iB
INFORMATIEBEVEILIGING
jaargang 18 - 2018
#1

Cyberveilig gedrag: Waarom dóen we het nou niet?

Nieuwe rubriek: Uit het bestuur

Hoe de zes geheimen van het overtuigen de mystery guest helpen

Generieke security awareness gericht op gedragsverandering vaak ineffectief

Oproep

Beste lezer,
Mogen wij u straks - na het lezen van deze IB - vragen wat u ervan vond? Of de artikelen interessant, leuk en nuttig zijn? Of u onderwerpen mist? Wij zijn benieuwd naar uw mening! Reacties plaatsen we graag in de volgende editie van IB en op onze website.

En heeft u een idee voor een artikel? Of heeft u wellicht een kant-en-klaar artikel liggen? Ook dan horen wij graag van u. IB is een blad van, voor en door de leden van PvIB, maar uiteraard zijn auteurs van buiten de PvIB gemeenschap ook van harte welkom.

Een aantal suggesties voor onderwerpen: hoe gaat het bij uw bedrijf/organisatie met de voorbereidingen voor de AVG/GDPR? Neemt u al maatregelen voor de Brexit? Hoe beschermt u uw IT park tegen fouten in de gebruikte processoren? Experimenteert uw organisatie al met 'block-chain' technologie, en wat voor beveiligingsmaatregelen zou je daarvoor moeten toepassen?

Zomaar wat vragen over actuele onderwerpen waar we elkaar als PvIB gemeenschap zeker mee kunnen helpen. En van elkaar kunnen leren. Geen probleem als u geen ervaring heeft met het schrijven van artikelen, daar kunnen wij u als redactie mee helpen.

Voor suggesties, opmerkingen, verbeterpunten, maar vooral artikelen kunt u terecht op hr@pvib.nl!

De redactie

ROULEREN

Zo, alweer 2018. Een beetje een nieuwe opzet na het vertrek van Lex Borger als hoofdredacteur. Om te beginnen het voorwoord. Elke uitgave van IB Magazine krijgt een andere hoofdredacteur, per toerbeurt. Een roulerend hoofdredacteurschap dus. Ondergetekende mag de aftrap doen voor het eerste nummer.
Verder is het plan om meer thematisch te gaan werken, in samenwerking met de andere PvIB commissies. Zoals vorig jaar al is aangekondigd, gaan we meer gebruik maken van de elektronische mogelijkheden. Daartoe pakken we rond mei het thema Internet-of-Things (IoT) als pilot. Zichtbaar op de website (blog), in een activiteit en in het magazine.
Processen/draaiboeken worden aangepast. We zijn benieuwd hoe dat gaat (be)vallen.
2018, het jaar van de GDPR, zo lijkt het wel gezien de aandacht in de media, van adviesbureaus, cursussen van opleidingsbureaus et cetera. Maar er komt nog meer, zoals PSD2 (Payment Services Directive 2) en eIDAS. Ook de laatste twee hebben veel privacyaspecten.
Veel aandacht voor Security Awareness. Dat blijft belangrijk, ook voor komend jaar. Uiteindelijk zijn de meeste incidenten toch te wijten aan de 'human factor'. Dit nummer heeft 'Security Awareness' als terugkerend thema en een aantal artikelen over dit onderwerp, gezien vanuit verschillende invalshoeken: wat is zinvol en wat niet, hoe verander je gedrag, hoe verbeter je de effectiviteit, de inzet van mystery guests… Andere artikelen gaan, onder andere, over het Use Case Framework (MaGMa) dat gebruikt kan worden binnen een SOC en het jaarlijkse Data Breach Investigations Report (DBIR) van Verizon. Voor elk wat wils dus.

Ik verwacht dat komend jaar helaas weer vele incidenten zullen plaatsvinden. Nog meer en heftiger dan tot nu toe. In de rubriek 'Achter het Nieuws' hebben een aantal redactieleden hun verwachtingen voor 2018 uitgesproken.

Tot slot: als lezers (leden en niet-leden!) zich geroepen voelen een artikel te schrijven? Graag! Loopt u over van ideeën, maar heeft u wat moeite met schrijven: de redactie is u graag behulpzaam.

Tom Bakker

In dit nummer

OPINIE

ZEVEN TRENDS DIE ENTERPRISE IT AANDRIJVEN IN 2018

Security komt voort uit business-IT alignment

Verizon heeft zijn jaarlijkse IT voorspellingen weer gedaan(1). Verizon's jaarlijkse Data Breach Investigations Report (DBIR) is al een favoriet naslagwerk voor mij, maar deze trendwatcher notitie biedt ook een goede gelegenheid om vooruit te kijken naar de security-uitdagingen waar we als professionals mee te maken gaan krijgen.

AI wordt 'security' maar in één van de zeven trendtitels genoemd, de beschrijvingen van de andere trends bevatten ook vaak verwijzingen naar security. Ik loop ze daarom allemaal even langs:

SDN has lift-off!

Verizon verwachtte in 2017 al dat software defined networking een grote vlucht zou nemen. SDN groeide wel, maar schoorvoetend. En het gaat hier ook over SDN buiten de datacenters. Dit vergt echt een overzichtelijke en controleerbare integratie van security in de SDN controllers. Wat ik hierbij mis voor de security professional zijn nieuwe beveiligingsmodellen en -raamwerken om zo de beheersing over SDN te regelen. De SDN controller moet zich bewust zijn van wat de security-aspecten zijn van de informatie die over het netwerk gaat. Verizon noemt dit het application-aware network.

Security goes underground

Ik worstel hierbij echt met de titel. Security moet juist duidelijk en transparant op tafel liggen. Verizon legt de nadruk op de plaats van de maatregel. Deze verhuist naar het platform, waar het dan grip heeft op alle informatie die in het platform verwerkt wordt en door het platform stroomt. Ook spreken ze hier over het globaal rekening houden met 'indicators of compromise' en het belang om deze met iedereen te delen. Dit is inderdaad een trend die we al waarnemen op dit moment. Als dit een stap verder getrokken wordt, dan is ook de effectiviteit van de security controls in je bedrijfsnetwerk kwantitatief te meten, wat integratie en enterprise risk management processen mogelijk maakt. En dan ligt security inderdaad duidelijk en transparant op tafel bij de raad van bestuur. Dat zou een mooie ontwikkeling zijn, al denk ik dat dit nog wel een paar jaar meer zal vergen.

Digital collaboration is table stakes

Al jaren verwachten medewerkers dat ze overal en altijd toegang hebben tot bedrijfsgegevens. En we zien ook de opkomst van de vele cloud-platformen die dit mogelijk maken, met alle kritische kanttekeningen die daarbij te maken zijn over de beveiliging. Dat remde adoptie bij ondernemingen, de financiële industrie en overheden. Verizon geeft aan dat dit nu ook veilig en snel zal kunnen. Hiertoe worden de technieken uit de eerste twee trends toegepast. Of het dan veilig genoeg is om ook op kritische informatie toe te passen, wachten we even af.

Artificial Intelligence and Robotics take on the Internet of Things

We hebben het regelmatig gehad over de IoT nachtmerrie. Verizon ziet een redding: Artificial Intelligence. Door AI toe te passen bij het beheer van IoT in de organisatie wordt grootschalige inzet mogelijk, zonder de infrastructuur overmatig te belasten. Als we inderdaad een controleerbaar SDN-beheer hebben, dan zie ik het beheer van IoT zo wel werken.

People take control of the digital experience

Mensen worden zich steeds meer bewust dat kennis over hen macht geeft. Door het geven van toegang tot hun informatie verwachten ze ook een effectieve en intieme dialoog met hun leverancier. Dit is de trend waar ik de meeste moeite mee heb om die te volgen. Als mensen bewuster worden, worden ze juist ook terughoudender met het beschikbaar maken van die informatie. Bedrijven die een goede klantbeleving kunnen inrichten, waarbij ze ook respect tonen voor de privacy van hun klanten, zullen de grootste stappen kunnen maken.

Interoperability will be a priority for public safety

Verizon wijdt een trend geheel aan 'first responders'. Dit komt door hun business focus, denk ik. Ze doen bijvoorbeeld goed werk in crisisgebieden om, bijvoorbeeld, snel schade in kaart te brengen met drones en de connectiviteit provisorisch te herstellen. Als je dit doet, moet je wat je leert ook willen delen. Ik zie dit geheel in het verlengde liggen van het delen van indicators of compromise, genoemd in trend 2. Dit kun je alleen grootschalig voor elkaar krijgen, als je de communicatie-infrastructuur en de beveiliging van de informatie los kunt trekken van elkaar. En dan is de link naar trend 2 compleet.

Simple is the goal

Dit roepen we als security professionals al jaren. Het zou inderdaad mooi zijn als eenvoud troef wordt. Verizon noemt het focussen op de kerntaken (the core) en het afstoten van de vervelende werkzaamheden (chores). Deze focus is wat startups hun snelheid in handelen geeft. Mijn grote zorg als beveiliger is dat security dan ook uiteen gaat vallen in core & chores. We zullen dus inzichtelijk moeten maken wat de kerntaken zijn en hoe goed we die taken uitvoeren. Dan kunnen de andere werkzaamheden inderdaad uitbesteed worden.

Ik kom tot de conclusie dat software defined networking en het meetbaar maken van het effect van de beveiligingsmaatregelen de grote uitdagingen gaan worden voor de security professional. Als we ons ervan kunnen overtuigen dat we SDN kunnen beheersen en de werking ervan goed kunnen monitoren, dan ben je grotendeels klaar om de uitdagingen die voortkomen uit al deze trends aan te pakken.

Referenties

(1) http://vz.to/2lS3C8d

Lex Borger is senior security consultant bij i-to-i. Hij is bereikbaar via l.borger@i-to-i.nl.

MAGMA: A FRAMEWORK AND TOOL FOR USE CASE MANAGEMENT

Introduction

A Security Operations Center (SOC) has a central role in protecting against and dealing with cyberattacks. In the ever-changing landscape of cyber security, there are many threats to protect against. Each of these threats can have unique indicators in different parts of the cyber killchain (1). It is the job of the SOC to recognize the cyber threats facing the organization in an early stage, mount the appropriate response and help to adjust security parameters to avoid breaches. This process of monitoring for manifestations of cyber threats is called security monitoring.

Security Monitoring

To support the security monitoring process, a security monitoring system is used. In particular a SIEM (Security Information and Event Management) system is an essential part of the security monitoring processes. Additional monitoring systems, such as anomaly detection, intrusion detection (both network based and host-based) and big data platforms for analytics can also be found in more elaborate security monitoring infrastructures.

Security monitoring use cases

To provide a structured approach to security monitoring, use cases are used. Essentially, use cases describe manifestations of threats from a high level (the modus operandi of the cyber criminals) to the lowest level (concrete security events in the infrastructure such as exploits, failed logins, etcetera). Use cases also describe follow-up actions (incident response) and are tied with business drivers to show how security monitoring reduces risk in the organization. Within the complexity of the security architecture, use cases can provide structure and overview.

MaGMa Use case framework

To organize use cases, a use case framework should be used. Such frameworks enable control over use cases and provide insight into identifying how well an organization is capable of defending against cyber threats. For this purpose the MaGMa Use Case Framework (hereafter called: MaGMa) was created, in a collaborative effort of several financial institutions associated with the Dutch Financial Information Sharing and Analysis Community (FI-ISAC). MaGMa stands for Management, Growth and Metrics & assessment. MaGMa is based on the existing framework and tool developed and used by ABN AMRO Bank, complemented with views, experiences and best practices from other financial institutions. The framework consists of a document outlining the framework and a supporting tool for actual management of use cases within the SOC.

