dat zo relevant dat ik er zelfs voor dit nummer een column over geschreven heb.
Meer in zijn algemeenheid geniet ik enorm van nieuws over technologische innovaties die bedoelde en onbedoelde neveneffecten hebben, omdat dit nu exact het soort nieuws is wat ons aller vakgebied zo leuk maakt.
Binnen de informatiebeveiliging heb ik een enorme volwassenwording gezien de afgelopen 10 jaar. Eentje waarop ik eigenlijk als privacyprofessional best wel een beetje jaloers ben. We staan nu namelijk waar de infosec 10 jaar geleden stond en hebben we nog een enorme weg te gaan. Voordeel is natuurlijk wel dat ik en mijn privacyconcullega's de kunst kunnen afkijken en het goede voorbeeld kunnen volgen. Het ontwikkelen van een kwalificatiestelsel voor informatiebeveiliging is een mooi hoogtepunt binnen de infosec waarvan ik van harte hoop dat het ook binnenkort in de privacywereld opgepakt gaat worden. Ik denk dat het PvIB alleen maar relevanter zal worden naarmate de tijd verstrijkt. Ik hoop dat iedereen die zijn eerste voetstappen binnen ons vakgebied zet, automatisch lid van het PvIB wordt en zo ook weer mooie, nieuwe en frisse ideeën meebrengt.

Rachel Marbus



TaHiTI: A THREAT HUNTING METHODOLOGY

Threat hunting is a relatively new area of expertise. While the activity itself is not new, specific hunting tools, models and best practices have been developed in recent years. As with any new area, there is often confusion on what exactly comprises this activity. Good definitions are lacking, as are common approaches on how to perform such an activity.

The 2017 SANS survey on threat hunting has indicated that only 4,6% of all companies engaging in threat hunting activities have adopted a published external methodology. Excluding outsourcing and companies that do not perform threat hunting, that leaves over 70% of organizations either using no methodology or a methodology that was created internally (1). This shows a clear lack of availability of threat hunting methodologies that cover the entire process in a structured fashion.

Members of the Dutch financial sector that were conducting threat hunting activities have come to the same conclusion. In-house methodologies and hunting expertise were being developed separately. As such, the timing was right for a joint effort in creating a common understanding and common approach in threat hunting, as well as sharing best practices amongst each other. The TaHiTI (which stands for Targeted Hunting integrating Threat Intelligence) methodology is a direct result of that effort. The methodology itself seeks to combine threat hunting and threat intelligence to provide a focused and risk-driven approach to threat hunting. Threat intelligence is used as a source for hunting investigations and is used throughout the investigation to further contextualize and enrich the hunt.

Threat hunting

To have a common understanding of threat hunting, a common definition is required. Threat hunting in TaHiTI is defined as follows:

'Threat hunting is the proactive effort of searching for signs of malicious activity in the IT infrastructure, both current and historical, that have evaded existing security defenses.'

This evasion of security defenses can be due to usage of new, improved or unknown attacker techniques, 0-day exploits or a lack of adequate detection technology within the organization. While incomplete or faulty configuration of detection technology or misinterpretation of security events by analysts during triage can be reasons for evasion as well, threat hunting assumes a properly running security monitoring process.

The main purpose of threat hunting is to reduce the time required to find traces of attackers that have already compromised the IT environment. By finding these traces as soon as possible, the impact of breaches to the organization can be minimized. Other benefits of threat hunting include:

- identification of gaps in visibility necessary to detect and respond to a specific attacker TTP;
- identification of gaps in detection;
- development of new monitoring use cases and detection analytics;
- uncovering new threats and TTPs that feedback to the threat intelligence process;
- recommendations on new preventive measures.

Breach detection gap

As indicated, the goal of threat hunting is to decrease the gap between initial compromise by an attacker and the discovery of that attacker in the environment: the breach detection gap also known as 'dwell time'. Figure 1 shows a timeline of an attack containing several key moments in time. The breach detection gap is the time between T=1 and T=2.

According to the latest Verizon Data Breach Investigation Report (DBIR), 68% of compromises went undetected for months (2). Threat hunting plays an important role in reducing the breach detection gap. This is also evident in the SANS threat hunting survey, where improvements to incident response were mentioned as key improvements due to threat hunting activities. Threat hunting will aid to accelerate the detection of attackers by introducing new or improving existing detection mechanisms and thereby further closing the breach detection gap. Continuous insight into the state of detection mechanisms is required

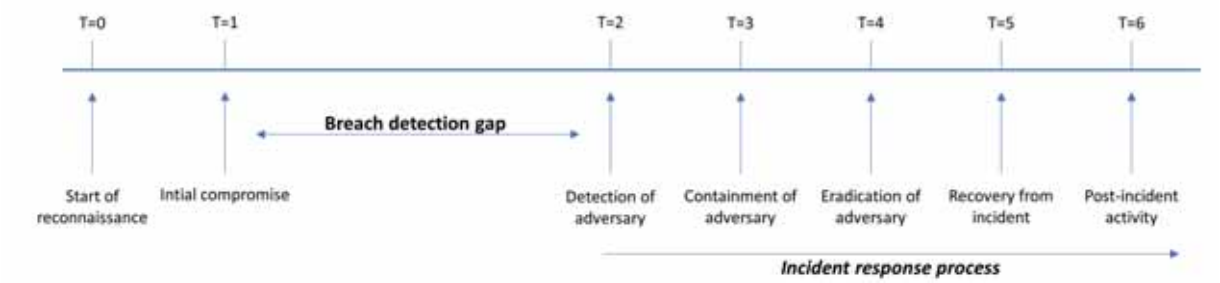


Figure 1 - Use case model

to avoid hunting for malicious activity that is already covered by traditional detection mechanisms. Use case management frameworks, such as MaGMa (3) can aid in such insight.

Types of threat hunting
When it comes to types of threat hunting, it basically drills down to 2 types: unstructured hunting and structured hunting.

Unstructured hunting is data-driven hunting. Potentially malicious activity can be detected by a hunter who is simply digging through available data looking for anomalies. This type of threat hunting does not start with a hypothesis, does not follow a predetermined path and is thus considered unstructured.

Structured hunting is hunting based on hypotheses: a hypothesis is created, the hunting activity is scoped and subsequently performed. TaHiTI is a structured hunting approach that involves several steps and a clear idea of what the hunters are looking for before any hunting activity is initiated.

Figure 2 - Pyramid of Pain. TaHiTI focuses on the top 3 layers of the pyramid (source: David Bianco, detect-respond blog).

Pyramid of Pain
The Pyramid of Pain (2) is an important and elegant concept that can be used in threat hunting and threat intelligence. The pyramid addresses how difficult it is for attackers to change certain characteristics of their attack. At the same time, it also shows how difficult it is for organizations to find these characteristics. Finding a file with a certain hash value is easy, but uncovering illegitimate use of PowerShell in an organization where PowerShell is commonly used poses an entirely different challenge. Similarly, it is trivial for attackers to generate a new file with a different hash, but much harder to move or modify an attacker technique to evade detection. Figure 2 shows the Pyramid of Pain.

The Pyramid of Pain connects threat hunting to threat intelligence. Threat intelligence provides relevant information on attackers on all layers of the pyramid. Threat hunting with the TaHiTI methodology will focus on the top 3 layers (but may use the lower 3 layers nonetheless) of the pyramid. TTPs (the methods of attack used by attackers) have the most focus in threat hunting investigations.

Threat intelligence
As with threat hunting, it helps to have a clear definition of threat intelligence. Threat intelligence is defined as follows:

'Threat intelligence is the process of gathering, processing and dissemination of information about threats and attackers. The goal of threat intelligence is to contextualize the information and to deliver actionable information that can be used in the decision-making process.'

The threat intelligence process puts information from the outside world into the organizational perspective and, if possible, advises on how to proceed. This requires determination of risk, impact and possibly mitigating measures from intelligence information. Threat intelligence also provides insight into how attackers operate, their motivation, the sectors and geographic locations they operate in and the level of capability they possess.

The relationship between threat hunting and threat intelligence

There is a clear relationship between threat hunting and threat intelligence. This has become apparent in the section on threat hunting, as some concepts in threat hunting are difficult to explain without basic knowledge of threat intelligence. For the TaHiTI methodology, 3 concrete elements of the relationship between threat intelligence and threat hunting are especially important:

- intelligence as a starting point for hunting;
- intelligence for contextualizing and driving the hunt;
- hunting to generate intelligence.

Intelligence as a starting point for hunting
As threat intelligence provides us with a lot of information on attackers and their capabilities, it can be a major source for engaging in hunting activities. For example, a threat intelligence report describing an attacker group and their distinct capabilities should be of great interest. If that attacker group also operates in your organization's sector and is also geographically relevant, the threat it poses may be significant. The threat intelligence process can trigger the threat hunting process based on this information and provide relevant context on the threat.

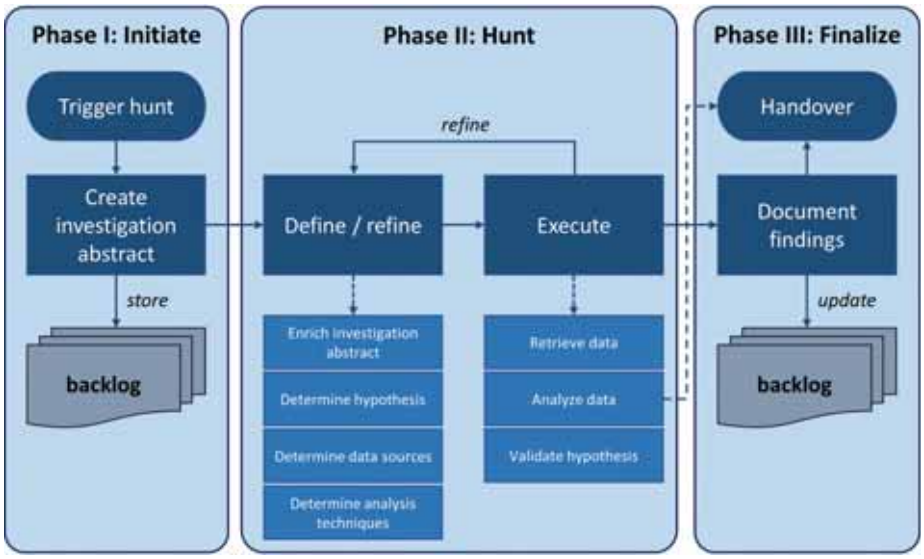


Figure 3 - The TaHiTI process.

Intelligence for contextualizing and driving the hunt

During hunting investigations, threat intelligence can be used for contextualization of findings. For example, a certain TTP may be uncovered during the threat hunting process. Using threat intelligence, that information may be used to find related TTPs (for example, using the MITRE ATT&CK framework (5)(6)) or additional information on that TTP. This can subsequently be used to further drive the hunt. This process is called pivoting and may lead to additional hunting activities or refinement of the active hunt. For the TaHiTI methodology, this interaction between threat intelligence and threat hunting is especially important. Context from threat intelligence may lead to extending the scope of the hunt, adding new data to the hunt, refining the hunting hypothesis or generating ideas for subsequent hunts.

Hunting to generate threat intelligence

As mentioned earlier, threat hunting can be a source for threat intelligence. Hunting investigations may uncover previously unknown TTPs for attackers. This information can be used in the threat intelligence process to build an attacker profile. All such information can subsequently be shared with peers in threat intelligence communities, providing them with information regarding the uncovered threat. If these peers start their own hunting investigations based on this new TTP, they may uncover additional indicators that can be shared with the threat intelligence community. This way, a more complete picture of attacker capabilities and TTPs can be built in a community effort. Within an active threat intelligence ecosystem, the sum is greater than the whole of its parts.

TaHiTI methodology

As indicated in the introduction, TaHiTI stands for Targeted Hunting integrating Threat Intelligence. 'Targeted' because the methodology uses hypotheses to drive hunting activities. This means threat hunting is conducted with a specific goal in mind. 'Integrating threat intelligence' because threat intelligence is a major source of threat hunting hypotheses, and is used to enrich and contextualize hunting activities. Lastly, threat intelligence may also be generated as a result of hunting activities.

The TaHiTI process overview

Figure 3 provides an overview of the TaHiTI process, and its 3 phases: initiate, hunt and finalize. The process has 6 steps in total.

Phase 1: initiate

The initiation phase is where the input for threat hunting is processed. First, there is an initial trigger to initiate the hunting process. Next, the trigger is converted to an abstract of the hunting investigation and stored on the hunting backlog.

The threat hunting process can be triggered from several processes. Figure 4 shows triggers for threat hunting. An important thing to notice is that the processes that could potentially provide triggers to start the hunt strongly overlap with the processes that receive output from the investigation (figure 5). When executed well, hunting can act as an accelerator for improvement of these other processes.

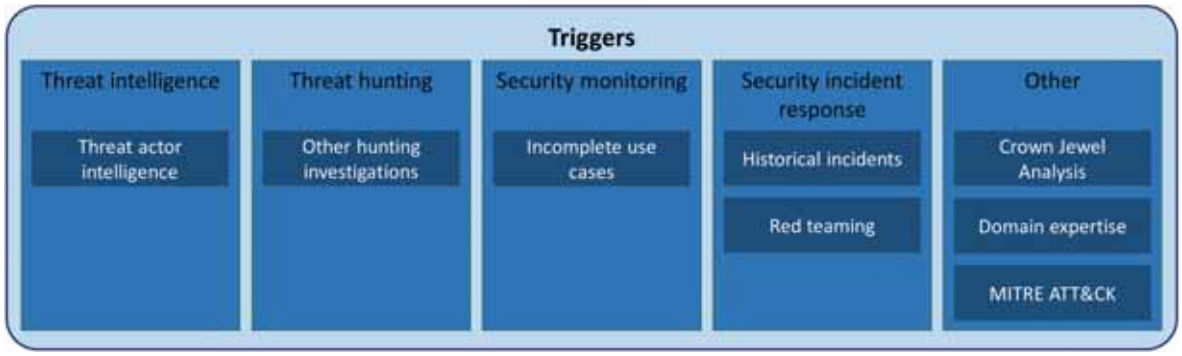


Figure 4 - Hunting triggers.

Of all these triggers, the MITRE ATT&CK framework is especially important. The MITRE ATT&CK framework can be used as input for potential attack vectors and techniques, and contains a wealth of information for any hunter. The framework also provides suggestions for detection, which is valuable for both hunting and security monitoring. Note that this is not the primary purpose of the framework and should be treated as guidance for monitoring only.