This article represents a brief version of the full MaGMa documentation. The full document and the tool can be obtained from:
www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/magma

MaGMa use case definition and model

The focus group started off by creating the following definition for use cases:
"A use case is a security monitoring scenario that is aimed at the detection of manifestations of a cyber threat". A use case has a strategical, tactical and operational component.

With the definition in place, elements of the use case could be identified to create a use case model. The elements that comprise the use case can be divided into three layers:

- Business layer: the business layer of the use case describes how the use case is connected to the organization's business needs;
- Threat layer: the threat layer of the use case describes the threat that the use case is intended for. Several aspects of the threat are important;
- Implementation layer: this is the operational layer, where aspects that are relevant for implementation of the use case in the operational security monitoring architecture are described.

These layers were discussed in detail, which led to the following use case model:

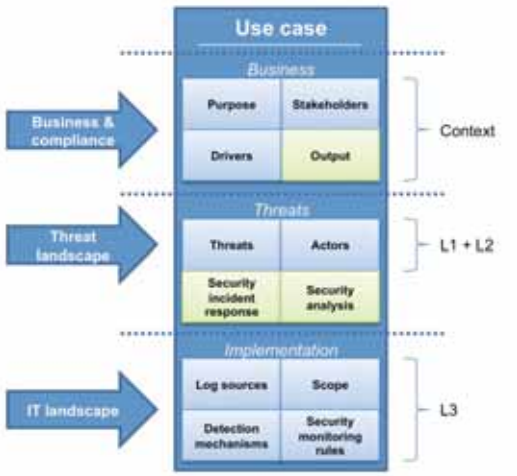


Figure 1 - Use case model

The blocks in blue color can also be found in the supporting MaGMa UCF tool. The green blocks are part of the use case, but documented elsewhere in the security monitoring documentation.

MaGMa elements

With the use case model in place, the basis for MaGMa was created. Each of the elements (Management, Growth and Metrics & assessment) will be explained hereafter.

Management of Use Cases

When the use case framework has been created, it also needs to be maintained. This is what use case management is for. Essentially, it is life cycle management for use cases and is built up out of four phases: onboarding, operational, maintenance and offloading.

Onboarding (plan and build)

For the onboarding of new use cases the use case elements from the model should be made concrete. Stakeholders that provide input into the use case must be made part of the process to ensure proper alignment with these stakeholders. Once all relevant information has been identified, the use case can be documented and operationalized.

Operational phase (run)

In the run phase of a use case all operational elements are implemented and running as part of daily security operations. Concretely, this means, that:

- log sources have been added to the security monitoring systems and supply the required information;
- scope has been determined and implemented for this use case;
- security incident response is known and documented;
- roles and responsibilities for this use case have been formally documented;
- security monitoring rules have been implemented, tested and documented.

Maintenance (change)

There are several types of input that lead to changes within the use case. Most likely, these changes will be carried out at the implementation level, although changes at the threat and business levels will occasionally be required. This section identifies potential sources for input into change management for use cases. These can be divided into two main drivers:

1 Environmental drivers: these are changes to use cases resulting from changes in the organization. Environmental drivers include changes to the threat landscape, changes to the business, changes in rules and regulations and changes in the IT infrastructure.
2 Operational drivers: additionally, operational drivers can lead to change as well. Red team testing as incidental input for improvement and lessons learned from incident response as a continuous input for improvement are important to consider. Threat hunting is also an important driver for change.

Offloading (decommission)

When use cases are no longer required, an offloading process should be followed to remove the use case from the framework at each of the layers. The same inputs that feed the change management of the use case may trigger the decommissioning of the use case.

Figure 2 provides an overview of the life cycle management process and the input received.

Figure 2 - Use case management overview

Growth (Capability and Maturity)

With a use case framework in place and several use cases implemented, an important question arises: how to move towards more mature and more effective security monitoring? To answer this question, two aspects must be evaluated. These aspects are capability and maturity.

Capability

Use case capability deals with how well a SOC is capable

of detecting security threats. Highly capable SOCs will have multiple layers of detection (detection-in-depth) and advanced security tooling for security monitoring. Of course, these SOCs also have highly professional personnel to ensure that their advanced technical capability is backed with equally advanced analyst knowledge.

Growing in use case capability can be done by growing the number of use cases (framework completeness), or by increasing the quality of an existing use case (use case completeness). This can be by increasing the number of assets (log sources), by adding new types of assets to the security monitoring systems or increasing the number of security monitoring rules.

The most effective risk-based approach to capability growth is by first using risk levels to identify high-risk use cases and then using residual risk to determine the required implementation level per use case before moving to the next use case.

Maturity

Maturity deals with how well a SOC is able to provide effective security monitoring continuously and how well it can adequately deal with the output of security monitoring. A highly mature SOC will provide consistent and repeatable output in terms of high-quality reports and effective incident response. Additionally, a highly mature SOC will improve continuously and consistently through a standardized process. Therefore, standardization and documentation are significant aspects of maturity.

According to the CMMI (2), the five maturity levels can be identified:

1. Initial: ad-hoc and chaotic operations;
2. Managed: structured security monitoring;
3. Defined: fully structured use case framework;
4. Quantitatively Managed: goals are set for quality in the use case management process;
5. Optimizing: characterized by continuous improvement.

Metrics & Assessment

To determine the effectiveness of the use case framework in delivering optimal security monitoring, metrics are required. The MaGMa framework should be regularly assessed using these metrics. The outcome of such assessments can be used to identify strong and weak spots within the framework. Note that the focus here is on quantifiable metrics. Three types of metrics have been identified: embedded metrics, control metrics and output metrics. Each of these types will be examined.

MaGMa UCF embedded metrics

There are several metrics embedded into the UCF. These metrics are used to provide steering information regarding the effectiveness of the use case framework. The embedded metrics include effectiveness, implementation level and coverage. From these values weight and potential are calculated. Weight is the overall score of effectiveness, implementation and coverage. Potential provides insight into the growth potential of the use case by calculating weight relative to effectiveness.

MaGMa control metrics

Control metrics provide governance information on the framework itself. The control metrics that can be used are: changes to the framework, growth in number of use cases: measure change in monitoring scope, growth in weight and changes to potential.

MaGMa output metrics

The last category of metrics is metrics on the output of the MaGMa framework. The following metrics were identified: the number of alerts, number of incidents per use case, false-positive ratio and number of false-negatives. False-positives indicate quality and efficiency, while false-negatives indicate gaps in security monitoring.

MaGMa tool

The MaGMa UCF tool supports the use case management process. The tool contains all elements of the use case model depicted as blue blocks in figure 1.

Tool layers

On the right-hand side of figure 1, the phrases L1, L2 and L3 are used. These represent the three layers of the use case as they are used in the MaGMa tool:

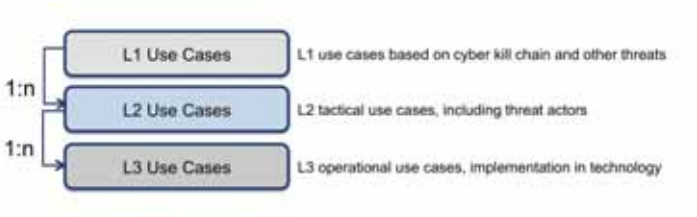


Figure 3 - Use case layers and relation

Each of these layers addresses different elements of the use case. At the L3 layer a technical use case at the operational level is described. At the L2 and L1 layer use cases are described at a tactical level and connected to threat actors, business drivers and compliance drivers.

The framework provides the ability to prove to your stakeholders that the SOC is in control and adequately managing and decreasing risk in the enterprise.

Tool usage

Usage of the tool is explained in detail in the tool itself, but the basic steps for implementation are the following:

- First, outline the strategical business layer. This will provide the necessary context for the concrete use cases. Outlining the business layer is done by speaking with business stakeholders and determining purpose, business drivers and optionally compliance drivers for the framework.
- Then create the L1 use cases using the threat landscape. The seven basic L1 use cases representing the steps in the cyber kill, complemented with six additional L1 use cases are already present in the tool. Additional L1 use cases that are specific for your industry should be added. For example: financial fraud (for the financial sector), industrial control system sabotage (for energy and utilities sector).
- Once the L1 use cases have been finalized, L2 use cases can be put into place. An extensive list of 62 L2 use cases is already present in the tool. This list was created using input from all participating organizations. The list may contain use cases that are not applicable to your organization, or may not fully cover your security monitoring requirements. Therefore, it is important to carefully select the proper use cases and extend upon this list where required and useful. Note that for steps 2 and 3, it is of vital importance to include security management stakeholders to ensure proper alignment with organizational risk & security management processes.
- Lastly, the L3 use cases should be outlined and operationalized. First, outline all of the actual L3 monitoring rules. Then fill in all other applicable operational elements (log sources, scope and detection mechanisms) for each of the L3 rules as desired. Furthermore, the embedded metrics as described in chapter 5 should be set for each of these rules when they are operationalized. A number of L3 rules are already present in the tool, based on the MITRE ATT&CK Matrix for Enterprise (3).

The MaGMa UCF tool can be used to setup a new monitoring environment or can be easily integrated into an existing environment.

Conclusion

Use case management is an essential activity in any mature SOC. The use case management process allows the SOC to gain control over a large and growing number of use cases by structuring the use cases, connecting them to business and compliance drivers and threats. The MaGMa framework was designed specifically to support the use case management process. The tool provides a very practical and flexible approach to managing use cases in any security monitoring environment, from simple to complex. In total, 12 L1 use cases, 62 L2 use cases and 169 L3 use cases have been predefined in the tool, giving organizations a jumpstart in use case management. MaGMa UCF works to be in control over your security monitoring process and align the security monitoring to business and compliance needs. The framework provides the ability to prove to your stakeholders that the SOC is in control and adequately managing and decreasing risk in the enterprise.

References

(1) lmt.co/2kH59Pl
(2) cmmiinstitute.com/
(3) attack.mitre.org/

Authors

Rob van Os, de Volksbank, lead author and UCF developer, rob.vanos@devolksbank.nl
Floris Ladan, ABN AMRO Bank, UCF lead developer
Thomas van Casteren, Rabobank, UCF developer
Robin Toornstra, Euroclear
Robert Metsemakers, Achmea
Lambrecht Nieuwenhuize, BNG Bank
Holger Grotenhuis, Triodos Bank

Additional contributions by

Kelvin Rorive, Rabobank
Marcus Bakker, ING Bank
Tony Tromp, ABN AMRO Bank, UCF developer

DENK EENS WAT VAKER AAN MIJ IN 2018

Netflix brengt aan het einde van ieder jaar haar kijkstatistieken uit. Tot grote hilariteit van velen. Toch altijd weer lachen om die ene persoon in Engeland die elke dag naar `Bee Movie' kijkt of om al die mensen die 18 keer naar een "slechte" kerstfilm keken. De publicatie gaat dan ook gepaard met prachtige billboards en tweets waarin de klant nog verder afgezeken wordt (maar we noemen geen namen hoor!). Zo twittert Netflix bijvoorbeeld: "To the 53 people who've watched `A Christmas Prince' every day for the past 18 days: Who hurt you?" Ik weet niet hoe het met u zit, maar ik krijg hier geen fijn gevoel bij als klant.