When a trigger is received, the hunting team creates a hunting investigation abstract. This abstract does not include all details, but is a basic description of the investigation. Most of the information will be refined and updated in a later stage, when the hunt is selected for execution. After the abstract is created, it is stored on the hunting backlog. This backlog does not need to be a complex tool. Simple collaboration tools such as Microsoft SharePoint or JIRA can suffice. The most important thing is that the backlog provides the hunting team with the required insight to select the most relevant abstract for the next hunt.

Phase 2: hunt

The second phase of the hunt is where the actual investigation takes place. There are 2 activities in this phase. The first activity in the hunting phase is called 'define/refine'. The second activity is called 'execute' and is the actual conducting of the hunt.

In the 'define/refine' step, the details for the hunt are defined and made more concrete. During this step, the abstract is turned into an investigation by refining and adding information. Some new elements are added, such as required data sources and data analysis techniques. Most importantly, a hypothesis is created that drives the hunt. Generating this hypothesis is a vital step in the hunting process. A badly defined hypothesis will likely lead to no results or even worse, wrong results and thus wrong conclusions and recommendations to the organization.

With 'define/refine' activity completed, the 'execute' activity can be started. During the 'execute' step of the hunt phase, data is retrieved and analyzed. Existing hunting documentation lists a number of data analysis techniques. Some of these techniques, such as querying, are simple and easy to perform. Other techniques, such as clustering are more difficult to understand and require some basic understanding of statistics to use them properly. Some analysis techniques can be applied manually by analysts, while other require some form of machine learning. Hunting platforms that contain analysis techniques and visualizations can be leveraged to simplify analysis. In the data analysis step, the hunting team may find omissions introduced in the define stage. At this point, the hunters will refine the initial investigation. This is an iterative process that is repeated until the investigation is optimized. Refinements can be done to hypotheses, scope, selected data sources and analysis techniques.

When performing data analysis, threat intelligence can be used to add context to investigations. The need for this depends on the investigation. When the threat hunting team finds matches on specific TTPs, further analysis into that TTP must be performed. If possible, this activity should be conducted in collaboration with the threat intelligence team. Such analysis may provide information on possible threat actors, their methods and capabilities, technical infrastructure and other victims of the same actor (the 4 features of the diamond model of intrusion analysis (7). The MITRE ATT&CK framework can be used this in this process. Additionally, the MITRE ATT&CK navigator, can be a useful resource as it associates attack techniques to APT groups. To determine which APT groups are relevant for your sector and organizational type, the APT threat tracking overview is a good starting point (8). This information can subsequently be used to extend the hunting investigation to find additional malicious activity. This provides the hunter with a more complete overview of the compromise that has taken place.

The final activity of the 'hunt' phase is hypothesis validation. When the hunting investigation is finished, the hypothesis must be validated. This will either result in a proven hypothesis (malicious activity found, incident response started), disproven hypothesis (no malicious activity found) or inconclusive. In the latter case, the hunter can cycle back to the first step (define/refine) to change some of the parameters of the hunt and repeat the execution. In some cases, the required data may simply not be available. In such case, the hunt can be considered to be failed. This can still lead to valuable lessons learned.

Phase 3: finalize

The final phase of the TaHiTI process is the documentation of results and handover to other processes.

The threat hunting team must process the results from the execution step and document findings. This documentation must cover the most important results of the hunt, and the conclusions drawn based on those results. The documentation may also have recommendations. Recommendations may include improvements to preventative measures (from simple configuration changes to architectural changes), recommendations for logging (additional sources, additional details, etcetera), recommendations for security monitoring use cases and process recommendations (improvements in vulnerability or configuration management). Finally, the document should have a 'lessons learned' sections that covers how the hunt has helped the hunters to improve. Lessons learned could also be that the hunters have gained valuable insight into parts of the infrastructure. Such insights may ultimately lead to new hunting activities and make subsequent hunts more efficient.

The final activity is handover to other processes. Potential processes that can receive input from the hunting investigation are security incident response, security monitoring, threat intelligence, vulnerability management and others. These processes are show in figure 5.

Metrics and MaGMa for threat hunting

Metrics are important to determine the efficiency and effectiveness of the threat hunting process and show its added value to the organization. There are 2 basic types of metrics: quantitative (numbers) and qualitative (value). The focus should be on how threat hunting adds value to the organization, so careful selection of metrics is required. The following is a short list of metrics that are indicators of the value added by the threat hunting process:

- the dwell time of the findings: since threat hunting should reduce dwell time this should be reported for any compromise uncovered in threat hunting;
- incident response: the number of incidents triggered by the threat hunting process;
- security monitoring: the number of added and updated use cases;
- threat intelligence: new threat intelligence created during the threat hunting process;
- security recommendations: new preventative measures suggested in threat hunting reports;
- vulnerability management: the number of vulnerabilities or misconfigurations uncovered.

When defining metrics for threat hunting, it is important to start out with the goal of the process and then determining useful metrics. While defining metrics that are indications of quality is harder than simply providing numbers, it is well worth the effort.

The TaHiTI methodology is supported by the 'MaGMa for threat hunting' tool, which allows hunters to document their results, structure the outcome of their hunting investigations and provide direction for growth of the threat hunting process. Some of the above metrics have been embedded in the MaGMa for threat hunting tool.

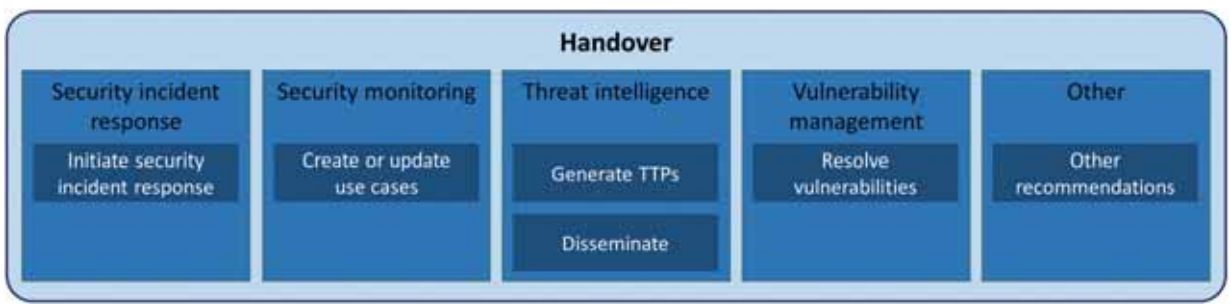


Figure 5 - Processes triggered by threat hunting investigations.

The TaHiTI methodology integrates threat hunting and threat intelligence and provides a clear step-by-step process

While this tool can be used separately from the MaGMa Use Case Framework, organizations that are already using MaGMa for their use case management will be able to more easily integrate threat hunting and security monitoring processes. This is due to the common language between these teams and their tools.

Conclusion

The TaHiTI methodology integrates threat hunting and threat intelligence and provides a clear step-by-step process that hunters can follow to conduct structured hunting investigations. Take these last considerations into account:

- carefully select, prioritize and document your input (triggers);
- execute hunting with care and apply critical thinking continuously;
- use hunting output to drive other security processes and mature and evolve the hunting process itself.

As with any methodology, not all of it may be required for every single hunt. In some cases, hunting investigations will be broad and look at different aspects of a complex TTP. In other cases, hunting investigations may be narrow and scoped at a single specific aspect. Some hunts will benefit from a very formal approach, while others may not. Because each hunt is different, investigations will have different requirements. It is up to the organization to apply the methodology in a flexible way that allows the hunters the freedom to hunt in a standardized and efficient manner, without introducing unnecessary overhead. The threat hunting team should consider which elements are required before initiating a hunt, while retaining the flexibility to apply changes where required.

The full documentation and the MaGMa for threat hunting tool can be obtained from: www.betaalvereniging.nl/en/safety/tahiti/

Authors

Rob van Os, de Volksbank, lead author. Rob is bereikbaar via rob.vanos@devolksbank.nl.
Marcus Bakker, Rabobank, co-author
Ruben Bouman, ING / FinancialCERT
Martijn Docters van Leeuwen, Rabobank
Marco van der Kraan, Rabobank / FinancialCERT
Wesley Mentges, de Volksbank
Armand Piers, ABN AMRO Bank / FinancialCERT

References

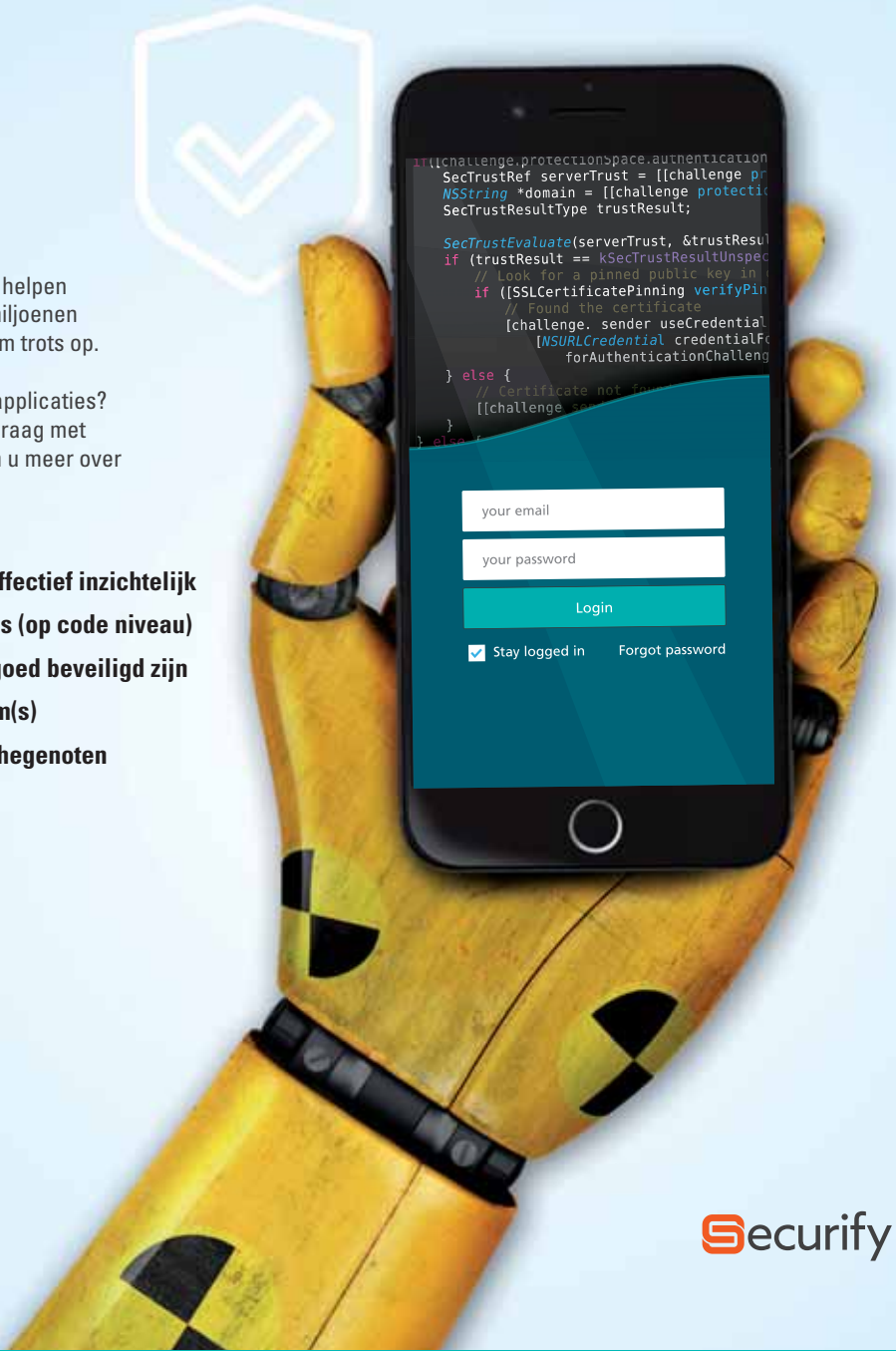
(1) www.sans.org/reading-room/whitepapers/analyst/hunter-strikes-back-2017-threat-hunting-survey-37760
(2) www.verizonenterprise.com/resources/reports/rp_DBIR_2018_-Report_execsummary_en_xg.pdf
(3) www.betaalvereniging.nl/en/safety/magma/
(4) detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
(5) attack.mitre.org/
(6) medium.com/mitre-attack/finding-related-att-ck-techniques-f1a4e8dfe2b6
(7) www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
(8) apt.threattracking.com

Uw applicaties goed **beveiligd!**

Veel bedrijven - van start-ups tot grote banken - vertrouwen al jaren op Securify om hun applicaties goed te beveiligen.

Met jaarlijks honderden pentesten en code reviews helpen wij achter de schermen mee om de gegevens van miljoenen Nederlanders veilig te houden. En daar zijn we enorm trots op.

Nieuwsgierig naar de beveiligingskwaliteit van uw applicaties? Of waarom Nederlands grootste bedrijven al jaren graag met ons samenwerken? Dan maken we graag kennis om u meer over onze aanpak te vertellen.



- ✓ **Alle beveiligingslekken en verbeterpunten effectief inzichtelijk**
- ✓ **Concreet en direct toepasbaar verbeteradvies (op code niveau)**
- ✓ **Maak aantoonbaar dat uw applicaties écht goed beveiligd zijn**
- ✓ **Een awareness boost voor uw ontwikkelteam(s)**
- ✓ **Leer waar u staat ten opzichte van uw branchegenoten**

www.securify.nl

Securify

Pentesting - Source Code Reviews - Agile Security - Red Teaming

Securify is specialist in web- en mobiele-applicatiebeveiliging en helpt bedrijven met het identificeren, verhelpen en voorkomen van technische beveiligingsrisico's.
Securify is opgericht door voormalig beveiligingsspecialisten van ABN AMRO, Delta Lloyd en Rabobank.

WAT JE IN KEULEN KUNT LEREN OVER SAMENWERKING

De manier van leven in Keulen kent veel plezier, weinig stress en een grote mate van tolerantie. Dit is samengevat in het 'Kölsche Grundgesetz' (zie tabel). Deze 11 levenswijsheden zijn ook bruikbaar voor medewerkers en managers van security-afdelingen. Vooral omdat ze positief zijn voor de samenwerking, wat heel belangrijk is in securityland.

Voor wie Keulen niet zo goed kent, eerst wat achtergrondinformatie over deze stad:

Keulen en Karneval

In de Dom in Keulen liggen de beenderen van de drie koningen uit het kerstverhaal. 'Kölle' is daarmee één van de vijf belangrijkste steden voor het christendom.
Keulen heeft ook haar eigen gelijknamige biersoort: Kölsch. Deze biersoort mag alleen in deze stad en directe omgeving gebrouwen worden. Het bijbehorende glas van 0,2 liter is slanker dan het bierflesje en laat het lichte, frisse bier stevig schuimen. Vanwege het tere glas klinkt men met de stevige onderkant van het glas. Dit gebeurt vaak, want zoals het lied 'Viva Colonia' meldt: 'Wir trinken gerne Kölsch und wir haben immer Durst'. Dit Duitse origineel van 'Viva Hollandia' noemt de plaatselijke voetbalclub, de ijshockeyvereniging, het gemeentelijk vervoerbedrijf, diverse theaterbedrijven en bekende cabaretiers. Het nummer gaat in op de grote tolerantie voor alternatief leven in deze grote Duitse stad, waar altijd wel iets loos is.

De jaarlijkse Christopher Street Day (CSD) parade is gericht op de LGBT-community, men is actief tegen racisme en iedereen, groot of klein, houdt van een feestje waarbij op kosten niet word gelet. Het 'Karneval' zit Keulenaars in het bloed, men is immers met een feestneus op geboren. Successen vieren, dat werkt. En God is als lieve Heer altijd aanwezig (zie de Dom). Het is feest, maar het blijft wel netjes wanneer ze, refererend aan hun dagelijkse zorgen, in het genoemde lied niet 'Leck mich am Arsch', maar keurig de afkorting 'LMAA' zingen. Het 'vijfde jaargetijde' begint in Keulen op 11 november en duurt tot Aswoensdag. Dat is het einde van Karneval, dat 40 dagen (de vastenperiode) voor Pasen valt. Eerste Paasdag is de eerste zondag na de eerste volle maan (na lente-equinox). Dit vijfde jaargetijde heeft dus elk jaar een andere lengte. Misschien legt dit lied daarom de nadruk op genieten van het moment (want elk moment is er slechts één keer) en op alles meenemen in het leven wat je krijgen kunt. Ook in security kun je niet op voorraad werken, je moet reageren op de situatie nu. En ook het incident van vorige week nogmaals oplossen, heeft geen zin.

Verbinding

'Da simmer dabei' uit 'Viva Colonia' is in de Nederlandse versie gewoon: 'We zijn er weer bij en dat is pri-hi-ma'. Maar de Höhner zingen in hun lied niet zomaar twee keer 'da' in dat korte zinnetje en bedoelen: 'dáár zijn we erbij, dáár horen we erbij'. Een feestlied over inclusiviteit dus, in een stad die 'jedem auf den Arm und an die Hand' neemt. Met precies die woorden legt Tommy Engel in zijn lied 'Du bes Kölle' uit dat inwoners zo de mensen ondersteunen die zelf nog niet kunnen gaan. Ze geven op die manier sturing aan mensen die een (klein) zetje in de goede richting kunnen gebruiken. 'Modern management' noemen we dat in Nederland, tijdens een training op de hei. Daar zingen ze het met zijn allen en drinken er een pilsje bij. Wat blijft er dan beter hangen? Zo'n managementstijl is goed bruikbaar op een security-afdeling met professionals die verschillen in ervaringsjaren.

Kölsche sproch

De Höhner zijn niet vernoemd naar de Hunnen, onder leiding van Attila, maar heten heel onschuldig: 'De kippen'. In een ander lied 'Hey Kölle, du bes un Jeföhl' stellen zij vast dat Keulen niet alleen een stad is, maar vooral een gevoel. Een gevoel dat je overal ter wereld kunt hebben. Ook als niet-inwoner. Zoals security ook een houding is, en niet alleen een afdeling. Mensen zingen daarom overal in Duitsland met een andere Keulse band (Brings) mee: 'Ich ben ne Kölsche Jung'. Een Keulse knaap dus. Of ze nu man, vrouw of genderneutraal zijn. Dit lied gaat over de Keulse straattaal, die wordt uitgesproken met het hart op de tong en die de (virtuele) inwoners onderling bindt als trotse eigenaars. Zoals security-jargon en eigen afkortingen ook kunnen binden. Samen tegen de rest van de wereld. Hoewel het Keuls sowieso als belangrijke basis Duits heeft, lieten eeuwen van vreemde invloeden door diverse bezettingen (de Romeinen ten tijde van Colonia, later ook Napoleon en zijn Cologne, en na de Tweede Wereldoorlog min of meer de Engelsen) hun sporen na in de 'Kölsche Sproch'. Als u echter uw Limburgse vrienden grotendeels kunt verstaan, zal het in Keulen ook wel lukken. Zeker omdat men daar bereid is voldoende luid te spreken en flink te gebaren.

Rijnlands model

Keulen ligt aan de Rijn en in het Rijnland. De Rijnlandse manier van zakendoen kenmerkt zich door jarenlange relaties, samenwerking ('partnership' in het Nederlands) en geven en nemen, over en weer. De vele familiebedrijven gaan generaties lang over van vader/moeder op dochter/zoon. Relaties het vel over de neus halen door leveranciers heel weinig te betalen of klanten heel veel te laten betalen, wordt er bij voorkeur niet gedaan. Zo smeden ze langdurige relaties die tegen een stootje kunnen. En die stootjes worden door een mix van tolerantie, gezelligheid en beleefdheid zoveel mogelijk vermeden. Het water in 'de Rhing' verbindt de steden en de inwoners. Het is een transportmiddel, maar soms ook een gezamenlijke vijand als de rivier door veel neerslag en smeltwater uit de bergen buiten haar oevers treedt. Zoals ook cybercrime een gezamenlijke vijand is, die medewerkers bindt. Over de Keulse Hohenzollernbrücke over die Rijn rijden dagelijks meer dan 1.220 treinen. Het is de drukste spoorbrug van Duitsland. Aan beide zijden van de brug is een wandelpad, zodat duizenden verliefde stelletjes en lossere vriendengroepen al meer dan 100.000 hangsloten aan deze brug konden bevestigen. Met daarop hun namen en een datum geschreven of zelfs gegraveerd. Door het sleuteltje in de Rijn te werpen, bevestigden zij hun onderlinge eeuwige band en die met de stad Keulen. Ze wonen er niet allemaal, maar dat minstens 200.000 mensen zoiets doen, geeft toch een bepaalde sfeer in je stad. Bijvoorbeeld bij de Angelsaksen zit het leven heel anders in elkaar. Zowel het United Kingdom als de United States namen 'verenigd' op in hun naam, maar het is daar allemaal iets competitiever ingesteld en meer gericht op de korte termijn: het kwartaalresultaat is wat telt. Waar men in het Rijnland een dialoog voert, waarin beide partijen hun mening toelichten zodat de ander die kent en er rekening mee kan houden, willen de Angelsaksen in hun discussies altijd één duidelijke winnaar hebben, wiens mening daarna als enige telt. Het water vormt voor beide eilanden (UK+USA) een 'muur' van waarachter klanten en leveranciers wél eenvoudig en op afstand extra oren kunnen worden…. Enfin, u begrijpt wat ik bedoel.

Levensstijl

Veel aspecten van de Keulse levensstijl zijn nuttig als tips en trucs voor medewerkers en managers van security-afdelingen. De elf zegswijzen zijn als geboden overal in de stad te vinden als het 'Kölsche Grundgesetz' (basiswet). Het is natuurlijk geen echte wet. Daar is men in deze 'Stadt am Rhing' net iets te eigengereid, prettig gestoord en brutaal voor. Maar als je er op bezoek bent, zul je veel zaken die zo effectief zijn in het

Robert Metsemakers is als ervaren IT auditor en informatiebeveiliging expert beschikbaar voor security advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

DAT KÖLSCHE GRUNDGESETZ

	Hoor in Keulen:	*Denk hierbij aan:*
1	Et es wie et es	Security-patches zijn nodig, elke maand. Security-budget is nooit onbeperkt. Sommige gebruikers klikken op duidelijk herkenbare phishing-mails. De volgende keer dat je geïrriteerd raakt over iets, vraag je dan af: kan ik het veranderen? En zo niet, neem het dan zoals het is en probeer de positieve kant te vinden.
2	Et kütt wie et kütt	Cybercriminelen vallen op vrijdagavond of net voor een feestdag aan, als iedereen naar huis wil. Het noodlot (`Schicksal') kiest zijn eigen weg. Sta daarom open voor wat er op je af gaat komen.
3	Et hät noch emmer jooj jejange	Wat gisteren werkte, zal morgen ook functioneren. De virusscanner doet het morgen ook. De meeste SPAM houden we aan de mailpoort tegen en volgende week ook. Leer van het verleden: ga na, wat ging er goed en wat niet? En bepaal zo wat je nog moet doen om dichter bij je doel te komen.
4	Wat fott es, es fott	Klaag en treur niet. Het directielid dat na vele awareness sessies eindelijk begrip kreeg voor het belang van security, gaat weg bij het bedrijf. Die ene medewerker, die je zelf opleiding hebt gegeven, stapt op. Accepteer de vergankelijkheid van het leven.
5	Et bliev nix wie et wor	Sta open voor veranderingen. Betrek ook medewerkers van andere bedrijven en organisaties in dezelfde branche, dus met grotendeels dezelfde security-problemen. Richt met collega-bedrijven een ISAC op, om informatie over security te delen en te analyseren.
6	Kenne mer nit, bruche mer nit, fott domet	Kijk goed welke verandering echt de moeite waard is en ook waar het nuttig kan zijn alles te laten zoals het was. Besef: niet alle vernieuwing is ook verbetering.
7	Wat wells de maache?	Leg je neer bij je lot, want soms is de `Schicksal' sterker dan jij. Er zijn situaties in het leven waarin we als mensen, dus ook als security specialisten, min of meer hulpeloos zijn en die we alleen kunnen aanvaarden. Onderzoek wel WAT je er zelf aan kunt doen.
8	Maach et joot, äver nit zo off	Let op je gezondheid als security specialist. Gezondheid - fysiek en mentaal - is onze belangrijkste troef. Drink genoeg water, beweeg (zelfs al is het alleen in de pauze).
9	Wat soll dä Quatsch?	Blijf nieuwsgierig en onderzoek dingen. En blijf vragen: waarom (5x zoals in LEAN) doen we dat zo?
10	Drinks de eine met?	Besteed tijd aan onderhoud van relaties. Ga als security specialist zoveel mogelijk samenwerkingen aan. Binnen je team, binnen je bedrijf, met andere afdelingen, met leveranciers en ook met concurrenten (over security!).
11	Do laachs de disch kapott	Doe het met humor. Relativeer de situatie, overdrijf hem, begrijp het met opzet verkeerd, combineer dingen die eigenlijk niks met elkaar te maken hebben. Zo start je een creatief proces en geef je via de ontstane lachbui ook een positieve impuls aan je eigen ademhaling en die van de omstanders.

Tabel 1 - Dat Kölsche Grundgesetz.

(zaken)leven herkennen in het dagelijkse gedrag van de Keulenaren. Tabel 1 bevat alle wetsartikelen in het Keuls. Hardop lezen, dan kom je een heel eind qua begrip! Pas die artikelen toe in je security-werk is mijn advies. Ik heb er een Nederlandse variant bijgezet om in het werkoverleg of de `dagstart' uitleg te kunnen geven aan niet-ingewijde collega's. En steekwoorden als reminders. Ze zijn ook bruikbaar als u een leukere werk-privé-balans of meer mindfulness zoekt. Of als u meer wilt genieten van het nu en zich geen zorgen wilt maken over de (voor iedereen) onzekere toekomst. En: niet blijven piekeren over gedane zaken en gebeurtenissen in het verleden. De Höhner in hun `Hey Kölle, du bes un Jeföhl' merken daarover terecht op dat de ergernissen van vandaag heel vlug `de goede oude tijd' van morgen zullen zijn!

Geluk gunnen

In de alcoholvrije versie van het Grundgesetz is 10 vervangen door een ander mooi gebod, dat de sfeer en daarmee de samenwerking op een security-afdeling kan verbeteren:
Man muss auch jönne könne
Je moet een ander ook iets gunnen. Verheug je over het geluk van anderen en vermenigvuldig daarmee de bestaande vreugde. Afgunst en jaloezie verwijderen ons alleen van het geluk in ons zelf. Iedereen heeft het recht om geluk en vreugde te ervaren en er ten volle van te genieten. Ook je collega… Alaaf!

IK SWIPE, DUS IK BEN

Nog niet zo lang geleden kreeg ik erg last van mijn rechterpols. Iets teveel en te langdurig met mijn rechterhand mijn telefoon bediend. Noodgedwongen overgegaan op mijn linkerhand, die gelukkig al goed getraind was, omdat ik daar al jaren de nailart op mijn rechterhand mee deed. Probeer maar eens met een dun penseel met je niet dominante hand een cirkel te maken op een heel klein en glad oppervlak. Valt niet mee hè? Het verplicht handen wisselen blijkt een geluk bij een ongeluk, want hierdoor heb ik hopelijk louche appfiguren om de tuin kunnen leiden.

Wat is het geval? Nog niet zo heel lang geleden presenteerde de Australische onderzoeksgroep Data61 CSIRO de uitkomsten van haar onderzoek naar swipegedrag van mobielgebruikers. En wat blijkt? Uit de manier waarop iemand swipet, konden zij met zeer grote mate van nauwkeurigheid de identiteit van de persoon achterhalen. Iedereen heeft namelijk unieke gebruikspatronen. Ben je een tikker? Een tapper? Een veger? Gebruik je beide handen of niet? Hoeveel druk gebruik je? Al deze verschillende bewegingen kunnen met gemak verraden dat jij degene bent die achter de mobiele telefoon zit. En ook of er meerdere personen gebruik maken van hetzelfde apparaat. Het onderzoek is gepubliceerd in het blad Proceedings on Privacy Enhancing Technologies. De uitkomsten en implicaties ervan zijn eigenlijk maar amper in het nieuws geweest.