Overigens is Netflix niet de enige waar ik een minder prettig gevoel bij kreeg. Maaltijdservice Thuisbezorgd stuurde me begin januari ook een prachtig overzichtsmailtje. Daarin stond hoe vaak ik bij ze had besteld in 2017 en wat mijn favoriete restaurant was om te bestellen. Daaronder stond ook hoeveel de top-besteller afgelopen jaar had besteld. Dat scheelde bijzonder weinig met mijn aantal bestellingen (ik = 75, top = 89). Ik kreeg daar toch een beetje een slecht gevoel bij: "Jeetje, bestel ik echt zoveel? Kook ik dus zo weinig?" En eerlijk is eerlijk, ik zou natuurlijk willen zeggen dat het restaurant waar ik het meest besteld had een enorm gezonde kaart heeft, maar dat is natuurlijk niet zo. Ik vond die big data-analyse van mijn eetgedrag toch iets te confronterend.

Maar waarom staat het me nu zo tegen om mijn eigen gedrag in een lijstje teruggeworpen te krijgen? Omdat het toch voelt als een privacyinbreuk. Bij het Netflix voorbeeld kun je nog zeggen: "Ach, het is heel erg gegeneraliseerd en je kunt de persoon niet herkennen, dus waar maak je je druk om?". Dat blijkt niet helemaal waar te zijn: de persoon die 'Bee Movie' elke dag kijkt, was zo gevonden door de pers; een jonge alleenstaande moeder met een huilbaby. De baby stopt met huilen, zodra die film opstaat. Daarnaast nagel je mensen aan een publieke schandpaal, en dat is toch wat anders dan: "Wij analyseren uw kijkgedrag om onze dienstverlening te verbeteren".
Het is, met alle middelen die tot onze beschikking staan, echt heel makkelijk geworden om iemand te vinden met maar een paar (meta)kenmerken. Van anonimiteit is nog maar zeer zelden sprake. Juist daarom wordt het tijd dat bedrijven, en ook overheden, eens wat vaker aan mij denken. Elke keer als zij data analyseren om 'kekke' dingen te doen, moeten zij zich eerst de vraag stellen: "Wat heeft de klant/burger eraan?". Als je daar geen fatsoenlijk antwoord op kunt vinden, moet je nog eens heel serieus overwegen of je het wel moet doen. En een extra gratis tip: grappige lijstjes waar je klanten een rotgevoel van krijgen, zijn natuurlijk nooit handig. Zo sta ik plots weer veel vaker te koken en heb mezelf bezworen dit jaar niet alleen minder te bestellen, maar er ook voor te zorgen dat áls ik bestel het ongezonde restaurant niet met stip op één staat aan het einde van dit jaar. Oh, en die mevrouw met die huilbaby stuur ik een DVD-tje op.
De beste wensen voor een 2018 waarin u maar zo min mogelijk geanalyseerd mag worden!

Mr. Rachel Marbus
@rachelmarbus op Twitter

Illustratie: Copyright Hoffmann Cybersecurity B.V.

CYBERVEILIG GEDRAG: WAAROM DOEN WE HET NOU NIET?

De toenemende aandacht voor de menskant van cybersecurity zal niemand ontgaan zijn. Naast het nemen van technische en organisatorische maatregelen, richten organisaties zich steeds vaker op hun werknemers. Om meer grip te krijgen op deze menskant, hebben wij de kennis van cybersecurity gecombineerd met expertise uit psychologie, de wetenschap van het gedrag. Dit levert interessante inzichten op die verder gaan dan de vaak gebruikte awareness trainingen. PvIB publiceert hierover een drieluik waarvan dit het tweede deel is. In de vorige editie werd uiteengezet dat organisaties zich zouden moeten focussen op gedrag als einddoel en niet alleen op bewustzijn. In het huidige artikel wordt verder ingegaan op gedragsverandering. Ook wordt ingezoomd op de redenen voor het ontbreken van cyberveilig gedrag. Waarom dóen mensen vaak niet wat er van ze verwacht wordt, terwijl ze wel wéten wat er van ze verwacht wordt (bewustzijn)?

Artikel 2 van Drieluik cyberveilig gedrag

Dat de menskant van cybersecurity aandacht nodig heeft, behoeft inmiddels geen betoog meer. Het volstaat niet langer om de risico's technisch af te dichten en dat weten veel organisaties inmiddels. Dit uit zich vooral in groeiende populariteit van awareness trainingen in verschillende vormen, zoals games, e-learnings of workshops. In de vorige editie van dit drieluik hebben we echter laten zien dat er een kloof is tussen awareness (weten mensen wat er van ze verwacht wordt) en gedrag (doen ze dat ook daadwerkelijk). Uiteindelijk is het voor een organisatie belangrijk dat de medewerkers zich veilig gedragen (Wetzer, 2017a).
Deel 1 van dit drieluik introduceerde een programma vanuit de psychologie dat zich direct richt op het veranderen van gedrag (Wetzer, 2017b). Het uitgangspunt van dit gedragsprogramma is dat gedrag heel specifiek gedefinieerd moet worden. Een breed begrip als `cyberveilig gedrag' kan immers niet gemeten of veranderd worden. Doordat het programma inmiddels voor een groot aantal gedragingen is uitgevoerd, is inzicht ontstaan in de specifieke gedragingen die door organisaties worden verstaan onder `cyberveilig gedrag'. Naast tal van voorbeelden van concrete gedragingen (bijvoorbeeld printen met een code of een pas, voor de werkomgeving een uniek wachtwoord gebruiken dat niet ook privé gebruikt wordt), zijn de belangrijkste conclusies:

- Er is een universele set van clusters van cyberveilige gedragingen;
- De universele gedragingen kunnen worden geclusterd in de volgende zes onderwerpen: wachtwoorden, clean desk, phishing mails, vertrouwelijke gesprekken, vertrouwelijke documenten en pc-gebruik;
- Het belangrijkste gewenste gedrag binnen een cluster verschilt per organisatie;
- Voor elke organisatie gelden tevens unieke gedragingen;
- Een deel van de gedragingen is doelgroep-specifiek.

Cyberveilig gedrag; wat houdt mensen tegen?

Nu er inzicht is in de concrete gedragingen die onder cyberveilig gedrag vallen, kan de stap naar gedragsverandering gemaakt worden. Als het gewenste gedrag in kaart is gebracht, heb je namelijk precies duidelijk wát je van je medewerkers zou willen. De wens tot gedragsverandering impliceert dat het gewenste gedrag nog niet (genoeg) optreedt. Om goed te begrijpen hoe je hier invloed op kunt uitoefenen, bestaat de volgende stap uit het onderzoeken waaróm het gewenste gedrag nu nog niet optreedt.

De redenen voor (het ontbreken van) gedrag kunnen volgens de gedragstheorie van MacInnis, Moorman & Jaworski (1991) worden opgedeeld in drie factoren: motivatie, capaciteit en gelegenheid. Met andere woorden: wíl iemand het doen, is hij in staat om het te doen en krijgt hij de kans om het te doen? Deze gedragstheorie stelt dat motivatie, capaciteit en gelegenheid alle drie op een bepaalde drempelwaarde aanwezig moeten zijn, anders vindt gedrag niet plaats: Men dóet het pas echt, als men het wil, kan én de kans krijgt om het te doen. Andersom betekent dit dus ook, dat medewerkers die bepaald gewenst gedrag níet vertonen, dat ofwel niet willen, ofwel niet kunnen, ofwel niet de kans krijgen. Inzicht in deze redenen voor de afwezigheid van gedrag geeft concrete handvatten voor maatregelen die genomen kunnen worden en is daarmee een zeer belangrijke stap naar gedragsverandering.
Het meten waarom gedrag nog niet optreedt, gebeurt door middel van diepte-interviews met werknemers uit de doelgroep. In 2017 heeft een team van psychologen van Hoffmann gesproken met meer dan 100 medewerkers van verschillende organisaties. Deze diepte-interviews zoomden in op concrete gedragingen die door management of(C)ISO's van de betreffende organisaties als meest gewenst waren benoemd in daarvoor bestemde workshops. Door de open gesprekstructuur van de diepte-

Dr. Inge Wetzer is sociaal psycholoog cybersecurity bij Hoffmann Cybersecurity. Inge is te bereiken via i.wetzer@hoffmannbv.nl

interviews en de gesprekstechnieken van de psychologen, gaf deze methodiek een zeer duidelijk inzicht in het waaróm van het ontbreken van het gewenste gedrag. Wij zetten de belangrijkste resultaten voor u op een rij.

Het ontbreekt regelmatig aan motivatie of gelegenheid

In tegenstelling tot wat de vele awareness programma's doen geloven, is het ontbreken van capaciteit zeer regelmatig niet de oorzaak van waarom mensen zich niet cyberveilig gedragen. Vaak wéét men wel wat er van hen verwacht wordt, maar dóet men het niet, omdat men het bijvoorbeeld niet belangrijk genoeg vindt of uit gemakzucht (motivatie). Ook vaker dan verwacht ontbrak het aan gelegenheid; dan wíl men de gewenste dingen dus wel doen, maar krijgt men de kans niet. Voorbeelden van deze resultaten zijn, dat men soms helemaal geen afsluitbare kast ter beschikking heeft voor het veilig opbergen van vertrouwelijk documenten, of dat men een pashouder heeft waar de pas steeds uitvalt, zodat men deze niet goed kan dragen. Deze gevallen vragen derhalve niet om een awareness-gerichte oplossing; maatregelen zouden regelmatig juist getroffen moeten worden om de gelegenheid of motivatie te verhogen.

Risico-inschatting is vaak laag

Voor veel gedragingen geldt dat men minder gemotiveerd is om ze te verrichten, omdat men het risico laag inschat. Risico wordt bepaald door de kans (hoe groot is de kans dat het mis gaat?) keer de impact (hoe groot zijn de gevolgen als het mis gaat). In opvallend veel gevallen houden werknemers maar met één van deze twee rekening en wordt de andere gebagatelliseerd. Uitspraken die duiden op een lage kans inschatting, zoals: "Als iemand deze papieren van mijn bureau zou meenemen, dan zouden we wel een groot probleem hebben. Maar ja, er kan hier toch niemand binnenkomen.", werden veelvuldig genoteerd. Opvallend was hier een groot vertrouwen in een aantal externe factoren, zoals de techniek, waar men van verwacht dat die er wel voor zorgt dat men geen malware kan binnenhalen, of de beveiliging, waardoor men geen rekening houdt met het feit dat onbekenden wellicht toch het pand binnen kunnen komen. Naast deze lage kans inschatting werd

Een andere belangrijke bevinding is dat medewerkers soms minder gemotiveerd zijn om zich veilig te gedragen, omdat dat voor hen voelt als sociaal onwenselijk.

voor andere gedragingen de impact juist onderschat ("Ja ok, dan heb je mijn wachtwoord. En dan?"), waarna pas bij specifiek doorvragen voor medewerkers duidelijk werd hoeveel informatie men vaak toch in bijvoorbeeld e-mail bewaart en hoe deze toch gevoelig blijkt als men wordt gevraagd te denken aan de gevolgen als bijvoorbeeld een journalist die in handen krijgt.