Veel apps gebruiken technologie om de bewegingen van de gebruikers van hun apps te monitoren. Een appeigenaar wil weten of de app gebruikt wordt, op welke manier en of er ergens iets fout gaat. Daarmee kan ook gekeken worden of de app beter en gebruiksvriendelijker gemaakt kan worden. Op zichzelf is daar natuurlijk niets mis mee, maar gegeven het feit dat handgedrag jou als een persoon kan identificeren, is er sprake van een persoonsgegeven. Daarmee is privacywetgeving onverkort van toepassing. Daarom moet er elke keer, als deze technologie ingezet wordt, ook verteld worden dat dit gebeurt (transparantiebeginsel). Ook moet duidelijk zijn waarom dit gebeurt (doelbinding) en zal er een gerechtvaardigd belang moeten zijn of misschien zelfs wel toestemming (rechtsgrond). Techcrunch deed er onderzoek naar en kwam tot de conclusie dat bij geen van de apps die zij onderzocht gemeld werd dat het gebruiksgedrag gemonitord werd. Ook werd nergens om toestemming gevraagd.

Ik kan me trouwens ook heel goed voorstellen dat dergelijke tech super interessant is voor opsporingsinstanties. Je zou een persoon cross-device kunnen volgen en er zeker van zijn dat je de juiste persoon aan het volgen bent. Het simpelweg wisselen van toestel is dan geen effectieve evasieve manier meer. Ik kan me daarnaast ook heel goed voorstellen dat databases waarin unieke swipe-patronen zijn opgenomen niet alleen zeer interessant zijn voor diezelfde opsporingsinstanties, maar ook voor cybercriminelen. Saillant detail in het onderzoek van Techcrunch: de gegevens die werden opgevangen door het monitoren bevatten bijvoorbeeld ook creditcardnummers. Deze gegevens werden niet op een veilige manier verzonden, waardoor ze door een eenvoudige man-in-the-middle konden worden ondervangen.

Hoog tijd dus om de discussie over de privacy en veiligheid van je swipes te gaan voeren en om actie te ondernemen. In de tussentijd swipe ik vandaag lekker links, morgen rechts en denk ik erover om overmorgen maar weer eens twee handen tegelijk te gebruiken.

Mr. Rachel Marbus
@rachelmarbus op Twitter

INTERVIEW

UITGELICHT: PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

Compliance staat in de belangstelling. Daar heeft GDPR, the General Data Protection Regulation, voor gezorgd. "Niemand kan nog nu ontkennen dat persoonlijke informatie waarde heeft", stelt Gabriel Leperlier, senior manager security consulting EMEA van Verizon. En hij verwijst naar de enorme boetes die de Europese wetgever al heeft opgelegd voor het niet naleven van de nieuwe privacywet. Deze hernieuwde aandacht voor compliance zou volgens de Fransman ook de aandacht binnen bedrijven voor de Payment Card Industry Data Security Standard (PCI DSS) een boost kunnen geven.

De Payment Card Industry Data Security Standard (PCI DSS) is de internationale beveiligingsstandaard die is opgesteld door een samenwerkingsverband van creditcardmaatschappijen. PCI DSS helpt bedrijven die betalingen met creditcards accepteren hun betaalsystemen te beschermen tegen datalekken en diefstal van gegevens van kaarthouders. Elk bedrijf dat creditcardbetalingen accepteert dient jaarlijks PCI DSS-compliance aan te tonen. Ondernemingen met meer dan zes miljoen kaarttransacties per jaar moeten elk jaar een audit op locatie laten uitvoeren door een QSA, Qualified Security Assessor. Dit geldt ook voor bedrijven die door een creditcardmaatschappij zijn aangemerkt als 'Level 1 merchant'. Voor andere bedrijven geldt dat zij een online vragenlijst (self assessment) in moeten vullen in combinatie met netwerkscans om zo aan te tonen dat ze compliant zijn. Meer informatie: pcisecuritystandards.org.

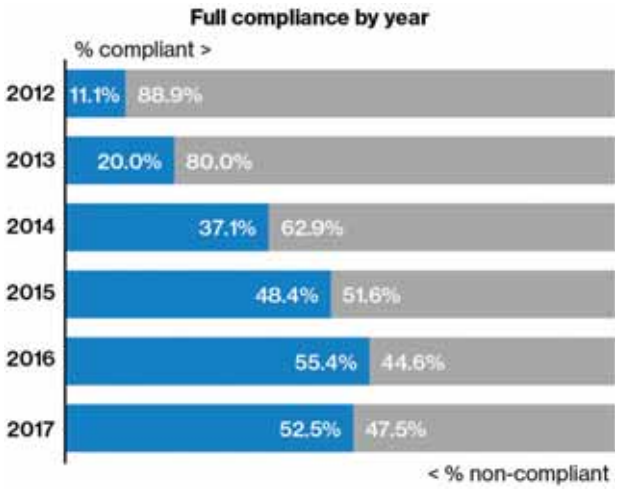
"Creditcardgegevens zijn immers ook persoonsgegevens", aldus Leperlier. Of er binnen bedrijven echter meer duurzame aandacht zal komen voor de PCI-standaard, vindt hij moeilijk te zeggen. Leperlier realiseert zich namelijk dat sommige bedrijven compliance blijven zien als 'checkbox management'. Dat meer duurzame aandacht voor PCI DSS nodig is, blijkt volgens hem uit het onderzoek dat Verizon elk jaar doet naar PCI DSS-compliance bij bedrijven. Onderzoek dat uitmondt in het jaarlijks Payment Security Report (PSR).

Minder bedrijven voldoen aan PCI-standaard

Uit het meest recente rapport, dat vorig jaar september verscheen, blijkt voor het eerst in zes jaar een daling wereldwijd van het aantal bedrijven dat PCI DSS-compliant is. Van alle bedrijven die in 2017 door Verizon op de PCI-standaard werden getoetst, bleek 52,5 procent PCI DSS-compliant. In 2016 was dat nog 55,4 procent.
"Let wel", gaat Leperlier verder. "Die 52,5 procent is het percentage bedrijven dat volledig voldoet aan de standaard nadat wij een eerste toets hebben gedaan en we bedrijven vervolgens nog één tot twee maanden de tijd hebben gegeven de puntjes op de 'i' te zetten. Zouden bedrijven die kans niet krijgen dan zou geen enkel bedrijf voldoen aan álle eisen van de PCI-standaard."

Kwetsbaar

Op basis van eerdere onderzoeken, de Data Breach Investigations Report-serie, concludeerde Verizon dat naleving van de PCI DSS eraan bijdraagt dat betaalsystemen beter beschermd worden tegen zowel datalekken als diefstal van kaarthoudergegevens. Dat in 2017 minder bedrijven voldeden aan de standaard noemt het bedrijf dan ook 'alarmerend'.
In het 2015 Payment Security Report – het rapport is inmiddels zeven keer verschenen – stelde Verizon: 'Compliant zijn, betekent niet dat een organisatie veilig is. Maar het feit dat een bedrijf níet voldoet aan de compliancy-eisen, is een behoorlijk sterk signaal dat het kwetsbaar is'. Een conclusie die Leperlier, die zelf als QSA (Qualified Security Assessor) PCI DSS-audits uitvoert, nog altijd onderstreept.
Hij denkt niet dat de daling van het aantal bedrijven dat volledig aan de PCI-standaard voldoet, te maken heeft met een 'lack of awareness'. "Veel eerder met een lack of



Figuur 1 – Full compliant by year

Tom Bakker is redacteur van iB Magazine. Tom is te bereiken via tombakker@pvib.nl

Sandra Kagie is freelance tekstschrijver/journalist. In het verleden is zij als eindredacteur nauw betrokken geweest bij iB-magazine. Ze is te bereiken via info@sanscriptoducties.nl.

resources", geeft hij aan. "Veel bedrijven zijn ooit een traject gestart om te voldoen aan de beveiligingsstandaard. Wanneer ze eenmaal het stempel 'compliant' hebben, dan is het in veel gevallen klaar. Er worden vervolgens geen mensen meer vrijgemaakt om de PCI-standaard intern te monitoren en te handhaven. Soms een kwestie van budget. Maar ook ontbreekt binnen veel organisaties de benodigde kennis en kunde."

Langere termijn

Om bedrijven toch vooral op het hart te drukken dat het blijven voldoen aan de PCI-standaard 'nooit klaar is', worden in het 2018 Payment Security Report negen factoren genoemd die ervoor zorgen dat een PCI-traject niet alleen leidt tot compliant zijn op het moment van de jaarlijkse audit, maar juist tot een breder, meer robuust compliance-programma op de langere termijn.
Een programma waarin gegevensbescherming in zijn algemeenheid centraal staat en niet puur het voldoen aan de PCI-standaard. De nadruk hierbij moet volgens Leperlier liggen op doorlopend toezicht en op regelmatige meting. Hij noemt vervolgens patchmanagement en vulnerability management als belangrijke aandachtpunten. Dat zijn volgens hem binnen veel bedrijven en organisaties zwakke punten die tot problemen kunnen leiden.
Het inbedden van het voldoen aan de PCI-standaard in een breder security-programma, is dus het advies van Leperlier: "Bedrijven hebben met zoveel IT-security standaarden te maken. En in die standaarden zit overlap. Door verschillende standaarden en audits niet steeds als losstaande gebeurtenissen te zien, maak je als organisatie op een slimme manier gebruik van die overlap. "
Een bedrijf dat zijn zaakjes goed op orde heeft, zou volgens Leperlier elk kwartaal een 'clean scan' moeten kunnen laten zien. Een pentest een keer per jaar is wat hem betreft niet voldoende. "Wat zegt zo'n test?", vraagt hij zich af. "Okay today, but what about tomorrow?"
Figuur 2 laat zien wat volgens Verizon de negen factoren zijn die bepalen of er binnen een bedrijf sprake is van een robuust en effectief securityprogramma: factor 1, het documenteren van de controleomgeving, is de kern waaruit de andere factoren voortkomen. Nadat de doelstellingen van de voorgaande factoren zijn bereikt, is het uiteindelijke resultaat het vermogen tot zelfbeoordeling. De output hiervan kan vervolgens worden gebruikt om alle andere factoren continu te verbeteren.

Figuur 2
Het negen-factorenmodel

Afbakening

Om de weg naar compliance te vereenvoudigen en de kosten te beperken, adviseert Leperlier de scope van een PCI-compliance-traject zoveel mogelijk te beperken. Het is vaak het eerste advies dat hij bedrijven en organisaties geeft wanneer ze hem vragen hoe ze een compliance-traject in het kader van PCI DSS het beste kunnen aanpakken. "Om de scope te bepalen, moet je die systemen die creditcardgegevens bevatten en alles en iedereen die hier direct mee communiceert, scheiden van de systemen waarvoor dit niet geldt", legt hij uit. "Een afbakening die heel helder moet zijn. Ik hoor wel eens: 'maar de gegevens waar het om gaat, staan bij ons maar op één server'. Vervolgens vergeet een bedrijf dataflows als e-mail, webmail, databases of bepaalde logs. En dan gaat het mis." Ook komt het volgens Leperlier regelmatig voor dat een bedrijf denkt zelf niks te hoeven doen omdat ze samenwerken met een Payment Server Provider. "Onze scope is '0', want we slaan zelf geen gegevens op, wordt dan gezegd. De redirection server wordt in zo'n geval echter gemakkelijk over het hoofd gezien", waarschuwt hij. "Is deze redirection server echter niet-secured dan is een bedrijf kwetsbaar voor bijvoorbeeld een man-in-the-middle-attack."

Duurzaam onderhouden

Waren de Payment Security Reports voorheen volgens Leperlier vooral gericht op het 'waarom' van PCI DSS en ook op de vraag 'hoe je als organisatie PCI-compliant wordt'. Nu ligt wat hem betreft de focus op het duurzaam onderhouden van de PCI-standaard en op het inbedden van de standaard in een breder security-programma. Een continu proces dat je wat hem betreft niet af kunt doen met 'checkbox management'. Niet wanneer je als bedrijf of organisatie gegevensbescherming daadwerkelijk serieus neemt. Het complete 2018 Payment Security Report is te vinden op de website van Verizon: https://enterprise.verizon.com/resources/reports/payment-security/2018/

ACCOUNTABLE

There is currently a disagreement about cybersecurity and privacy at The Walt Disney Company. It raises the issue of accountability of the Board with respect to the shareholders.
Accountability is an important concept in today's business world. It is one of the key elements of the RACI method of analysing stakeholder relationships and carries a great deal of moral weight in corporate governance frameworks. Let's first examine what the dictionaries tell about this attribute: Accountable: required or expected to justify actions or decisions; responsible, liable, answerable, chargeable, to blame for failures. An example: 'Ministers are accountable to Parliament.' Another example: 'The government was held accountable for the food shortage.' Now let's look at what is going on at Walt Disney. Their corporate website tells us who and what they are:
'The mission of The Walt Disney Company is to be one of the world's leading producers and providers of entertainment and information. Using our portfolio of brands to differentiate our content, services and consumer products, we seek to develop the most creative, innovative and profitable entertainment experiences and related products in the world.'
'Disney's leadership team manages the world's largest media company and are the visionaries behind some of the most respected and beloved brands around the globe. Their strategic direction for The Walt Disney Company focuses on generating the best creative content possible, fostering innovation and utilizing the latest technology, while expanding into new markets around the world.'

What we learn from this is that the Disney enterprise is a global media company, dealing primarily in published information of various types, including a lot of digital entertainment products. We also note their commitment to deploying the latest technology. It is pretty clear to The Attributer that this is a description of Disney's core business. Its value chains are based on the activities mentioned in these statements of vision, mission and leadership.

Disney already has a scheme linking executive compensation to various performance metrics, including information security management. There is trouble now because some shareholders have come forward with a proposal that this should be extended to include cybersecurity and data privacy explicitly, to focus the company's attention on these modern emerging security issues. Their supporting statement for their proposed resolution at the 2019 stock holders' meeting reads:
'Disney links senior executive compensation to various performance metrics, including information security metrics. Cybersecurity and data privacy are vitally important issues for Disney and should be integrated as appropriate into senior executive compensation to incentivise leadership to reduce needless risk, enhance financial performance, and increase accountability. Rewarding executives for risk mitigation as well as growth generation will better position Disney as a trusted brand.'
What can we determine from this shareholder proposal? It seems to The Attributer that this group of shareholders believes that at Disney the SABSA Risk Balance is out of kilter. There is too much focus on exploiting opportunities without sufficient attention to mitigating threats. And yet in this very same industry in 2011 Sony suffered an outage on its PlayStation Network as a result of an 'external intrusion' (that's Sony-speak for 'hack'). The personal details from approximately 77 million accounts were compromised and PlayStation users were prevented from accessing the service.