Vriendelijkheid gaat vaak boven veiligheid

Een andere belangrijke bevinding is dat medewerkers soms minder gemotiveerd zijn om zich veilig te gedragen, omdat dat voor hen voelt als sociaal onwenselijk. De deur sluiten voor iemands neus, een onbekende zonder pas aanspreken, weigeren informatie te geven… Dit gedrag vraagt iets extra's van medewerkers. Uit de diepte-interviews blijkt dat mensen in veel gevallen liever behulpzaam en vriendelijk zijn. Het veilige gedrag wordt gezien als onvriendelijk, soms zelfs onbeleefd, waardoor medewerkers soms tóch die deur even openhouden of die informatie weggeven. Wederom een voorbeeld waaruit blijkt dat niet de awareness ontbreekt (men wéét wel wat er verwacht wordt), maar motivatie het gedrag bepaalt.

Ontbreekt awareness? Dan vaak een specifiek element

De resultaten van de diepte-interviews tonen aan, dat in de gevallen dat awareness de reden is waarom mensen iets niet doen, dit vaak heel specifiek is. Awareness valt in de gedragstheorie van MacInnis et al. onder 'capaciteit'. Het gaat hier om verschillende aspecten van awareness, die allemaal belangrijk zijn: weten mensen dat het gedrag van hen verwacht wordt? Weten ze hoe ze het moeten doen? Weten ze waarom het belangrijk is? Blijft men zich ook op lange termijn bewust van dit gedrag en belang? Op het moment dat gedrag niet plaatsvindt als gevolg van gebrek aan capaciteit, is het dus van belang om te weten welk specifieke stuk awareness ontbreekt. Zo kan er veel gerichter gestuurd worden op het verhogen van de awareness. Dit is niet alleen efficiënter, maar verhoogt ook de impact, omdat werknemers alleen díe informatie krijgen die voor hen relevant is en niet worden overspoeld met algemene awareness informatie die ze al wisten.

Gemakzucht verklaart, maar minder dan gedacht

In voorbesprekingen met managers of CISO's werd vaak gespeculeerd over de redenen voor de afwezigheid van gewenst gedrag. Veelvuldig werd dan genoemd dat men veronderstelde dat gemakzucht de verklaring zou zijn: de medewerkers doen het niet, omdat ze het teveel moeite vinden. Uit de resultaten van de diepte-interviews bleek dat gemakzucht soms wel een rol speelt in het verklaren waarom medewerkers iets niet doen, maar meestal niet alleen en meestal ook niet zo sterk. In veel gevallen was gemakzucht een gevolg, bijvoorbeeld een lage risico inschatting, maar niet de enige en belangrijkste oorzaak.

Hoe nu verder?

In het eerste artikel van dit drieluik over gedragsverandering is uiteengezet hoe belangrijk het is om gedrag specifiek en concreet te maken. Daarnaast is inzicht gegeven in deze concrete gedragingen. Het huidige artikel laat zien waarom medewerkers zich niet altijd cyberveilig gedragen, en wat de oorzaken hiervan zijn. Nu er meer inzicht is in de redenen waarom mensen zich niet altijd cyberveilig gedragen, kan de stap naar interventies worden gemaakt. Kennis over waaróm medewerkers iets nu nog niet doen, geeft handvatten om gerichte interventies te ontwerpen die op deze redenen ingrijpen. In de volgende editie van InformatieBeveiliging vindt u het laatste artikel uit het drieluik cyberveilig gedrag, dat ingaat op de maatregelen die genomen kunnen worden om gedrag te veranderen, gegeven de onderzochte oorzaken.

Referenties

- MacInnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads. Journal of Marketing, 55, 32-53.
- Wetzer, I. M. (2017a). Voorbij awareness; grip op cyberveilig gedrag. InformatieBeveiliging,17 (3), 24-26.
- Wetzer, I. M. (2017b). Cyberveilig gedrag: Meer dan alleen het locken van je beeldscherm. InformatieBeveiliging, 17 (6), 4-7.

E-mailphishing blijft een hardnekkig probleem

HOE PAREER JE GERICHTE AANVALLEN?

E-mailphishing is al ruim 20 jaar oud. Door steeds geraffineerder te werk te gaan, blijven internetoplichters echter bijzonder succesvol. Welke tegenmaatregelen zijn nodig? We geven 10 tips voor een effectief anti-phishingprogramma.

ABN Amro slaagde er eind november in om van phishing landelijk nieuws te maken (1). In een e-mail stelde de bank zijn medewerkers als kerstpakket een Echo Dot in het vooruitzicht; een speaker die met Amazon's spraakassistent Alexa werkt. Voor het 'verzilveren' van het cadeau moesten de medewerkers wel even op een linkje in het bericht klikken.

Eén op de vijf medewerkers kon de verleiding niet weerstaan. Na het klikken kregen deze medewerkers echter de melding dat ze in een phishingmail waren getrapt. Dat hadden ze kunnen zien aan de afzender (abnamro.ml in plaats van abnamro.nl) en aan het ontbreken van een ondertekening met naam.

Met deze campagne wilde de bank testen hoe alert de medewerkers zijn op phishing. Het onderwerp van de phishingtest lag misschien gevoelig, maar de financiële instelling genereerde hiermee wel veel aandacht voor een hardnekkig probleem: phishing per e-mail.

Kunst van het misleiden

Het eerste geval van phishing dateert al uit 1996. En ruim 20 jaar later is het versturen van phishingmails nog altijd een beproefde methode om inloggegevens binnen te hengelen. Uit cijfers van Verizon (2) blijkt dat 21 procent van alle securityincidenten verband houdt met phishing. Mimecast becijferde bovendien dat 11 procent van de ontvangers van een phishingmail klikt op een link of de bijlage opent. 90 procent van de securityincidenten begint met een e-mail.

Om succesvol en vooral onder de radar te blijven, gaan de oplichters steeds geraffineerder te werk. Phishers spreken het slachtoffer niet alleen direct aan, maar doen zich ook voor als beste vriend, gewaardeerde collega of leverancier waar het slachtoffer al jaren een goede relatie mee onderhoudt. Daarvoor zetten ze meerdere technieken in:

Spoofen van e-mailadressen

Onlangs nog werd duidelijk hoe makkelijk het nabootsen van een e-mailadres kan zijn. Een journalist van onderzoeksplatform Follow the Money slaagde erin om uit naam van onder andere Halbe Zijlstra, Geert Wilders en Alexander Pechtold diverse mails rond te sturen in politiek Den Haag.

Ook ABN Amro maakte voor zijn phishingtest gebruik van spoofing, door de '.nl' te veranderen in '.ml'. En wat te denken van een mailtje dat afkomstig is van 'mirnecast.com' in plaats van 'mimecast.com'? Het is de slachtoffers van phishing bijna niet aan te rekenen dat ze in deze trucjes trappen, zeker niet als het bericht afkomstig lijkt van een bedrijf dat ze heel erg goed kennen.

Volgens de Stichting Internet Domeinregistratie Nederland (SIDN) spoofen phishers dan ook op steeds grotere schaal de merknamen van de Nederlandse topbedrijven (3). Met name luchtvaartmaatschappijen, bouwbedrijven en mediabedrijven zijn hiervan het slachtoffer.

Maskeren van URL's

Om de misleiding compleet te maken, doet de aanvaller er alles aan om ook het linkje in de e-mail er vertrouwd uit te laten zien. Zo'n link kan eruitzien als de legitieme URL van een bank of zakenpartner. Met behulp van URL-masking wordt het slachtoffer echter ongemerkt naar een andere website geleid.

Op de malafide website neemt de aanvaller het laatste restje argwaan weg. Vaak is zelfs het groene slotje aanwezig. Dit moet de bezoeker het gevoel geven dat de verbinding veilig is. Waarschijnlijk heeft de aanvaller bovendien de trukendoos opengetrokken om het webadres in de URL-balk er zo vertrouwd mogelijk uit te laten zien. Zo kan de hacker handig gebruikmaken van Unicode-karakters. Een onderzoeker demonstreerde onlangs nog dat het mogelijk is om browsers te foppen (4) met de domeinnaam 'xn—80ak6aa92e.com'. Onder andere Chrome en Firefox toonden in de adresbalk 'netjes' apple.com.

E-mailberichten klonen

De phisher stuurt vanaf een gespooft e-mailadres een kopie van een legitieme e-mail die al eens eerder is verstuurd. Zeker voor aanvallers die het netwerk al zijn binnengedrongen en e-mailberichten kunnen onderscheppen, is dit een koud kunstje.

De ontvanger denkt al snel dat het om een update van een eerdere mail gaat. De gekloonde e-mail is echter niet volledig identiek aan het oorspronkelijke bericht. Grote kans dat de aanvaller een kwaadaardige bijlage bij de mail heeft gestopt of dat een link naar een andere website leidt.

Het is zelfs niet ondenkbaar dat criminelen de inhoud van een e-mail pas na aflevering aanpassen. Dit probleem speelt met name bij webmail die gebruikmaakt van Cascading Style Sheets (CSS). Door na aflevering van een e-mail de CSS aan te passen, kan een aanvaller een onschuldige link alsnog laten leiden naar een kwaadaardige website. Deze kwetsbaarheid staat ook wel bekend als ROPEMAKER (5), een acroniem voor Remotely Originated Post-delivery Email Manipulation Attacks Keeping Email Risky.

Anti-phishingprogramma

Een geslaagde phishingaanval kan verstrekkende gevolgen hebben. Volgens een onderzoek van Vanson Bourne kosten phishingaanvallen gericht op grote bedrijven gemiddeld 1,6 miljoen dollar (6). En

Lisette Sens is Director Northern Europe bij Mimecast, een specialist in e-mailsecurity- en archivering. Zij is bereikbaar via lsens@mimecast.com en @Lsens.

volgens onder andere Gartner blijft e-mail de komende jaren de belangrijkste aanvalsvector. Dat vraagt om een geavanceerd anti-phishingprogramma waarin niet alleen technische, maar ook procedurele en educatieve maatregelen worden opgenomen. Hierbij kunt u onder andere denken aan de volgende 10 maatregelen:

Time-to-click URL-filtering
Deze vorm van URL-filtering gaat ervan uit dat een link niet alleen wordt gecontroleerd bij de aflevering van een e-mail, maar ook op het moment dat een gebruiker op een link klikt. Cybercriminelen die een link pas na ontvangst naar een kwaadaardige website laten leiden, vallen hiermee door de mand.

Sandboxing van bijlagen
Sandboxing is een beproefde manier om te kijken hoe verdachte files zich gedragen in een gesimuleerde pc-omgeving. Deze aanpak is effectiever dan de traditionele analyse op basis van signatures, maar er kleven ook nadelen aan. Zo zorgt sandboxing voor een vertraging in de aflevering van e-mailberichten. Ook hebben criminelen manieren gevonden om deze vorm van detectie te omzeilen, bijvoorbeeld door uitvoerbare bestanden te verstoppen in Office-bestanden en pdf's.

Content disarm and reconstruction (CDR)
Dit is een methode om in files verstopte kwaadaardige code alsnog op te sporen. CDR 'stript' een bestand door alles weg te gooien wat er volgens de ISO-standaarden of bedrijfspolicy niet in thuishoort. Daarna wordt er weer een 'schoon' bestand opgebouwd. Ook deze aanpak heeft een nadeel: het kan gebeuren dat CDR code eruit haalt die erin zat voor de functionaliteit.

Strikt patchbeleid
Een goed patchmanagement is altijd belangrijk, ook voor het tegengaan van phishing. De (nogal ruime) schatting van Gartner is dat het op tijd patchen van Microsoft Office- en Adobe-programma's 30 tot 80 procent van de verstopte malware tegenhoudt.