You might think therefore that the Disney Board would be grateful for the prompt from the shareholders. You would be wrong. The Board has advised shareholders to vote against the proposal.
Board Recommendation: *'The Board recommends that you vote against this proposal because it is unnecessary and would not promote enhanced protection of data security and data privacy.'*
Wow! So, there is to be a head-on collision at the 2019 meeting, in which the Board does not want to extend its accountability in this area. What could be their motives? Perhaps the lawyers are advising that the more they publish about how they manage privacy and cybersecurity, the more they are likely to be held liable (accountable) for any breaches – i.e. failures. Also, what effect would a reported breach have on the share price? Or is it merely the case that the Board believes that cybersecurity and privacy are technical issues, nothing to do with the core business, owned by the CISO? If that is so, then they are sorely out of touch with modern thinking. Cyber risk in a digital information company is a core business risk. Perhaps someone should introduce them to SABSA – a business driven approach to cyber risk management.

The Attributer

PRIVACY & INFORMATIEBEVEILIGING: DE TRENDS VOOR 2019

Data privacy staat volop in de belangstelling. Sinds mei 2018 is de Algemene Verordening Gegevensbescherming (AVG of GDPR) van kracht. Ook de e-Privacy Verordening (ePV) komt eraan, al duurt het mogelijk nog tot mei 2020 voordat deze aanvulling op de AVG echt in werking zal treden.

Door de AVG worden onze persoonsgegevens weliswaar beter beschermd, maar veel bedrijven worstelen nog met alle noodzakelijke maatregelen. Datalekken zijn aan de orde van de dag en de Autoriteit Persoonsgegevens laat steeds vaker van zich horen via controles, dwangsommen of boetes.

De AVG/GDPR vraagt om een integraal geborgd proces. Om compliant te worden en te blijven, moeten de onderwerpen privacy en informatiebeveiliging goed verankerd zijn in het beleid van de organisatie. Ook moet er voldoende draagvlak bij medewerkers zijn. Als Data Protection Officer (DPO), Chief Information Security Officer (CISO), Privacy Officer (PO) of Functionaris Gegevensbescherming (FG) heb je dus de zware taak meer bewustwording te creëren voor het belang van privacy en informatiebeveiliging in alle lagen van de organisatie. Hoe maak je deze verantwoordelijkheid waar?

Voor 2019 zien wij de volgende trends:

1. Maak het praktisch voor de werkvloer met behulp van digitalisering

Werknemers hebben moeite met ingewikkelde juridische of technische maatregelen: zij willen vooral weten waar ze concreet rekening mee moeten houden. Dat vraagt om een goede vertaling van de wetgeving naar de dagelijkse werkpraktijk en een slimme manier om de informatie te verspreiden. Eenmalige bewustwordingsprogramma's zijn daarvoor weinig effectief. Het werkt beter om de werkvloer regelmatig te laten stilstaan bij wat ze praktisch kunnen doen en waarom dat belangrijk is. Met online self-assessments sla je twee vliegen in een klap: medewerkers krijgen inzicht in (het waarom van) de maatregelen én toetsen zichzelf in de mate waarin ze al in control zijn. Meer resultaat met minder moeite dus. Dat is waar digitalisering voor bedoeld is!

2. Zoek de feedback op

Met self-assessments kunnen beleidsvisies en -maatregelen worden gekoppeld aan uitdagingen voor de werkvloer. Een dergelijke evaluatie is tevens een ideaal startpunt om een feedbackloop op gang te brengen die organisaties helpt om continu verbeterslagen te maken. De praktijk laat zien dat mensen hun eigen gedrag in een self-assessment kritischer beoordelen dan via traditionele audits. Een positief neveneffect is dat de werkvloer de uitkomsten ook in een team kan bespreken; deze ervaringen kunnen vervolgens weer op beleidsniveau worden meegenomen. Op die manier stimuleren organisaties een enorm verbeterpotentieel en handelen medewerkers steeds meer in lijn met de wet. Een prettige gedachte.

3. Kijk verder dan privacy champions

Self-assessments kunnen onder een groot deel van de medewerkers worden uitgezet. Het is ook mogelijk om gebruik te maken van privacy champions, die de toetsvragen invullen en in hun teams bespreken. Zorgvuldigheid is hierbij wel geboden. Bij een sterke focus op privacy champions (of initiatieven zoals 'de privacymedewerker van de maand') ontstaat het risico dat andere medewerkers gedemotiveerd raken. Uit Organisational Behaviour Management weten we dat belonen beter werkt dan straffen. Wie alleen de koplopers beloont, zegt daarmee impliciet dat anderen verliezers zijn - en zo geef je hen eigenlijk een straf in plaats van een positieve stimulans. Zorg er dus voor dat je ook degenen die nog niet zo hoog scoren bedankt voor hun medewerking en prestatie. Elke kleine verbeterstap is er één.

4. Zie privacy als nieuwe kwaliteitsnorm

Privacy en informatiebeveiliging zijn nieuwe onderdelen van de kwaliteitseisen waarmee elke organisatie rekening moet houden. Het creëren van bewustwording is best een flinke klus. Maar wie aansluiting zoekt bij wat er al is - bijvoorbeeld op het vlak van kwaliteit en veiligheid - kan er makkelijker mee aan de slag, zonder dat het voor de werkvloer een extra opgave wordt. Bedenk daarbij dat het eigenlijk heel normaal is dat we goed omgaan met persoonsgegevens. Het hoort anno nu bij maatschappelijk verantwoord ondernemen. Als je deze boodschap aan de werkvloer kunt overbrengen, heb je direct een voedingsbodem voor goede naleving. Iedereen wil graag werken zonder dat er kinderarbeid of milieuschade bij komt kijken - en dus ook zonder dat de bescherming van persoonsgegevens onder druk staat. Zo wordt de AVG ineens heel logisch.

smile

SMILE

De passie van SMILE is om mensgerichte visie op kwaliteit & veiligheid; privacy & informatiebeveiliging; en governance, risk & compliance te verbinden met nieuwe technologie. Hiermee wil SMILE een positieve bijdrage leveren aan de maatschappij. Meer informatie is te vinden te vinden op: www.smile.nl

STUDENTEN TREDEN IN VOETSPOREN CYBERCRIMINEEL OM MEER INZICHT TE KRIJGEN IN SOCIAL ENGINEERING

Social engineering is een techniek die veel gebruikt wordt door cybercriminelen. Door het slinks toepassen van beïnvloedingstechnieken op medewerkers kunnen die verleid worden om gevoelige informatie prijs te geven. In dit artikel beschrijven we de resultaten van 98 social engineeringsaanvallen op organisaties, verricht door studenten van de Haagse Hogeschool. Dit geeft meer inzicht in de kwetsbaarheden, wat kan helpen meer cyberweerbaar te worden.

Cybercrime is een veel voorkomende vorm van criminaliteit. Hacken komt bijvoorbeeld vaker voor dan fietsendiefstal (respectievelijk 4,9 en 4 procent (1)). Het gedrag van mensen wordt steeds vaker erkend als belangrijke risicofactor bij cybersecurity (2). Een schatting van Ernst en Young (3) is dat 83 procent van alle cyberincidenten te wijten is aan menselijk handelen. Cybercriminelen richten zich in hun aanvallen dan ook vaak op 'de mens'. Met behulp van allerlei verleidingstechnieken proberen ze medewerkers aan te zetten tot het uitvoeren van onveilige handelingen, zoals het invullen van gegevens op een phishingwebsite of het klikken op een link met een malwarebesmetting tot gevolg. Deze misleiding wordt ook wel social engineering genoemd. Door de medewerker te misleiden kunnen technische en fysieke beschermingsmaatregelen worden omzeild (4) (5).

Maatregelen

Organisaties – de kleinere organisaties vaker dan de grotere – hebben te weinig kennis en mogelijkheden om zich te wapenen tegen dergelijke aanvallen. Enkele technische basismaatregelen (zoals up-to-date software en een virusscanner) nemen ze vaak nog wel, maar maatregelen die medewerkers bewust moeten maken van cybergevaren, trainingen of scenario's 'Wat te doen bij een cyberaanval?' ontbreken (6). Het ontbreekt bij organisaties dus vaak aan middelen om social engineering tegen te gaan. Kennis over social engineering kan een belangrijke eerste stap zijn in het treffen van effectieve maatregelen. Belangrijke vragen hierbij zijn: Hoe gaan social engineers te werk? Hoe kunnen we social engineering ondermijnen? Welke kenmerken maken een organisatie of medewerker beïnvloedbaar?

Om organisaties te helpen aan inzicht in de eigen beveiliging en om kennis op te bouwen over social engineering voeren studenten HBO Informatie Communicatie Technologie (ICT) van de Haagse Hogeschool (HHS) jaarlijks social engineeringsaanvallen uit op organisaties. Studenten gaan in de schoenen van de cybercrimineel staan en proberen, door het beïnvloeden van medewerkers, toegang te verkrijgen tot gevoelige informatie. Zowel online, telefonisch als fysiek. Hierdoor leren studenten hoe social engineeringsaanvallen werken en hoe je mensen kunt beïnvloeden, zodat zij als toekomstig professional beter in staat zijn om zich te wapenen tegen cyberaanvallen. Bovendien maakt het de meewerkende bedrijven bewust van de gevaren van social engineeringsaanvallen. In dit artikel beschrijven we de onderliggende psychologische mechanismen van social engineering en presenteren we de resultaten van dertig groepen die in totaal 98 aanvallen op organisaties hebben uitgevoerd tussen 2015 en 2018.

Een kwetsbaarheid is vaak het onbewuste, onveilige gedrag van de medewerkers. Dit is meteen wel een lastige, ogenschijnlijk ongrijpbare schakel, want er kunnen vele oorzaken zijn van cyberonveilig gedrag. In dit artikel richten we ons op een onderdeel hiervan, namelijk: het verstrekken van of (indirect) toegang verschaffen tot gevoelige gegevens aan onbevoegden.

Onbewust automatisch gedrag

Het is van belang om te weten dat mensen vuistregels gebruiken om snel een probleem op te lossen, of een beslissing te nemen in de overdaad van beschikbare informatie (7). Beslissingen worden vaak genomen op basis van één kenmerk van de situatie. Dit wordt 'selectieve perceptie' genoemd. Vuistregels zijn noodzakelijk om te kunnen functioneren en het gebruik ervan is doorgaans een onbewust proces. Volgens Kahneman (7) is het grootste gedeelte (95%) van het menselijk gedrag automatisch en irrationeel. Slechts een beperkt gedeelte van ons gedrag is dus bewust beredeneerd. De mens gedraagt zich dan ook voorspelbaar irrationeel als het aankomt op het maken van afwegingen en keuzes (8). We willen dat keuzes ons zo gemakkelijk mogelijk worden gemaakt en we kiezen bij voorkeur voor routinematige oplossingen. En dat is, rationeel gezien, lang niet altijd de meest gunstige keuze. Overigens nemen mensen doorgaans prima beslissingen op basis van deze vuistregels, maar omdat ze automatisch en irrationeel zijn, kunnen ze worden misbruikt door cybercriminelen.

Michelle Ancher is docent bij de opleiding HBO ICT (richting Information Security Management) en onderzoeker bij het lectoraat 'Cybersecurity in het mkb' van de Haagse Hogeschool. Michelle is sociaal psycholoog en richt zich op de menselijke factor van de information security. Ze is bereikbaar via m.ancher@hhs.nl

Cybercriminelen maken gebruik van verleidingstechnieken om mensen te overtuigen om bepaalde regels te omzeilen. Een voorbeeld: als een aanvaller zich voordoet als directeur (een autoriteit) en verzoekt om vertrouwelijke data, dan zijn mensen sneller geneigd om dit te doen dan wanneer een collega of onbekende dit vraagt.

Beïnvloedingsprincipes

Gedrag is dus in de regel automatisch en kan beïnvloed worden door cybercriminelen. Er bestaan verschillende beïnvloedingsmechanismen, veelal gebaseerd op fundamentele psychologische mechanismen (9) (10).

De verleidingstechnieken van Cialdini (11) worden in marketing en (ook met succes) door social engineers gebruikt (9). Cialdini (11) beschrijft zes manieren van beïnvloeding:

- wederkerigheid (de neiging iets terug te doen als iemand ons iets geeft);
- sympathie (sneller iets aannemen van iemand die we aardig vinden, die op ons lijkt);
- sociale bewijskracht (iets doen omdat anderen dat ook doen);
- autoriteit (de neiging om de expert te volgen);
- commitment & consistentie (de neiging om consistent te blijven bij wat we eerder hebben gezegd of gedaan);
- en schaarste (iets graag willen omdat het beperkt beschikbaar is).

In het principe van schaarste zie je de theorie van 'loss aversion' (12) terug. Dit is het fenomeen dat veel keuzes niet gebaseerd zijn op rationeel de beste optie zoeken, maar op de gedachte dat verlies vermijden belangrijker is dan winst behalen. Bij schaarste zijn we bang om iets mis te lopen. Deze angst zorgt ervoor dat we niet geheel rationeel meer nadenken. Een voorbeeld: de aanvaller die zich voordoet als ICT-medewerker en verzoekt om inloggegevens, omdat anders de toegang tot de werkbestanden geblokkeerd wordt.

Daarnaast blijkt een effectieve overtuigingstechniek het zogenoemde 'distraction' (9). Dit is het afleiden van een persoon door het aanwakkeren van emoties, zoals verrassing, gejaagdheid, angst of paniek. Dit principe gebruiken criminelen om ervoor te zorgen dat personen aan een verzoek voldoen, terwijl in een 'normale' situatie die persoon dat niet zou doen (10).

Ook de sociale omgeving is een belangrijke bepalende factor van gedrag (13). De cultuur in een organisatie en bijbehorende kernwaarden bepalen voor een groot deel hoe medewerkers communiceren en hoe ze omgaan met afspraken, regels, onderlinge feedback, verantwoordelijkheden en missers. De bedrijfscultuur kan afbreuk doen aan de cyberveiligheid: een leider die zelf niet volgens de veiligheidsvoorschriften werkt, of collega's die niet veel oog hebben voor veiligheid. Ook de sector, de grootte van de organisatie (hoe meer mensen des te groter de kans op fouten) en het ontwerp van de fysieke en technische omgeving (14) hebben hun weerslag op het gedrag van medewerkers (15).

Methode

Dit artikel beschrijft een verkennend onderzoek naar vatbaarheid van organisaties voor social engineeringsaanvallen. De groepen studenten waren vrij om, in samenspraak met de opdrachtgever, een concrete invulling te geven aan het opzetten van de aanvallen, het gebruik van verleidingstechnieken en het selecteren van doelobjecten.

In totaal werden 98 aanvallen uitgevoerd op dertig organisaties. De meeste organisaties deden mee via het netwerk van de HHS. Die organisaties werden benaderd door docenten en onderzoekers. Ook benaderden organisaties de HHS zelf, omdat ze via-via gehoord hadden van de mogelijkheid om deel te nemen. Er deden organisaties mee uit diverse sectoren, zoals de overheid, de zorg, de financiële sector en diverse mkb-bedrijven, zoals softwareontwikkelaars, grafische- en metaalbedrijven.

Drie typen social engineeringsaanvallen werden gebruikt: 1. fysiek, 2. telefonisch (vishing) en 3. digitaal (phishing). Studenten bepaalden met de opdrachtgever wat voor type gevoelige informatie er bemachtigd ging worden. Variërend van elektronische dossiers tot inloggegevens van medewerkers. Bij de aanval richtte de student zich op een bepaald doelobject, in feite de sleutel tot de gevoelige informatie: een medewerker (in totaal 71 keer), een locatie, zoals het hoofdkantoor en daarbinnen de serverruimte (38 keer) of een object, zoals een usb-stick (4 keer).

Bij de fysieke aanval probeerden studenten op de locatie van de organisatie toegang te verkrijgen door (a) gewoon naar binnen te lopen, al dan niet met een medewerker (het zogeheten 'tailgating'), of (b) via interactie met een medewerker door zich voor te doen als iemand anders (bijvoorbeeld als auditor of stagiair facility management). Een enkele keer werd er (c) een usb-stick neergelegd om te kijken of een medewerker deze in een pc zou plaatsen.

De telefonische aanvallen waren gericht op een bepaalde persoon of afdeling voor het verkrijgen van: (1) klant- of organisatiegegevens zoals rekening- of uitkeringsgegevens,

(2) inloggegevens van medewerkers en/of (3) contactgegevens van medewerkers.

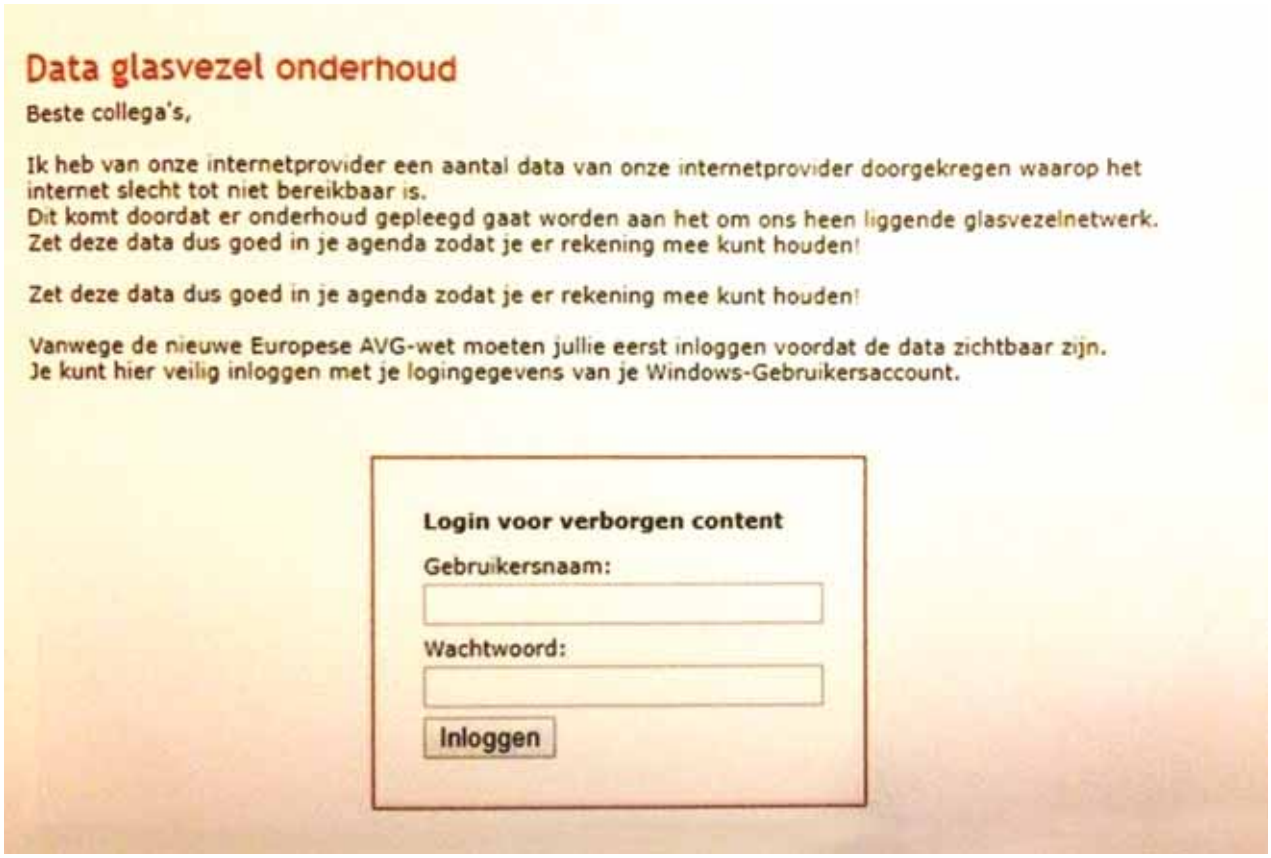
Bij de digitale social engineeringsaanvallen werden medewerkers verleid tot het aanklikken van een link in een phishingmail of tot het prijsgeven van gevoelige data via e-mail. Een voorbeeld: studenten stuurden een e-mailbericht (zogenaamd afkomstig van de directeur) met een hyperlink en het verzoek om via de hyperlink mee te doen aan een werktevredenheidsenquête. In werkelijkheid deden de medewerkers dan niet mee aan een enquête, maar werden ze omgeleid naar een phishingwebsite.

Fasen onderzoek

Studenten gingen volgens de 'social engineering attack lifecycle' (16) te werk. In de eerste fase, het vooronderzoek, brachten ze de specifieke organisatiecontext in kaart middels deskresearch, het afnemen van een cultuurscan (17) en het observeren van de (sociale) omgeving van de organisatie. Hiervoor hadden ze ongeveer 5 dagen. Vervolgens selecteerden ze een doel en één of meer overtuigingsprincipes van Cialdini (11). Het tijdstip van de aanval kon als hefboom fungeren. Bijvoorbeeld met Valentijnsdag een e-card met phishinglink versturen. Met deze input ontwierpen de studenten een aantal aanvalsscenario's (fase 2) waaruit ze de meest kansrijke kozen en de interactie aangingen met medewerkers van de organisatie (fase 3). Ze rondden de aanval af (fase 4) door de organisatie te verlaten en de opdrachtgever te informeren.

De studenten hielden zich bij de aanval aan de wet- en regelgeving. Vernieling of identiteitsfraude was bijvoorbeeld niet geoorloofd. Dat werd door de opdrachtgever en een coach van de HHS gecontroleerd. Echter, in overleg met de opdrachtgever mochten studenten wel bepaalde interne bedrijfsregels overtreden (bijvoorbeeld zichzelf toegang verschaffen tot een bedrijfsruimte) of het sturen van een phishingmail naar medewerkers. In het geval van een fysieke social engineeringaanval hadden de studenten een vrijwaringsverklaring bij zich, mochten ze ontmaskerd worden.

Om de opdrachtgever een garantie te geven dat er betrouwbaar met hun gegevens werd omgesprongen,



tekenden de studenten een geheimhoudingsverklaring. Dat betreft alle gevoelige informatie die ze zouden aantreffen bij het bedrijf. Ze stelden een protocol op voor de omgang met vertrouwelijke informatie, een ethische gedragscode en legden een Verklaring Omtrent Gedrag (VOG) voor.

Tijdens de aanval verzamelden de studenten gegevens door bijvoorbeeld het doen van observaties; het vastleggen van bewijslast op beeld of in gespreksverslagen; en door het loggen van het aantal clicks op een phishingmail. Studenten rapporteerden de geanonimiseerde resultaten aan de opdrachtgever en deden aanbevelingen voor verbeteringen. Na afloop vernietigden ze het eventueel verkregen bewijsmateriaal.

Het bleek dat bijna de helft van de aanvallen die de studenten uitvoerden succesvol was. Gelukkig voor de meewerkende organisaties lukken aanvallen lang niet altijd, maar het is opvallend dat de aanvallen van de studenten zo'n aanzienlijk succespercentage hadden.

Fysieke aanval

Van de in totaal 39 fysieke aanvallen waren er 22 succesvol (56%). Dit gebeurde door `gewoon' binnenlopen en middels tailgating (59% succesvol). Of door toegang te vragen bij de receptie door zich voor te doen als iemand anders, bijvoorbeeld als onderhoudsmedewerker van de koffieautomaat (53% succesvol). Bij drie van de vier aanvallen waar een usb-stick was achtergelaten, werd de usb-stick door de receptie of een medewerker in een pc gestoken. Bij geslaagde aanvallen werden niet gelockte computers aangetroffen en dikwijls vertrouwelijke gegevens (bijvoorbeeld een lijst met ID-gegevens). Ook lukte het in vier gevallen om toegang te krijgen tot een serverruimte. Het was de aanvallers niet gelukt om via een fysieke aanval inloggegevens te bemachtigen.
Eén derde van de aanvallers kon vrij in het gebouw rondlopen. Hierbij werden ze, op twee gevallen na, wel door een medewerker aangesproken wat ze kwamen doen. Met een smoesje kwamen de meesten hiermee weg, maar niet iedereen. Zij werden geverifieerd bij de receptie en vielen door de mand. Sympathie (de vriendelijke student die zich voordoet als zoon van een medewerkster en haar werkplek wil versieren voor haar verjaardag), autoriteit (veiligheidsinspectie of afspraak met de manager) en distraction (met een grote taart door de toegangspoort lopen) werden met succes toegepast (respectievelijk 8, 4 en 2 keer).

Een voorbeeld van een succesvolle fysieke aanval was dat studenten met een taart een toegangssysteem wisten te omzeilen. De opdrachtgever dacht dat de fysieke toegang ondoordringbaar was. De studenten deden zich voor als medewerkers van een andere locatie en liepen met de taart middels tailgating met een medewerker mee. Eenmaal binnen ging één student op onderzoek uit, terwijl de anderen met de taart voor afleiding zorgden bij het personeel door de taart te geven. Ze hadden zich van tevoren goed verdiept in de organisatiecultuur. "We kwamen erachter dat dit een trots bedrijf is dat overal zijn logo op plakt en graag successen deelt. Daarom kozen we voor een taart met daarop het logo en een felicitatie van een andere afdeling", aldus één van de studenten.

Bij de niet-succesvolle aanvallen liet de receptie de aanvaller zonder afspraak niet binnen of werden de aanvallers netjes begeleid door het pand. De medewerkers hielden zich aan het protocol en checkten in vijf gevallen de afspraak. Sympathie en autoriteit werden hier in drie gevallen zonder succes toegepast. In één geval werd de student aangesproken door een beveiligingsmedewerker: "Het viel hem op dat ik geen Apple-laptop had, terwijl iedereen daar met een Apple werkt."

Telefonische aanval

De telefonische aanvallen (33 totaal) waren minder succesvol (30% geslaagd). Telefonisch lukte het in 25% van de (8) gevallen om inloggegevens te krijgen. Dit gebeurde doordat de aanvaller zich voordeed als ICT-medewerker of als medewerker die niet kon inloggen. Hier werd het principe schaarste (tijdsdruk) gebruikt en autoriteit (ICT-medewerker met kennis van zaken). In de andere gevallen lukte het niet om inloggegevens te bemachtigen. De aanvaller werd wel geloofd, maar de medewerker hield zich aan het protocol, bijvoorbeeld door naar de identiteit van de beller te vragen. Ook de medewerkers die kennis van ICT hadden en doorvroegen, bijvoorbeeld over het zogenaamde netwerkprobleem dat er zou zijn, trapten er niet in. Twintig procent van de aanvallen op klant- of organisatiegegevens (12) slaagden met name door gebruikmaking van sympathie en wederkerigheid. Een aanvaller deed zich voor als samenwerkingspartner van de organisatie met de vraag om een relatiegeschenk te sturen naar de directeur. Ook werd distraction toegepast. De aanvaller vertelde als zogenaamd familielid dat er een misdrijf gepleegd was bij een klant (opwekken van afschuw). Bij de aanvallen waar gevraagd werd om contactgegevens (13), informatie die vervolgens gebruikt zou kunnen worden voor een gerichte aanval, slaagden er vijf en werden e-mailadressen of telefoonnummers van medewerkers gegeven. De gebruikte overtuigingsprincipes waren hier heel divers.

Een voorbeeld van een telefonische aanval is een student die zich voordeed als ICT-medewerker om inloggegevens te verkrijgen voor een elektronisch dossier. Tijdens het vooronderzoek waren gegevens van een medewerker gevonden die bevoegd was in het elektronisch dossier te werken. Ook was de naam bekend van het externe ICT-bedrijf waar de organisatie mee werkt. Er waren eerder die week al storingen geconstateerd op het netwerk, werd door de opdrachtgever verteld.
De aanval verliep als volgt: via de receptie kreeg de student in de rol van ICT-medewerker (autoriteit) de medewerker aan de lijn en legde uit dat er een dubbele loginactiviteit was gemonitord en dat een aantal andere medewerkers ook moeite hadden met inloggen (sociale bewijskracht) en gebeld waren. Voorstel was om het wachtwoord direct te wijzigen (schaarste in tijd) middels hard resetten. Het verhaal van de ICT-medewerker werd geloofd. Alleen wilde de medewerker het wachtwoord niet telefonisch doorgeven, maar stelde voor om zelf het wachtwoord te wijzigen.

Digitale aanval

Van de in totaal 26 digitale aanvallen waren er 12 succesvol (46%). Achttien aanvallen waren gericht op het laten klikken op een phishinglink, waarmee het slachtoffer malware binnen kon halen (50% succesvol). Acht aanvallen waren gericht op het verkrijgen van data van met name persoonlijke- of inloggegevens (38% succesvol).

Een succesfactor bij de digitale aanvallen is het gebruik van het principe van autoriteit (7), bijvoorbeeld doordat iemand zicht voordoet als ICT-medewerker of manager. De combinatie met sympathie blijkt volgens Ferreira nog effectiever te zijn. Dit is terug te zien bij elk van de drie aanvallen. Bij het niet-slagen was de diversiteit van gebruik van overtuigingstechnieken in de scenario's groot - wederkerigheid (2), commitment en consistentie (3) en autoriteit (7) - en is de reden lastiger te achterhalen.