Implementatie SPF, DKIM en DMARC
Implementatie van deze standaarden is een krachtig middel om spoofing te ontdekken. Met Sender Policy Framework, DomainKeys Identified Mail en Domain-based Message Authentication, Reporting and Compliance kan een mailserver controleren of de afzender van een e-mail wel is wie hij zegt te zijn, en of hij de rechten heeft om namens het betreffende domein e-mail te versturen.

Inspectie content op basis van trefwoorden
Phishingmails bevatten vaak woorden als 'gebruikersnaam', 'wachtwoord' en 'belangrijk''. Steeds meer e-mailsecurityoplossingen waarschuwen gebruikers als een mailtje op basis van de inhoudelijke inspectie verdacht is.

Tweefactor-authenticatie
Phishers is het vaak te doen om de inloggegevens van de gebruiker. Zorg er daarom voor dat gevoelige bedrijfstoepassingen alleen toegankelijk zijn met behulp van twofactor-authenticatie. Een phisher heeft niets aan alleen gebruikersnaam en wachtwoord als er voor het inloggen ook nog een 'one-time password' nodig is.

Anti-Phishing Behavior Management (APBM)
Dit is een belangrijk onderdeel van een compleet security-awarenessprogramma. Met de APBM-oplossingen van bijvoorbeeld het SANS Institute, PhishMe en Wombat Security Technologies is het mogelijk om phishingaanvallen te simuleren, gebruikers te informeren en gedrag te corrigeren als de reactie op een phishingtest niet naar wens is. Uiteraard moet de aandacht niet alleen uitgaan naar phishingmails, maar ook naar phishing per social media, per sms ('smishing') en per telefoon ('vishing').

Interne processen en controles
Een phishingaanval is niet altijd direct gericht op bijvoorbeeld de inloggegevens van het slachtoffer, maar bevat soms ook een oproep. Een bekend voorbeeld is de e-mail waarin zogenaamd de CEO een finance medewerker vraagt om een geldbedrag over te maken. Dan helpt het als een 4-ogenprincipe wordt toegepast. Ook moet het voor iedereen duidelijk zijn hoe te reageren op een phishingaanval. Een snelle melding vergroot de kans dat het Computer Security Incident Response Team adequaat kan handelen.

Cyber resilience
Zelfs met de beste beveiliging, een optimale security-awareness en de juiste processen en controles zullen er altijd nog mensen zijn die in phishingmails trappen. Dan is het zaak dat er een 'plan van aanpak' in werking treedt en wachtwoorden en toegangsrechten worden gewijzigd. Leidt het openen van een bijlage bijvoorbeeld tot een gijzeling van data? Dan helpt het als er een extra kopie van de data beschikbaar is.

Die kopie is ook belangrijk voor naleving van de Wet bescherming persoonsgegevens en vanaf 25 mei 2018 de Algemene Verordening Gegevensbescherming. Het niet meer kunnen herstellen van persoonsgegevens geldt immers ook als een datalek.

Referenties

(1) http://bit.ly/2iKCNCa
(2) http://vz.to/2qihidi
(3) http://bit.ly/2AbFTFg
(4) www.xudongz.com/blog/2017/idn-phishing/
(5) http://bit.ly/2CfgFrt
(6) http://bit.ly/2CJBNHg

RAOUL VERNÈDE

Een nieuwe rubriek, met het bestuur van de PvIB als lijdend voorwerp. En ik mag het spits afbijten. Spannend, want ik ben pas recent toegetreden tot het bestuur, waar ik met mijn kennis en kunde op het gebied van security in de onderwijs-/onderzoekswereld een bijdrage aan hoop te leveren. Als aanvulling op de vertegenwoordiging uit bijvoorbeeld het bankwezen en de commercie.

In het dagelijks leven ben ik Information Security Officer en Security Architect bij Wageningen University & Research en verantwoordelijk voor de beveiliging van de gehele organisatie waar het IT betreft. Van het gevoerde beleid op beveiligingsgebied tot de daadwerkelijk beveiliging van netwerk, PC's en laptops.

In die hoedanigheid ben ik ook betrokken bij SURF, de ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland. Binnen SURF is er een zeer actieve security community, enerzijds technisch, anderzijds beleidsmatig. Onderlinge kennis en praktische (inside) ervaringen delen staat hierbij centraal. Binnen het bestuur van PvIB ben ik op deze manier een mooie linking pin met de onderwijs- en onderzoeksinstellingen. Andersom kom ik dankzij deze bestuursfunctie in aanraking met mensen uit andere branches wiens ervaringen op het gebied van security ik mee terug kan nemen naar de onderwijs-/onderzoeksector.

Mijn aandachtsgebied binnen het bestuur is nog niet helemaal bepaald. Ik schreef al eerder artikelen voor IBmagazine over informatiebeveiliging (zo ben ik ook het bestuur ingerold), en gezien mijn affiniteit met publicaties en kennisspreiding, zou ik het leuk vinden me daar op te kunnen richten. Meer synergie tussen de verschillende communicatiekanalen die de PvIB tot haar beschikking heeft, is wenselijk om een grotere impact te hebben. Willen we een bijeenkomst organiseren rondom een bepaald actueel thema, dan kun je het IBmagazine en eventuele sociale media daar mooi op afstemmen. Die afstemming is er nu nog te beperkt lijkt het. Daarnaast is het goed om te blijven kijken naar de doelstelling van de PvIB. Waar is de beroepsvereniging voor bedoeld? Wat is de toegevoegde waarde voor leden? We zijn namelijk groeiende. De kunst is om die groei te managen, om een goede kern te behouden en te voorkomen dat kwantiteit de overhand krijgt op kwaliteit en persoonlijk contact. Het is belangrijk de professionele focus te houden op het delen van kennis en kunde binnen ons vakgebied en in te springen op actuele onderwerpen.

Zoals het verontrustende nieuws waar 2018 mee begon: dat chips (Meltdown & Spectre) die leveranciers wereldwijd in alle devices verwerkt hebben, gehackt kunnen worden. Deze ontdekking raakt werkelijk alles! Waar de kwetsbaarheden voorheen vooral in software voorkwamen, merken we nu dat ook de hardware niet veilig is. Een hele uitdaging, want een simpele update is in dit geval niet afdoende.

Een ander actueel onderwerp is privacy. De invoering van de AVG heeft grote invloed op alle sectoren. Je merkt dat organisaties en bestuurders zenuwachtig worden, mede doordat de nieuwe wet boetebevoegdheden geeft. Juist nu moeten we daarom de kans grijpen om van elkaar leren en concrete stappen vooruit te zetten. De afgelopen jaren is binnen security al veel ervaring opgedaan met privacy, dankzij de eerder verscherpte wet- en regelgeving en internationale kaderstellende normeringen. Zenuwachtig worden is dan ook niet nodig. Maar het is belangrijk dat organisaties én individuen het belang van privacy steeds serieuzer nemen, en mooi dat er een maatschappelijke discussie ontstaat over privacy. Waar iedere website nu nog allerhande persoonlijke informatie vraagt voor een account, vragen we ons meer en meer af: Welke informatie is echt nodig? Wat kan na registratie weer weg en wanneer? Maar we staan pas aan het begin van dit traject. Het compleet doorvoeren van de privacywetgeving, en dus privacy by design en default, kost nog jaren. Genoeg materiaal om IBmagazine te blijven vullen, denk ik zo. Ook daar lever ik graag mijn bijdrage aan.

raoul.vernede@wur.nl - 06-23313023

HOE DE ZES GEHEIMEN VAN HET OVERTUIGEN DE MYSTERY GUEST HELPEN

Steeds meer organisaties zien de bewustwording van medewerkers als een belangrijk onderdeel van informatiebeveiliging. Eén manier om een bijdrage te leveren aan awareness is door de inzet van een social engineer(1). In de praktijk krijgt deze social engineer vaak de titel 'mystery guest'. Dit artikel gaat in op de theorie van Cialdini en laat met voorbeelden zien hoe de mystery guest de psychologie van overtuiging in de praktijk inzet.

Wat is het doel van een mystery guest?

Bij een mystery guest-aanval wordt op verzoek van een opdrachtgever een locatie gecontroleerd aangevallen. Een mystery guest-aanval kan verschillende doelen hebben:

- inzicht krijgen in de mate waarin een bepaald doelobject weerstand kan bieden aan pogingen om onbevoegd toegang te krijgen tot bedrijfsmiddelen. Een doelobject kan bijvoorbeeld een fysieke locatie, een informatiesysteem of de paspoortenkluis zijn;
- meten van het huidige niveau van de weerbaarheid tegen social engineering;
- verhogen van de bewustwording van de medewerkers;
- meten van de effectiviteit van reeds genomen maatregelen;
- verkrijgen van inzicht in te nemen maatregelen;
- vergaren van (beeld)materiaal voor verdere bewustwordingscampagnes.

Om deze doelen te bereiken, maakt de mystery guest gebruik van de zes principes van Cialdini.

Zes overtuigingsprincipes van Cialdini

`Een brutaal mens heeft de halve wereld', zo luidt een oud spreekwoord. Natuurlijk moet een mystery guest over brutaliteit en lef beschikken: het is spannend om aan te vallen! Echter, van een mystery guest wordt meer gevraagd dan brutaliteit alleen, anders zou hij snel tegen de lamp lopen. Het doel van een mystery guest is om mensen te beïnvloeden tot het vrijgeven van informatie of het uitvoeren van handelingen. Met andere woorden: zaken die onder normale omstandigheden niet zouden gebeuren.

Robert Cialdini is hoogleraar psychologie en auteur van het boek `Invloed: de zes geheimen van het overtuigen'. In dit boek presenteert hij zes wetenschappelijk onderbouwde overtuigingstechnieken uit de sociale psychologie. Deze technieken worden niet alleen gebruikt in de marketing, maar worden ook veelvuldig ingezet door mystery guests.

Figuur 1 – Overtuigen.

Wederkerigheid

Bij wederkerigheid maakt de mystery guest gebruik van het principe `geven en nemen'. Wanneer jij iets voor een andere persoon doet, is deze sneller geneigd iets voor jou terug te doen. Dit geldt extra zwaar in het geval van een ongevraagde gunst. Dan ontstaat een schuldgevoel bij de ontvanger van de ongevraagde gunst, dat ertoe kan leiden dat deze persoon eerder in zal stemmen met het doen van een gunst die groter is dan de gunst die hij zelf heeft ontvangen.

"Als galant persoon houd ik de deur voor iedereen open. Natuurlijk vooral de deuren die niet zijn afgesloten. Ik doe dit om te zorgen dat een medewerker de volgende deur, die wel afgesloten is, voor mij open doet. Dit is meestal het geval, want het zou toch onaardig zijn om dan ineens te vragen wat iemand komt doen."

"Ik doe mij graag voor als helpdesk-medewerker. Ik zeg tegen een medewerker dat zijn device kuren vertoont en hij misschien al zijn werk kwijt raakt, maar dat ik hem natuurlijk kan helpen om dit te voorkomen! Als de medewerker mij zijn wachtwoord geeft, los ik het op en kan hij snel weer

André van Soest en Patricia van Schaik werken als consultants informatiebeveiliging bij LBVD. Zij voeren opdrachten uit voor grote en kleine organisaties in allerlei branches. Als mystery guests voeren zij veel aanvallen uit en passen hierbij de principes van Cialdini toe. André en Patricia zijn bereikbaar via avansoest@lbvd.nl en pvanschaik@lbvd.nl.

verder werken. Medewerkers met minder technische kennis gaan snel overstag en zijn blij dat je hen helpt, want stel je toch eens voor dat ze hun werk kwijt zijn."