Een voorbeeld van een geslaagde phishingaanval was de e-mail aan medewerkers over glasvezelnetwerkonderhoud. De mail was zogenaamd afkomstig van de directeur (principe van autoriteit) met het bericht dat ze de onderhoudsdata in hun agenda moeten zetten om problemen te voorkomen. Deze data kunnen ze zien door op een link te klikken waar ze moeten inloggen met hun account vanwege de nieuwe AVG-wet (weer autoriteit). Uit vooronderzoek kwam de opvallende schrijfstijl van de directeur, die elke zin op een nieuwe regel zet. Er is gebruik gemaakt van een domeinnaam die erg lijkt op die van de organisatie, een kopie van de website van de organisatie en een extra pagina met een loginveld.
Het resultaat was dat van de 150 e-mails er 56 zijn aangekomen. Er hebben vijftien van de 56 medewerkers op de link geklikt. Vervolgens hebben acht medewerkers hun inloggegevens ingevuld. Drie van deze medewerkers hebben dit gemeld. Voor de organisatie zijn dit acht inlogcombinaties teveel. Immers, één is al genoeg om het systeem te compromitteren.

Conclusie

Cybercrime is inmiddels een veelvoorkomende vorm van criminaliteit en organisaties hebben iedere dag te kampen met cyberaanvallen. Aanvallen richten zich daarbij vaak succesvol op de mens via social engineering. Om meer inzicht te krijgen in de vraag waarom social engineering zo goed werkt en hoe organisaties zich hiertegen kunnen wapenen, voerden studenten social engineeringsaanvallen uit op organisaties. Bijna de helft van de aanvallen was succesvol, ook bij organisaties die de basisbeveiliging dachten goed op orde te hebben. Dit geeft aan dat social engineering een serieus probleem is.

Bij succesvolle aanvallen werden verschillende beïnvloedingstechnieken gebruikt. Het principe sympathie is vaak succesvol toegepast, vooral bij een fysieke aanval. Ook is vaak, met name bij de telefonische aanval, succesvol gewerkt met de principes schaarste en autoriteit. Een andere veelgebruikte overtuigingstechniek is distraction, waarbij een emotie werd opgewekt als verrassing of afschuw. Het principe schaarste werkt ook op deze manier. Bijvoorbeeld door tijdsdruk op te leggen om inloggegevens te verstrekken, omdat anders het systeem crasht.

Het belang van vooronderzoek is duidelijk terug te zien. Het blijkt heel makkelijk om schijnbaar onschuldige informatie over medewerkers te verkrijgen via openbare bronnen, vooral social media. Deze informatie kan ingezet worden als hefboom om personeel van de organisatie te manipuleren. Door een telefoontje konden studenten eenvoudig de naam van IT-systeembeheerder achterhalen of het e-mailadres van de directeur. Een phishingmail kan dan al snel worden gemaakt. Kennis over de organisatiecontext helpt om aan te sluiten bij de herkenbare omgeving. Dit heet 'framing' en is vaak toegepast. Door observaties was bijvoorbeeld de 'dresscode' eenvoudig te achterhalen en maakte

Het demonstreren van kwetsbaarheden aan medewerkers, maakt ze bewust onbekwaam en vergroot zodoende de risicoperceptie

tailgating succesvol. Enige terughoudendheid bij het prijsgeven van schijnbaar onschuldige informatie, zoals een e-mailadres van het werk en een specifieke functie via social media, is aanbevelingswaardig.

Een bepaalde organisatiecultuur lijkt een rol te spelen in het makkelijker prijsgeven van voor cybercriminelen relevante informatie. Studenten wisten regelmatig informatie te verkrijgen over doelen door in te spelen op de servicegerichtheid van medewerkers zoals in de zorg en overheidssector. Een medewerker die zeer behulpzaam was en het leuk vond over zijn vak te vertellen, liet studenten, die zich voordeden als studenten Bouwkunde, foto's maken op een beveiligde locatie.

Sommige aanvallen waren onvoldoende voorbereid of sloten te weinig aan bij de organisatiecontext, zoals in het voorbeeld van de studenten die met een HP-laptop rondliepen in een bedrijf waar overwegend wordt gewerkt met Apple-computers. Ook bleken medewerkers met een voldoende ICT-kennisniveau minder gevoelig voor phishing te zijn.

Een belangrijke voorwaarde voor het succesvol pareren van een aanval is dat de organisatie de basisbeveiliging op orde heeft (10), zoals gedragsprotocollen, functiescheiding en toegangsbeleid. Dit geeft echter geen garantie. Studies zoals (18) (19) geven mooie aanvullende oplossingsrichtingen uit de psychologie. Hieronder bespreken we enkele van deze richtingen.

Kennis over de organisatiecultuur en bijbehorende waarden geeft input over kwetsbaarheden (18). Bovendien kan een informatieveilige cultuur gestimuleerd worden (20). De mate van sociale controle in een organisatie is belangrijk. Als deze hoog is, kan onveilig gedrag van sleutelfiguren in de organisatie, zoals het delen van wachtwoorden, snel worden overgenomen door anderen. Andersom kan dit ook werken. Als de norm het naleven van veiligheidsvoorschriften is, kan sociale controle dit gedrag versterken.

Een oplossingsrichting om te zorgen dat mensen zich bewust worden van hun automatische gedrag, is het inbouwen van vertraging in de interactie met onbekenden indien gevraagd wordt naar gevoelige informatie. Bijvoorbeeld middels een standaardprotocol om de persoon kort daarop terug te bellen, voor het checken van de identiteit (18). Of om te vragen aan onbekenden om hun verzoek te sturen via de email. Het helpt om nadrukkelijk medewerkers permissie te geven om personen te verifiëren (21). Ook technische aanpassingen zijn denkbaar om e-mails van mensen die niet voorkomen in je adresbestand, in platte tekst zonder opmaak, aan te leveren, zodat een bewuste handeling vereist is om eventuele links te openen in de browser (22).

Het ondergaan van social engineering is een interventie op zich. Het demonstreren van kwetsbaarheden aan medewerkers, maakt ze bewust onbekwaam en vergroot zodoende de risicoperceptie (23). Vooral indien mensen hier vervolgens op reflecteren (24). Ook Schaab (25) benadrukt het belang van blootstelling aan social engineering, bijvoorbeeld via rollenspelen. Hierdoor kunnen medewerkers, vooral diegenen met een sociale functie en met persoonlijkheidstrekken als volgzaamheid (18) (26), oefenen met gewenste reacties in de sociale interactie.

Ook Cialdini (11) zelf oppert oplossingsrichtingen hoe mensen en organisaties zich kunnen wapenen tegen de door hem beschreven beïnvloedingsprincipes. Neem het tegengaan van het principe sympathie. Hier kan nieuw (automatisch) gedrag worden aangeleerd. Een receptionist kan geleerd worden (in een training of game) om een mentaal script te doorlopen bij interactie met een persoon die vraagt om gevoelige informatie: 'Vind ik de persoon aardiger dan onder gegeven omstandigheden te verwachten?' en indien ja, deze relatie met de persoon loskoppelen van het verzoek dat gedaan wordt door vriendelijk te antwoorden dat het verzoek niet ter plekke ingewilligd kan worden.

Daarnaast is kennis over beïnvloeding toe te passen om medewerkers te stimuleren tot meer cyberveilig gedrag. Deze technieken kunnen toegepast worden om mensen te verleiden of aan te zetten tot meer cyberveilig gedrag. Twee voorbeelden: Speel via overtuigende communicatie in op 'loss aversion': (zonder back-up kun je al je bestanden kwijtraken). Of zet de sociale omgeving in als hefboom voor meer cyberveilig gedrag: via communicatie

met een boodschap als '80 procent van de medewerkers heeft zijn password reeds gewijzigd' kunnen medewerkers worden overtuigd om zich veiliger te gedragen. Zo maak je van de mens de sterkste schakel.

Co-auteurs

Rick van der Kleij
Rick van der Kleij is sr. onderzoeker bij het lectoraat 'Cybersecurity in het mkb' van de Haagse Hogeschool en sr. onderzoeker bij TNO. Rick is psycholoog en richt zich op cybergedrag van individuen en de cyberweerbaarheid van organisaties. Rick is bereikbaar via r.vanderkleij@hhs.nl

Rutger Leukfeldt
Rutger Leukfeldt is lector Cybersecurity in het mkb bij de Haagse Hogeschool en senior onderzoeker cybercrime en coördinator van het cybercrime cluster van het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). Rutger is te bereiken via e.r.leukfeldt@hhs.nl

Referenties

(1) CBS. (2017). ICT kennis en economie 2017. Den Haag: Centraal Bureau voor de Statistiek.
(2) Leukfeldt. (2017). Research Agenda Human Factor in Cybercrime and Cybersecurity. Den Haag: Eleven International Publishing.
(3) EY. (2017). 10th Annual Global Information Security Survey 2017.
(4) Schneier, B. (2003). Beyond fear. Copernicus books.
(5) Mitnick. (2003). The art of deception. John Wiley & Sons Inc.
(6) Leukfeldt. (2018). De 'human' factor in cybersecurity. oratie. Den Haag: De Haagse Hogeschool.
(7) Kahneman. (2011). Thinking fast and slow. New York: Farrar, Straus and Giroux.
(8) Ariely. (2010). Predictably irrational. USA: Harper Collins.
(9) Fereirra. (2015). Principles of persuasion in social engineering and their use in phising. HAS 2015, (pp. 36-47).
(10) Gragg. (2002). A multilevel defense against social engineering. White paper, Sans Institute.
(11) Cialdini. (2017). The psychology of persuasion. HarperCollins Publishers Inc.
(12) Tversky, K. e. (1992). Advances in prospect theory: Cumulative representation of uncertainty. Journal of Risk and Uncertainty, Volume 5, Issue 4, pp 297–323.
(13) Ajzen. (1991). Theory of planned behavior. Organizational Behavior and Human Decision Processes Volume 50, Issue 2 , Pages 179-211.
(14) Johnson. (2012). Designing with the mind in mind. Morgan Kaufman.
(15) Robbins, J. (2018). Organizational behavior. UK: Pearson Education Limited .
(16) Mcafee. (2015). Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity. Retrieved from http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf.
(17) Handy. (1985). Understanding Organisations , 3rd ed. Harmondsworth: Penguin.
(18) Parsons, C. (2010). Human factors in information security: individual culture en security environment. Science en technology.
(19) Fan. (2017). Social engineering: I-E based model of human weakness for attack and defense investigations. International journal of Computer Network and Information Security, 1-11.
(20) Glaspie. (2018). human factors in IS culture: a literature review 2018.
(21) Intelsecurity. (2017). Hacking the human operating system. Retrieved from http://computer weekly.com.
(22) NCCIC, N. C. (2017). Enhanced Analysis of GRIZZLY STEPPE Activity. Retrieved from http://theconversation.com/the-only-safe-email-is-text-only-email-81434
(23) Sagarin, B. J., Cialdini, R. B., Rice, W. E., & Serna, S. B. (2002). Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion.". The Journal of Personality & Social Psychology, Vol 83(3), 526-541.
(24) Hof, C. (2013). Social engineering. Soesterberg: TNO.
(25) Schaab. (2017). Social engineering defence mechanisms and counteracting training strategies. Information & Computer Security, Vol. 25 Issue: 2, 206-222.
(26) Workman. (2008). A test of interventions for security threats from social engineering. Information Management & Computer Security, Vol. 16 Issue: 5, .463-483.

Jaaroverzicht 2018

Artikelen

(a)Adriaansen, B.	De wet beveiliging netwerk- en informatiesystemen: een redder in nood?	iB6: 22
(v)Bakker, T.	Uitreiking Joop Bautz Information Security Award	iB6: 7
(a)Barda, I.	Integratie van cybersecurity en fysieke beveiliging	iB3: 6
(a)Barda, I.	Vijf stappen om de veiligheid van uw industriële controlesystemen te evalueren	iB5: 12
(o)Borger, L.	Zeven trends die enterprise IT aandrijven in 2018	iB1: 5
(a)Conquet, J.	PViB: meer slagkracht en zichtbaarheid in 2019	iB6: 28
(a)Deursen, N. van	De feestdagen voor cybercrime	iB6: 16
(a)Deursen, N. van	Wie is de meest gezochte informatiebeveiliger?	iB4: 12
(a)Deutekom, P. van	Elk implementatietraject heeft zijn security aspecten in zich!	iB4: 26
(a)Eygendaal, R.	AVG… wat moeten we ermee	iB6: 20
(a)Gittens, M.	Smart Risk Management	iB6: 8
(a)Halfweeg, J.	1.500.000 collega's gezocht	iB5: 8
(a)Hartsuijker, M.	Organisaties worstelen met AVG-identificatie	iB4: 4
(a)Huistra, A.	Concreet aan de slag met de NIS/NIB	iB5: 14
(v)Jochem, A.	Oefeningen… Terugblik uitreiking 'Artikel van het jaar'	iB3: 22
(i)Kagie, S.	Crisismanagement borgen in organisatie	iB4: 8
(i)Kagie, S.	We laten ons graag verrassen door onze opvolgers	iB2: 4
(a)Kogenhop, G.	Herziening Business Continuity Management norm ISO 22301 onderweg	iB3: 8
(a)Leisink, H.	Cybersecurity hoort niet thuis in de directiekamer	iB4: 22
(a)Leisink, H.	Zicht en grip op informatie	iB2: 20
(a)Luijff, E.	Samen werken aan cybersecurity: de 'global agenda for cyber capacity building'	iB2: 16
(b)Metsemakers, R.	Generieke security awareness gericht op gedragsverandering vaak ineffectief	iB1: 26
(a)Metsemakers, R.	Lessons Learned bij het schrijven van security risk scenarios	iB4: 18
(a)Metsemakers, R.	Omgaan met medische behandelplannen	iB2: 12
(a)Metsemakes, R.	SIEM Lessons Learned by autoturven	iB5: 18
(a)Metsemakers, R.	Vier manieren om security-resultaat te verknallen	iB6: 30
(a)Niamat, R.	Online communicatie over de AVG	iB5: 4
(a)Os van, R.	MaGMa: A framework and tool for use case management	iB1: 7
(a)Redactie	Oktobermaand = Conferentiemaand	iB6: 21
(a)Redactie	Voorstellen nieuwe redactieleden	iB5: 24
(a)Redactie	Voorstellen nieuwe redactieleden	iB6: 26
(a)Reuijl, A.	CIP producten: die mag jen iet missen!	iB3: 4
(a)Sens, L.	Hoe pareer je gerichte aanvallen?	iB1: 16
(a)Soest, A. van	Hoe de zes geheimen van het overtuigen de mysterie guest helpen	iB1: 20
(a)Vlugt, J. van der	Iemand heeft iets fout gedaan…	iB6: 12
(a)Vlugt, J. van der	Last van de bystander bug	iB3: 26
(a)Vlugt, J. van der	Ouderlijk toezicht… op je ouders…	iB4: 21
(a)Vries, V. de	Catching an insider spy	iB3: 12
(v)Wessels, J.	Wie of wat is de security professional in 2018?	iB3: 20
(a)Wetzer, I.	Cyberveilig gedrag: Waarom doen we het nou niet?	iB1: 12
(a)Wetzer, I.	Psychologen over cyberveilig gedrag: handvatten voor de praktijd	iB2: 8
(a)Zwaan, A.	Metadata: een onbekend risico	iB6: 4

(a)artikel
(v) verslag
(i) interview
(o) opinie
(b) blog

EUROPE FIRST?

D66 stelde deze maand de vraag of het G5-netwerk niet verboden terrein moet worden voor Huawei. Dennis 't Jong constateerde daartegenover dat Huawei's hard- en software het goed functioneren en nakomen van NPO's publieke taak mogelijk maakt. Wordt het tijd voor een Europees ICT-beleid waarbij het bedrijfsleven met de Europese overheid werkt aan een heruitvinding van Web 2.0/Industry 4.0/informatiebeveiliging X.0? Of wordt Europa gekoloniseerd in een technologisch verbonden wereld en vloeit haar 'big data', de ICT-professional en diens creativiteit af naar de empires Amerika, China en Rusland?

Chris de Vries

Een aardige vergelijking met het verleden zou zijn: China versus Europa in 1421. De toenmalige Chinese keizer Zhû Di, de machtigste man ter wereld, heeft miljoenen soldaten onder de wapenen, een armada van 3.750 schepen (`treasure ships', patrouille vaartuigen, gevechts- en slagschepen alsook vrachtboten, graanschepen en water tank boten) dat beschikt over buskruit, bronzen en metalen kanonnen, mortieren, brandende pijlen en exploderende granaten. Aan boord: gezanten, paarden, honden, vee en grote visvijvers binnen in de boot. En dit alles kon, zonder aan land te gaan, 3 maanden op zee blijven en ruim 8.000 kilometer afleggen. De machtigste Europese vloot was die van de Venetianen. 300 Galleien bemand door roeiers, bestemd voor eiland 'hopping', in de rustige zomerperiode op de Middellandse zee en beschermd door boogschutters. Een strijd tussen de gehele Europese vloot in die tijd versus de Chinese vloot zou gelijken op een strijd tussen een school haaien en een school sprot. Is de huidige situatie op ICT-terrein niet erg gelijkend op die van 1421? Er zijn alleen drie 'empires'. Dat zijn Amerika, China en Rusland. Wie heeft met deze 'vrienden' nog een vijand nodig?

Patrick Dersjant

Tegenwoordig kun je niets meer alleen. Je bent afhankelijk van leveranciers, ketenpartners, en soms zelfs concurrenten. Daardoor kun jij je specialiseren waar jij goed in bent, of 'jij' nu een bedrijf, overheid of ander soort organisatie bent. Maar ben jij ook kwetsbaar omdat je risico's loopt als de ander zich niet aan de afspraken houdt – of je die misschien niet eens hebt gemaakt? Europa is goed in verscheidenheid en vreedzame samenwerking. De invloed die Europa heeft, is vele malen groter dan de bevolkingsomvang van Europa zou doen verwachten. We exporteren niet alleen producten en diensten, maar ook onze idealen. Door regelgeving (zoals de AVG) die wereldwijd als voorbeeld wordt gezien, en door talent dat overal graag wordt ontvangen. Samenwerken op ICT-vlak vergt dialoog, met cloud-providers, Amerikanen, en Chinezen. Of het nu gaat om bedrijven of overheden, elkaar herinneren aan afspraken over samenwerking, en aan de waarden die daaraan ten grondslag liggen, ligt aan de basis van het vertrouwen dat we nodig hebben om zaken te doen. Daar hoort ook bij: elkaar aanspreken als we zien dat niet iedereen zich aan die afspraken houdt, bijvoorbeeld door misbruik van (persoons)gegevens of het inbouwen van achterdeurtjes. Werkt die dialoog niet, dan is er altijd nog de mogelijkheid van een boete, of als laatste stap, een verbod. Maar eigenlijk heb je dan al verloren.

Maarten Hartsuijker

We zijn (met Stuxnet als voorloper) in een nieuwe wapenwedloop terechtgekomen. Een wedloop waarin het voor sommigen draait om het kunnen controleren van de


Maarten Hartsuijker


Chris de Vries


Patrick Dersjant


Fook Hwa Tan

techniek waarop onze maatschappij draait. En daarnaast om toegang tot data voor financieel gewin of macht. Ook is de IT-industrie inmiddels goed voor vele banen en zijn IT-componenten belangrijke exportproducten geworden. De belangen zijn hiermee zo groot dat het aantrekkelijk is om je invloed aan te wenden om de concurrentie schade toe te brengen.

De moderne armada's zijn clouddiensten geworden. Hierin brengen we vrijwillig onze gegevens onder regie van landen waarvan we weten dat ze heel anders met privacy omgaan dan wijzelf. Maar de diensten zijn zo handig dat we onze kop als een struisvogel in het zand steken en er maar op vertrouwen dat de bedrijven die de cloud beheren onze wetten boven hun eigen wetten zullen stellen.

De moderne armada's worden tegenwoordig met pallets tegelijk overgevlogen. Daarna betalen we er flink voor om er ons hele leven in op te slaan, wetende dat de fabrikant van de hardware en het OS (en de bouwers van de vele van de door ons geïnstalleerde apps) meekijken. We weten inmiddels ook dat onze interesses vervolgens worden gebruikt om ons te beïnvloeden. Te beïnvloeden om bijvoorbeeld een product te kopen of een politieke partij te steunen.

Data is macht en IT is het middel om de data te vergaren. Moeten we ons dan zorgen maken om een partij als Huawei? Niet meer of minder dan om andere spelers. Er zijn vele manieren om op netwerken in te breken zonder dat je het risico loopt dat één van je grootste bedrijven zijn westerse markt kwijt raakt. En veel van de interessante data verstrekken velen al vrijwillig. Hierdoor lijkt het mij heel aannemelijk dat Huawei's bewering (dat ze zich niet voor 5G-spionage lenen) klopt. Tegelijk is het voor een mogendheid (niet alleen voor China) strategisch wel heel interessant om je hardware op zoveel mogelijk plekken in gebruik te hebben en te houden. Er is immers slechts één firmware-update nodig om die systemen wel offensief in te zetten.

Fook Hwa Tan

In 1958 is de Europese Unie (Verdrag van Maastricht) gevormd door zes landen en dat vond haar oorsprong in de Europese Gemeenschap voor Kolen en Staal (Verdrag van Amsterdam) en de Europese Economische Gemeenschap (Verdrag van Rome). Deze verdragen dienen ter ondersteuning van een verdere samenwerking tussen verschillende landen binnen de Europese Unie (EU). Het EU-beleid richt zich op het vrij laten bewegen van arbeid, goederen, diensten en kapitaal, het uitvaardigen van wetgeving op het gebied van justitie en binnenlandse zaken en het aanhouden van een gemeenschappelijk beleid op het gebied van handel, landbouw, visserij en regionale ontwikkeling.

Ondanks de ontstane samenwerkingen tussen de verschillende lidstaten zijn er vaak nog steeds verschillende afspraken tussen de lidstaten. Alle lidstaten stellen hun eigen nationaliteit en soevereiniteit vaak boven het 'Europees' zijn. Dit bevordert vaak niet de samenwerking en het vormen van één front.

Naast de nationale trots, die de verschillende lidstaten hebben, komen afspraken pas na lange discussies min of meer tot stand. Dit is vergeleken met de Amerikaanse, Russische alsook de Chinese machten in de wereld een hele andere situatie, waar deze machten vaak al veel langer centrale aansturing kennen. Het gepolder bevordert niet een snel te vormen front.

Ons nieuws heeft de laatste tijd in het teken gestaan van de Brexit. Voor sommigen zijn dit de eerste haarscheuren in een al fragiel front in de wereld. Ook de economisch minderbedeelde lidstaten staan vaak ter discussie of het niet beter is voor deze lidstaten om de EU te verlaten. Al met al vormt de EU nog geen sterk eenduidig front.

De volgende stap zou beleid moeten zijn op het vrij laten bewegen van data. Hierbij is de veel besproken Algemene Verordening Gegevensbescherming voor het vrijelijk uitwisselen van persoonsgegevens een mooie start. De vraag is echter of er met beleid op IT, informatie-beveiliging of cybersecurity daadwerkelijk de gehele keten onder controle gekregen kan worden. De discussie is onlangs begonnen over netwerkapparatuur van Huawei, maar realiseren we ook dat er bijna in alle elektronica tegenwoordig wel wat Chinese fabricage is? Dan hebben we het alleen nog maar over Chinese invloeden. Hoe zit het dan met de Amerikaanse en Russische invloeden? Of zelfs andere onbekendere machten?

Ik ben daarom van mening dat elke organisatie zelf duidelijk zicht moet hebben op de eigen supply chain keten van alles wat ze heeft. Dit is echter niet voldoende. Elke organisatie dient ook de verkregen hard- en software te onderwerpen aan periodieke testen naast het monitoren van dataverkeer van en naar de organisatie.

COLOFON

IB is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

PvIB
Platform voor InformatieBeveiliging

REDACTIE
Tom Bakker
Bianca Brooijmans
Patrick Dersjant
Nicole van Deursen
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
José Broekhuizen
Lisa Petersen
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
Jan van de Vis
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

UITGEVER
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2018 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E secretariaat@pvib.nl

ISSN 1569-1063

VEILIG, VEILIGER, VEILIGST

In mijn eerdere columns sprak ik vaak over de risico's die een normale internetgebruiker loopt. Ik heb het niet over acties die je als gebruiker hebt geïnitieerd als zijnde het niet updaten van je antivirus, of het niet dichtzetten van je firewall of het ingaan op één van de vele phishingmails. Nee, ik heb het over risico's die je als gebruiker automatisch loopt als je specifieke telefoon of hardware aanschaft. Trouwe lezers zullen ongetwijfeld weten welke voorkeur ik heb. Dat heeft dan met name met het aspect van veiligheid te maken. Ik gebruik al heel lang de producten van Apple, omdat ik geloof dat deze stukken veiliger zijn dan de andere apparatuur die op de markt te vinden zijn.

U herinnert zich vast nog de rechtszaak die de Consumentenbond aanging tegen Samsung, die voornemens was om een telefoon twee jaar na het uitkomen niet meer van beveiligingsupdates te voorzien. De Consumentenbond heeft deze zaak verloren.

Dat betekent dat Samsung slechts twee jaar na introductie van een toestel beveiligingsupdates moet uitbrengen voor het betreffende toestel.

Android-telefoons hebben het sowieso bijzonder lastig om veilig te blijven. Iedere fabrikant moet namelijk zijn eigen updates maken, omdat iedere fabrikant zijn eigen appjes en uiterlijkheden plaatst om zijn toestellen te onderscheiden van de rest van de markt. Zijn iPhones dus veiliger dan Android-telefoons ? Honderd procent zeker. Dat komt omdat Apple zowel leverancier is van de hardware als van de software. Apple weet precies waar de updates aan moeten voldoen om te kunnen plaatsen. Ook omdat Apple al precies weet welke appjes op de telefoon kunnen draaien. Schijnbaar controle over de gehele telefoon, maar ervaring leert dat Apple ook wat controle verliest. Op mijn iPhone 2 (ja, dat is inderdaad een tijdje gelden) werd eens een zeer grote update gedaan van het besturingssysteem IOS. Een jaar later kreeg deze telefoon weer een volledige update. Vandaag de dag krijgt iedere iPhone nog steeds ieder jaar een volledige update van het besturingssysteem, maar helaas is de functionaliteit de afgelopen jaren zoveel groter geworden dat er nu steeds meer updates over de updates komen. Veiligheidsproblemen komen meer en meer voor en Apple probeert de bekende problemen op te lossen. Mijn vermoeden is dat het lastig is om bij de huidige zeer complexe software alles te voorkomen. Ik weet niet welke beveiligingsproblemen vandaag in de software zitten. Dat merken we de komende maanden wel. We doen meer en meer met de telefoons en ik vind het toch wel plezierig dat ik degene ben die mijn betalingen regelt, die mijn eigen foto's bekijkt en die kennis kan nemen van de vele mailtjes en appjes die ik dagelijks krijg. "Is alles dan veilig op onze telefoons?" vroeg mijn vrouw laatst. Met veel bluf zei ik "ja", maar ik realiseer me dat ik ook weleens ongelijk heb.

Berry

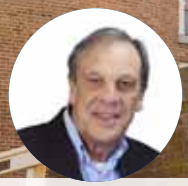
Business Resilience Masterclass

Woerden | 21 maart, 28 maart, 4 april, 11 april, 18 april

Inclusief Master Slot Event in het Grand Kasteel Woerden

JOHAN BAKKER
CISSP - ISSAP - CPT

GERT KOGENHOP
(HON.) MBCI - FINANCE - AT



MICHIEL KUETHE
CRISISMANANAGEMENT - AT

BRENNO DE WINTER
HACKER - BEVEILIGINGS- & PRIVACYEXPERT

Betrek het topmanagement bij de resilience van uw organisatie

De maatschappelijke ontwikkelingen vragen van de overheid en het bedrijfsleven een toenemende kennis op het gebied van Business Resilience.

Schrijf u nu in voor deze unieke Masterclass, waarin u in vier interactieve sessies ontdekt wat de combinatie van Information Security (IS), Business Continuity Management (BCM) en Crisis Management (CM) kan betekenen voor de resilience in uw organisatie.

Ter afsluiting vindt een Master Slot Event in het Grand Kasteel Woerden plaats, waarvoor u één of meerdere introducees mag uitnodigen.

Interesse in deze Masterclass? Neem een kijkje op onze website voor meer informatie of vraag de brochure aan.

Security Academy | www.securityacademy.nl
0348 40 80 61 | info@securityacademy.nl

SECURITY ACADEMY | SECO INSTITUTE