Commitment en consistentie

Vreemd genoeg hebben mensen over het algemeen een sterke drang naar consistentie. Als een persoon een bepaalde beslissing genomen heeft, dan blijft deze er vaak consistent mee, of dat nu verstandig is of niet. Verder zijn mensen geneigd om in toekomstige situaties te handelen naar keuzes die ze eerder in soortgelijke situaties hebben gemaakt. Dit principe uit zich bijvoorbeeld in het feit, dat indien mensen op meerdere opeenvolgende vragen 'Ja.' hebben geantwoord, de kans groter is dat zij de eerstvolgende vraag op dezelfde manier zullen beantwoorden.

"Ik zeg dat ik ingehuurd ben door de afdeling ICT, omdat er netwerkproblemen zijn en dat ik het probleem kom onderzoeken. Ik vraag aan de medewerker of hij ook last heeft van het trage netwerk. Als hij dit positief beantwoordt, laat ik een apparaatje zien (USB-keylogger) en vertel dat ik daarmee de netwerksnelheid kan meten en verbeteren. Dit zal het probleem van de medewerker oplossen. Ik vraag de medewerker om toestemming om het apparaatje aan te sluiten. Als het antwoord ook nu positief is, sluit ik het apparaatje aan en zeg dat de medewerker de PC moet afsluiten en weer moet inloggen. Mijn ervaring is dat de werknemer meewerkt, want hij heeft steeds meegewerkt en wil dat het probleem wordt opgelost. Hij heeft niet door, dat ik hiermee zijn gebruikersnaam en wachtwoord afvang."

"Ik gebruik het volgende principe om een medewerker af te leiden en zijn werkplek onbeheerd achter te laten, zodat een collega mystery guest toe kan slaan. De vraag 'Mag ik iets vragen?' wordt vrijwel altijd met 'Ja.' beantwoord. De vervolgvraag: 'Bent u bekend op deze gang?' heeft ook een grote kans om met 'Ja.' beantwoord te worden, aangezien de medewerker op de desbetreffende gang werkt. De derde vraag: 'Kunt u mij alstublieft laten zien waar de brandslang hangt?' zal waarschijnlijk ook positief worden beantwoord, wat maakt dat de medewerker onverwachts zijn werkplek verlaat. Mogelijk zonder de PC te vergrendelen en met vertrouwelijke documenten op het bureau. Nu kan de andere mystery guest toeslaan."

Sociale bewijskracht

Het derde principe speelt in op het feit dat als anderen iets doen, de kans groot is dat jij dit ook gaat doen. Niet alleen kinderen zeggen 'Maar hij deed het eerst!'. Het referentiekader van mensen, ook volwassen mensen, wordt beïnvloed door te kijken naar wat anderen (niet) doen of vinden. De effectiviteit van dit principe is mede afhankelijk van de onzekerheid van de medewerker.

"Ik vraag aan een medewerker of hij toegang tot de serverruimte heeft. Als hij daar positief op antwoordt, geef ik aan dat we alle kamers en ruimten hebben onderzocht op 'brandmelders, brandblussers en nooduitgangen'. Ik zeg dat collega's van de man daar al bij hebben geholpen en ik alleen nog moet kijken naar de voorzieningen in de serverruimte. Vaak loopt de medewerker mee naar de ruimte. Eenmaal in de ruimte kan de ene mystery guest bij de medewerker blijven en hem afleiden, terwijl de ander mogelijk malware kan installeren of een Raspberry PI kan plaatsen, zodat toegang vanaf buiten mogelijk is."

"Kan je de deur voor mij openen? Je collega heeft me net ook binnengelaten!"

"Wanneer we de specifieke opdracht krijgen om wachtwoorden te ontfutselen, maken we een lijst met fictieve wachtwoorden bij bestaande e-mailadressen. Deze lijst laten we aan medewerkers zien. Daarbij geven we aan dat hun collega's al wel hun wachtwoord hebben opgeschreven voor het onderzoek naar de kwaliteit van de wachtwoorden. Dit trekt de twijfelende medewerker vaak over de streep om toch zijn wachtwoord op te schrijven."

Sympathie

Een mystery guest wil mensen beïnvloeden tot het vrijgeven van informatie of het uitvoeren van handelingen. Het is dus belangrijk voor de mystery guest om mensen 'Ja' te laten zeggen. Cialdini stelt in zijn boek 'Influence', dat mensen eerder 'Ja' zeggen tegen personen die ze kennen en sympathiek vinden. Daarom maakt een mystery guest regelmatig gebruik van een aantal factoren die meer aantrekkelijk en sympathiek maken.

"Binnenkomen met een grote doos en zeggen: 'Ik heb mijn handen vol. Wil jij alsjeblieft even de deur voor mij openen? Mijn pas zit in mijn binnenzak.' Iedereen herkent de situatie dat je met volle handen voor een dichte deur staat en is graag behulpzaam."

Fysieke aantrekkingskracht	Aantrekkelijke mensen zijn beter in het misleiden van mensen en het veranderen van de houding van mensen.
Gelijksoortigheid	Het blijkt dat mensen eerder geneigd zijn om in te gaan op een verzoek van iemand die net zo is als hijzelf.
Lof / vleierij	Het geven van complimenten kan sympathie opwekken. Een mystery guest past hier wel mee op, want als het voor de ander niet oprecht aanvoelt, kan het een tegengesteld effect hebben.
Vertrouwen	Wanneer het contact onder positieve omstandigheden plaatsvindt, kan herhaaldelijk contact de sympathie bevorderen.
Associatie	Wanneer je iemand wilt beïnvloeden, moet je de indruk wekken dat je op die persoon lijkt. Een social engineer zal zoeken naar overeenkomsten en hierop inspelen.

"Wanneer ik binnenkom, bied ik bij de receptie direct mijn excuses aan en zeg dat er vorige week al een inspectie heeft plaatsgevonden. Helaas zijn bij een computerstoring alle gegevens gewist, waardoor de inspectie over moet. Ik zeg zuchtend, dat het altijd gedoe is met de computers en vraag of ze het herkennen. Na dit praatje zeg ik, dat het niet nodig is om de facilitaire medewerker weer van zijn werk te houden om mij te begeleiden; als de receptiemedewerker mij toegang geeft, loop ik even snel door het gebouw, en is het zo geregeld."

"Ik houd van vleierij en zeg dingen als: 'Wat heb je een leuke bril of toffe schoenen."

"Ik rook al jaren niet meer, maar als mystery guest steek ik graag een sigaretje op. De rookplek is een makkelijke ingang; andere rokers doen altijd de deur voor je open."

"Ik doe er alles aan om mij te kleden als de mensen in de organisatie. Ik heb hiervoor diverse outfits; van bouwhelmen tot legerkleding en laboratoriumjassen. Eenmaal binnen groet ik iedereen op een vrolijke manier, alsof ik niets te verbergen heb. Het liefst eet ik mee in de kantine, daarna 'hoor je erbij'. Ik merk dat de gesprekken met mensen die mij in de kantine hebben gezien veel eenvoudiger gaan, en dat ik sneller mijn doel bereik."

Autoriteit

Autoriteit heeft alles te maken met gezag. Uit diverse onderzoeken is gebleken, dat mensen geneigd zijn om gehoor te geven aan autoriteit. In de meeste gevallen zonder daar zelf bij na te denken. Een mystery guest maakt veelvuldig misbruik van dit principe, ook bij de keuze van de dekmantel. Er wordt vaak voor een autoritaire dekmantel gekozen. Een bekend voorbeeld is het uitvoeren van een inspectie. Bij voorkeur in opdracht van een (nog hogere) autoriteit.

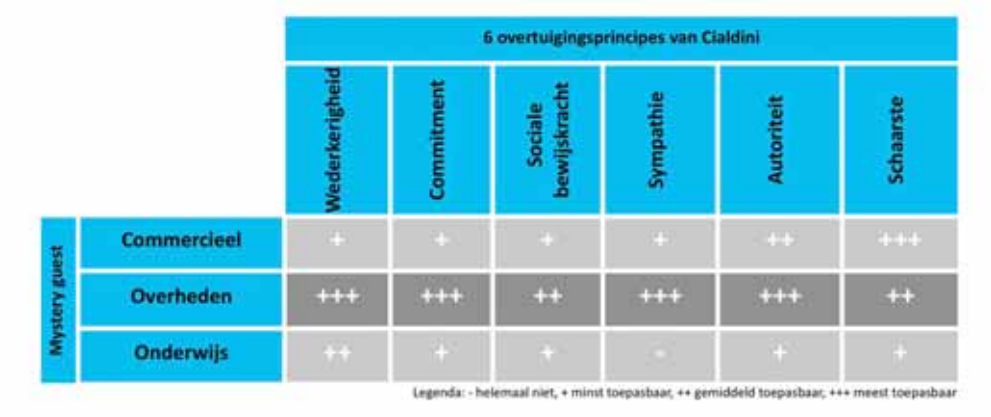
"Wanneer mensen assertief zijn en vragen of ik iets of iemand zoek, geef ik aan dat ik geen hulp nodig heb en bezig ben met een onaangekondigde inspectie. Na deze boodschap draai ik mijn lichaam af en ga door met waar ik mee bezig was. De meeste mensen schrikken van deze autoritaire reactie en vragen niet meer door."

"Ik noem vaak de directie van het desbetreffende bedrijf als opdrachtgever en zeg dat deze mij heeft ingehuurd om een inspectieronde uit te voeren. Ik zeg erbij, dat de directie heeft gevraagd om het te melden als mensen niet meewerken. De namen van de directie staan meestal op de website/LinkedIn-pagina van de organisatie en wanneer het nodig is, gebruik ik ze. Deze aanpak werkt het beste bij grotere organisaties. Ook dan is het zaak dat je wegblijft van de directievloer."

Schaarste

Bij dit principe zijn mensen geneigd om zaken die moeilijk(er) te verkrijgen zijn, waardevoller in te schatten. Ondanks dat dit principe door een mystery guest beduidend minder wordt toegepast dan de andere vijf principes, wordt het wel degelijk toegepast.

Bij het versturen van phishing e-mails wordt het principe veel gebruikt. Mensen zijn bereid persoonsgegevens af te staan, als ze kans maken op een aanbieding, concertkaartjes of een bijna uitverkocht product.



Figuur 2 - Overtuigingsprincipes van Cialdini.)

"Wij sturen een phishing e-mail naar medewerkers, waarin staat dat de organisatie iets extra's wil doen voor de medewerkers vanwege hun inzet de afgelopen periode. Wij lokken de medewerkers met de mededeling dat er een beperkt aantal gratis kaarten beschikbaar is voor een theatervoorstelling in de buurt van de vestigingsplaats van de organisatie. Wil men gebruik maken van de aanbieding, dan dient men op de link te klikken voor meer informatie over data en voorwaarden."

"Door phishing USB-sticks op parkeerplaatsen te leggen, over hekken bij bedrijven te gooien, op te sturen of gewoon rond te laten slingeren, bereik je veel resultaat. Mensen willen de USB-stick hebben of kunnen hun nieuwsgierigheid niet bedwingen. In april 2017 hebben we een onderzoek gedaan met 25 USB-sticks; een derde daarvan is op zakelijke PC's/laptops aangesloten."

Cialdini versus mystery guest

In dit artikel hebben we met praktijkvoorbeelden laten zien hoe de mystery guest de psychologie van overtuiging inzet. In de afgelopen vijf jaar hebben we als mystery guests meer dan honderd aanvallen uitgevoerd bij verschillende organisaties. Op basis van de verkregen informatie hebben we in kaart gebracht of de toepasbaarheid van de overtuigingsprincipes van Cialdini voor alle organisaties hetzelfde is. Hiervoor hebben we de resultaten van deze principes vergeleken per branche. We maken daarbij een onderscheid tussen overheden, commerciële organisaties en onderwijs.

In figuur 2 is per branche onderzocht in welke mate wij de principes toepasten (hoe wordt een slachtoffer benaderd) en hoe effectief dit was. Hiervoor hebben wij per branche minimaal dertig bevindingenrapportages genalyseerd. De toepasbaarheid van de principes is weergegeven met een score per branche.

Conclusie

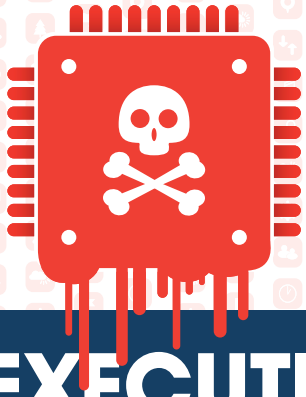
We concluderen dat tijdens het uitvoeren van de mystery guest-aanvallen alle principes van Cialdini zijn toegepast. Wij kunnen niet zeggen of andere social engineers deze principes op dezelfde wijze toepassen.

We hebben de overtuigingsprincipes effectiever kunnen gebruiken bij overheden dan bij commerciële organisaties. Dit kan te maken hebben met de dienstbaarheid van medewerkers die bij de overheid werken. De principes 'Wederkerigheid, Commitment, Sociale bewijskracht, Sympathie en Autoriteit' zijn effectiever bij overheden. 'Schaarste' is juist doeltreffender bij commerciële organisaties. Bij commerciële organisaties is het percentage medewerkers dat op een phishing e-mail klikt of een gevonden USB-stick in de computer prikt veel groter dan bij de andere branches.

Gebleken is dat in het onderwijs de principes het minst effectief zijn. Dit komt mogelijk, doordat het onderwijs een open cultuur heeft en erg toegankelijk is. Bij de meeste onderwijsinstellingen loop je direct naar binnen zonder dat men je aanspreekt of tegenhoudt. Dit draagt er, bijvoorbeeld, aan bij dat de principes 'Sociale bewijskracht en Sympathie' minder effectief zijn. Uit de analyse is gebleken, dat als scholen wel bewaking en toegangspoorten hebben, de principes 'Sociale bewijskracht en Sympathie' wel effectief zijn.

Referenties

(1) In dit artikel worden de social engineer en mystery guest aangeduid met hem/hij. Hiermee willen we de vrouwelijke social engineers/mystery guests niet tekort doen, ook zij zijn zeer succesvol.



TRUSTABLE EXECUTION

The recent revelations of the Meltdown and Spectre attacks on hardware CPUs brings us back to something that The Attributer has addressed in previous articles: emergent properties of complex systems. (See IB2 in 2016: the attribute Emergent). For those readers who might have missed that article, highly complex systems exhibit unexpected and unwanted behaviours that are the result of component interactions in the system. All the system components are working exactly as designed, but what emerges is a behaviour pattern that was unforeseen by the designers. In this case 'the system' is the hardware CPU. Since the mid-90s CPU architecture has been designed to optimise performance. The exact way that these performance enhancement techniques work leads to possible 'covert channels' (sometimes called side-channels) for data leakage. It is beyond the scope of this article to describe the details of these vulnerabilities. What concerns us here is the impact of these revelations on the future of security architecture. They are of major landmark significance. They are not 'run of the mill' discoveries.

Looking back to November 1983, at Lehigh University, Bethlehem, PA, USA, a researcher called Fred Cohen demonstrated the possibility of creating self-replicating code that could 'infect' other code and penetrate the system to the highest root privilege level. He had invented the computer virus.

Fred Cohen's computer virus was a pivotal moment in the development of computer security and malicious attacks on computer systems. It would change the game forever. In the opinion of The Attributer we have just witnessed, in the disclosure of Meltdown and Spectre, another development of equally pivotal significance – another game changer.

We must now abandon all previous assumptions about hardware security that have underpinned the previous twenty years of computer security thinking. In the future we can expect many more hardware vulnerabilities to be discovered. Almost by definition any hardware is vulnerable to 'covert channel' data leakage. This is because when a hardware component operates it can be observed to be doing something, and with enough context information an observer can guess what it might be doing, even if the operation itself is hidden by privilege protection. This was the basis of Paul Kocher's attack on smart cards, to be able to read out the bits of a private RSA key. When a transistor operates it demands a tiny amount of extra power. If you can measure those increments of power consumption you can analyse patterns and interpret what the hardware is doing. Differential power analysis (DPA) does exactly that, and since the smart card is powered from an external source, the differentials are exposed as a covert channel that can be monitored.

So what should we do? Yes, of course, apply the patches for the recent vulnerabilities – but these only hide the problem, they do not solve the fundamental flaw in the hardware design. The word 'patch' is appropriate because that's all it is – a sticking plaster to cover the wound – it does nothing to heal the wound.

We must remind ourselves that security architecture is a holistic thing. SABSA addresses the totality of the systems that are subject to the architecture. It must not make assumptions about the secure independence of one application system from another when they share the same hardware platform. If you do not have a trusted execution platform, you cannot fix the problem at the higher layers of the software architecture.

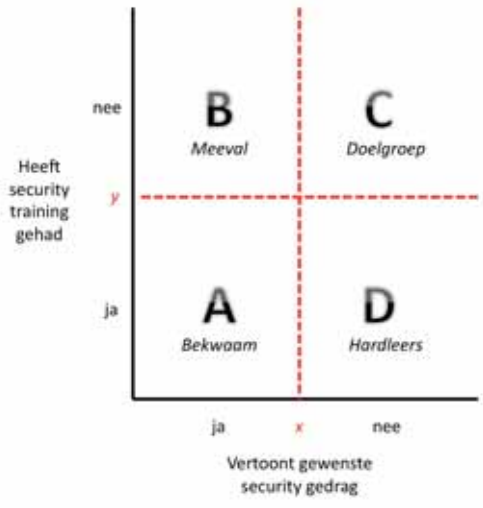
In order to ensure that hardware covert channels (whether or not we have yet discovered them) cannot be used to subvert highly sensitive systems, we must reconsider the architecture of shared hardware platforms, multi-user systems, cloud services on shared servers and the possible escape from the control of the operating system or the hypervisor. The industry hasn't spotted it yet, but those are seismic changes to the way we architect modern systems. Once the patch frenzy is over, there will be some serious debate about the suitability of shared hardware platform architectures, including those for web services and cloud services.

The Attributer

GENERIEKE SECURITY AWARENESS GERICHT OP GEDRAGSVERANDERING VAAK INEFFECTIEF

In marketingland wordt wel gezegd: "De helft van je reclamebudget is weggegooid geld. Je weet van tevoren alleen niet wèlke helft." Dit geldt ook voor security awareness trainingen. Behalve dat daar vaak nog meer dan de helft wordt weggegooid en dat je dat deel van tevoren al kunt weten. Ik heb het daarbij over een situatie waarin de security awareness training gericht is op het bereiken van gedragsverandering. De awareness is een middel en geen doel op zich: 'Iedereen moet jaarlijks een awareness training krijgen'. Het wel en niet gewenste security-gedrag is daarbij vooraf bepaald en vastgelegd, bijvoorbeeld in een gedragscode computergebruik. Daardoor valt objectief te meten of medewerkers zich aan het beleid houden, of niet, of deels.

En ook doel ik op een generieke security awareness training, die voor alle medewerkers in de populatie gelijk is, zonder onderscheid te maken naar hun voorkennis of gedrag. Iedereen krijgt dezelfde e-learning module, dezelfde gekleurde wuppie op zijn bureau en dezelfde postertekst op de koffieautomaat of in de lift te lezen. U merkt; ik heb er al een paar gedaan.



Figuur 1 – effectiviteit security awareness training.

Op de x-as in de grafiek hierboven is de populatie verdeeld in twee groepen: (1) mensen die zich wel (geheel) aan de gedragscode houden en (2) personen die dat niet doen. Op de y-as is dezelfde populatie verdeeld in (1) mensen die een awareness training hebben gevolgd en (2) personen die dat nog nooit hebben ondergaan. De medewerkers zijn dus in te delen in vier groepen: A, B, C en D.

A zijn de personen die een awareness training hebben gevolgd, in uw bedrijf of elders, bijvoorbeeld tijdens hun opleiding. Deze personen houden zich bovendien aan de afspraken in de gedragscode. "De kracht van reclame zit in de herhaling" wordt ook vaak gezegd, maar dan wel vooral door advertentieruimte-verkopers, in de hoop dat u voor het hele jaar tegelijk boekt. Zelf heb ik, en velen met mij, alle klassen van de lagere en middelbare school slechts één keer doorlopen en daarna toch één of meer universitaire studies met succes en in de minimale tijd afgerond. In één keer en succesvol kennis overdragen die daarna een leven lang moet worden toegepast is dus wel mogelijk, wil ik maar zeggen. Economisch gezien heeft het geen nut om personen die al een training hebben gehad en zich ook aan het beleid of de gedragscode houden, nogmaals op te leiden. Dat is weggegooid geld.

B zijn de medewerkers die geen training hebben gehad, maar die zich toch aan de afspraken uit de gedragscode houden. Dat is niet erg verwonderlijk, want veel gedragscodes gaan niet veel verder dan: houd je wachtwoord geheim, klik niet zomaar overal op en denk logisch na als je ineens een erfenis van een Nigeriaanse prins ontvangt via email. Stop dingen die je op straat vindt niet zomaar in je computer, kijk uit met wat je aan software installeert en als er iets raars is met je computer meldt dat dan als security incident. Met gezond boerenverstand kom je immers ook al een heel eind. Ook in deze groep heeft het geen economisch nut een training te geven, want onbewust bekwaam houdt men zich al aan de gedragscode en dat was het beoogde doel uit de inleiding.

C is de droom-doelgroep van security awareness. Ze houden zich niet (geheel) aan de gedragscode, maar dat is (/positief mensbeeld aan) ook geen wonder, want ze zijn niet opgeleid. Als je een grote groep A hebt, kun je heel optimistisch aan een awareness traject beginnen. Bij een grote groep B zou ik zelf minder enthousiast zijn. De meeste medewerkers doen het in dezelfde organisatie immers al vanzelf goed.

Dan resteert groep D. Mensen die wel awareness training hebben gehad, maar zich toch niet aan de gedragscode houden. Deze groep noem ik 'hardleers'. Hierin zitten medewerkers die de cursus niet begrepen hebben of niet kunnen onthouden. Dat is jammer, maar het is geen goed idee om hen de generieke awareness training te geven die gericht is op de gemiddeld intelligente lezer. De security-risico's moeten voor hen misschien nog meer in Jip en Janneke-taal worden toegelicht. In de hardleers-groep zitten echter ook personen die willens en wetens de gedragscode overtreden. Die zeggen: "Ik mag geen bedrijfsdata uitwisselen met een USB-stick, maar wel met een SD-kaartje, want daarover staat niets in de gedragscode." Deze groep creatieve lezers nogmaals de generieke training geven heeft geen nut. En security awareness heeft soms ook een negatief effect.
In mijn eerste werkmaand kregen we als afdeling een e-mailbericht van onze manager. Hij opende klassiek met het goede nieuws. Er was vastgesteld dat we allemaal tijdig ons wachtwoord hadden veranderd en dat de wachtwoorden nu allemaal voldeden aan de aangescherpte en geautomatiseerd afgedwongen nieuwe eisen over voldoende lengte en ingewikkeldheid. Prima en hulde. Helaas was ook gebleken dat sommige medewerkers de nieuwe wachtwoorden hadden geprogrammeerd onder de ongebruikte functietoetsen op hun terminal-toetsenbord. Bij mij wakkerde dit een levenslange belangstelling aan in het maken van macro's, robotisering van toetsaanslagen en het herdefiniëren van toetsenborden. Maar door deze goedbedoelde awareness actie kwamen wel meer medewerkers op een - in de basis - 'slecht' idee.

Als A, B en D weggegooid geld zijn, blijft alleen C over als een mogelijk nuttige investering. In het rekenvoorbeeld in de grafiek komen we dan uit op ongeveer 75 procent weggegooid geld. Bij 30 procent van de medewerkers die awareness hebben gevolgd en 30 procent die zich aan het beleid houden, is er een C-groep van 70x70; een situatie van 49 procent niet-weggegooid geld (zie: reclamebudget). Maar als 70 procent (!!) van de medewerkers zich niet aan de gedragscode houdt, zijn ook technische maatregelen nodig, of meer controle en/of sancties. Of zelfs (horror!) het versoepelen van de gedragscode zelf.

Bij een grote groep A (zeg 90x90) is de organisatie 'klaar': de C is dan zo klein (1 procent) dat het bijna niet meer de moeite waard is om dat laatste contingent te gaan trainen (door iedereen te trainen). Bij een grote groep B (zeg ook 90x90) heeft de organisatie geluk dat het gros van de medewerkers zich vanzelf aan de afspraken houdt. Hierbij heb je ook een kleine groep D. Een ideale en goedkope situatie die niet vaak voor zal komen, maar waarin ook niet meer generiek getraind hoeft te worden.

Bij een grote groep C is een generieke awareness actie op zijn plaats, omdat het veel kan opleveren. Als ook hier een vlak van 90x90 bestaat, betekent dit dat 9 van de 10 medewerkers zich niet aan de gedragscode houden. Dan is er toch wel een serieus probleem, dat ook op andere wijze moet worden aangepakt. Het kan echter in theorie nog erger bij een grote D. Dan zijn veel medewerkers opgeleid, maar doen ze het nog niet goed. Met opzet of omdat ze het gewoon niet begrijpen. Bovendien is groep B (de meeval) dan klein en valt groep C (de echte awareness doelgroep) ook tegen (zijnde ongeveer 9 procent).

Kortom: in de meeste situaties is een groot deel van een generieke security awareness training gericht op positieve gedragsverandering ineffectief. En heb je veel meer aan e-mailfiltering en het blokkeren van USB-poorten, webmail en filesharer-sites om verlies van vertrouwelijke bedrijfsdata en het binnenkrijgen van trojans en RATS te vermijden.
De eerste vraag van uw security adviseur (die u meer awareness training wil verkopen) moet niet zijn: "Wanneer was de laatste awareness training en met welk deelnemerspercentage?", maar juist: "Hoeveel procent van de medewerkers houdt zich aan de afspraken in de security gedragscode?". Want als dat hoog is, heb je vanzelf een grote groep A+B en een (relatief) kleine groep C+D. En dan hoef je geen training meer te organiseren.

Robert Metsemakers is Enterprise Security Officer bij Achmea IT. Robert is bereikbaar via metsemakers@live.com

Achter Het Nieuws

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over de informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kunt u sturen naar ibmagazine@pvib.nl.

TERUGBLIKKEN, VOORUITKIJKEN

Aan het begin van het nieuwe jaar blikken we terug op 2017 en kijken vooruit naar 2018. Wat waren de belangrijkste ontwikkelingen van het afgelopen jaar en wat staat ons te wachten in 2018? De redactie reageert.

Tom Bakker

Terugkijkend op 2017 was het meest opvallend wel de ransomware aanvallen, met als dieptepunt de Wannacry/Petya/NotPetya uitbraken. Op zich niks nieuws qua ransomware, maar bij deze was de impact enorm. In Nederland onder andere bij Maersk en APM terminals, en in Groot Brittannië bij de National Health Service (NHS), waardoor ziekenhuizen platlagen. De verspreiding is uiteindelijk gestopt, doordat iemand bij toeval een zwakte in de code vond.

Nu, bij het begin van 2018, komen opeens kwetsbaarheden van Intel- en AMD-processoren naar boven. Spectre en Meltdown. Die soort hadden we nog niet eerder gezien. Deze kwetsbaarheden blijken al 20 jaar te bestaan! Men ging er blijkbaar van uit dat processoren intrinsiek veilig waren. Niet dus. Een oplossing is ook niet een-twee-drie beschikbaar. Er komen wel patches, softwarematig, maar dat zijn compenserende maatregelen, die weer impact hebben op de prestaties. Daar zitten voornamelijk Cloud providers weer mee. Een echte oplossing zal wel een tijd op zich laten wachten. Tot nu toe hadden hackers het voornamelijk gemunt op het hacken van software. Nu deze kwetsbaarheden algemeen bekend zijn geworden, verwacht ik dat ze hun pijlen nu gaan richten op de processoren, omdat er nog geen robuuste oplossing is (behalve je apparatuur weggooien, wat natuurlijk geen optie is). Er staat voor 2018 nog een hoop ellende klaar met deze kwetsbaarheden in processoren. Want wat is nog niet ontdekt?


Maarten Hartsuijker


Lex Dunn


Tom Bakker

Maarten Hartsuijker

De afgelopen jaren zijn overheden steeds meer gevoelige gegevens over medewerkers en burgers gaan verzamelen. De mogelijkheden van Big Data lonken ook hier als nooit tevoren. De Belastingdienst aggregeert en analyseert binnen haar broedkamer. En de inlichtingendiensten hebben hun sleepnet gekregen om onder andere alle netwerkdata die zij voor hun werk nuttig achten in te zien en te analyseren. Afgelopen jaar zagen we bij de Belastingdienst al dat het uitnutten van de analysemogelijkheden soms vooruitlopen op de noodzakelijke beschermingsmaatregelen die passen bij zo'n grote dataverzameling over ons allemaal. En jaren eerder zagen we al dat ambtenaren het CIOT (de opsporingsdatabase met onze telefoonnummers en IP-adressen) naar hartenlust gebruikten voor andere doeleinden dan waarvoor het is opgezet.
Hopelijk houden de inrichters van de sleepnetdatabanken dit soort voorbeelden uit het recente verleden in hun achterhoofd bij de inrichting van de beschermingsmaatregelen van het sleepnet.
Ook floreerden de Ransomware varianten afgelopen jaar weer als nooit tevoren. Met Wanacry als 1 van de hoogtepunten, waarin recent uitgelekte exploits van een Amerikaanse inlichtingendienst werden ingezet om talloze bedrijven te besmetten en miljarden aan schade en omzetderving te veroorzaken. Hier zijn we in 2018 nog niet van af.
En natuurlijk is daar de cloud met zijn specifieke aandachtspunten waaraan we allemaal nog moeten wennen. Afgelopen jaar lekten er via Amazon S3 buckets met 'out of the box' autorisaties terabytes aan data uit. Data die vroeger achter de bedrijfsfirewalls stonden (en bij fouten enkel onterecht door technisch vaardige medewerkers konden worden ingezien), blijken in de cloud voor de hele wereld toegankelijk te zijn na een autorisatiefout. Komend jaar zullen we in de cloud met elkaar een modus moeten vinden in het veilig gezamenlijk delen van hardware zoals CPU's en GPU's.
Tot slot kijken velen feitelijk al bijna twee jaar uit naar 2018. 25 mei 2018, om precies te zijn. Het moment waar vrijwel elke security- en privacyprofessional momenteel naar toe werkt, is bijna aangebroken. De laatste sprintjes worden volop getrokken om alle klanten vanaf dat moment te (kunnen) bieden waar ze recht op hebben. Is iedereen er klaar voor?

Lex Dunn

2018 begint al goed met een hardware kwetsbaarheid in vrijwel alle in gebruik zijnde processoren, ongeacht fabricaat en/of operating systeem. Is dat vreemd? Eigenlijk niet, als je bedenkt hoeveel logica er in zo'n Intel I7 processor zit. Als je weet dat Google uit ongeveer 10 miljard regels code bestaat (1) en een laatste generatie Intel I7 processor ongeveer 1 miljard transistoren bevat, dan is het niet zo vreemd dat er ook kwetsbaarheden in processoren voorkomen. We zullen in 2018 ongetwijfeld nog meer Spectre- en Meltdown-achtige kwetsbaarheden in diverse soorten hardware gaan zien, want de onderzoeksdrift van de hackers is nu ook daarop gericht. Daarnaast zullen we meer en meer malware zien, die zich niet zozeer richt op het ransomware model, maar die stilletjes gebruik gaat maken van geïnfecteerde machines om een 'mining net' te vormen, en zo Bitcoins en andere digitale valuta te creëren. Daarbij zullen op een gegeven moment ook 'mining nets' van IoT devices gebruikt gaan worden, vanwege de grote beschikbaarheid, en de bedroevende mate van beveiliging. Ook denk ik dat de 'state actors' nog actiever worden dan ze nu vermoedelijk al zijn. Als je de spierballentaal tussen Tim Toupet en zijn Noord-Koreaanse tegenhanger volgt, dan gaan we daarvan geheid nog het nodige merken in de vorm van gerichte aanvallen en afluisterpraktijken. Trouwens, ik zeg wel 'tegenhanger', maar als je het zo op een afstandje bekijkt, zijn het net twee kinderen die in de zandbak spelen en tegen elkaar opbieden: "Mijn pa heeft lekker een grotere auto dan de jouwe!". Tot slot: block-chain. Steeds meer pilots, nieuwe aanpakken voor oude problemen, en ook nieuwe initiatieven. Het is dus te verwachten dat er ook (grootschalige) aanvallen op block-chain mechanismen zullen gaan plaatsvinden. Desondanks wens ik u allen een voorspoedig, veilig en hopelijk ook plezierig 2018 toe!

Links

(1) www.informationisbeautiful.net/visualizations/million-lines-of-code/

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
Kas Clark
Lex Dunn
Maarten Hartsuijker
Hugo Leisink
Rachel Marbus
Bart van Staveren

BLADMANAGEMENT
MOS bv
Deirdre Bernard
José Broekhuizen
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 voor 2018 is nog niet bekend. De abonnementsprijs van 2017 bedroeg € 118,50 (exclusief btw).

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

ISSN 1569-1063

SCIENCEFICTION? NEE!

Mijn zoon is een slimme en knappe vent (van wie zou hij het hebben?) en de laatste tijd is hij bezig om zijn huis te automatiseren; kachel hoger, gordijnen dicht, lichten aan, garagedeur open enzovoort. Allemaal met zijn telefoon, en zijn vrouw vindt het zelfs handig. Zelf twijfel ik altijd een beetje aan die oplossingen; je zal je telefoon maar kwijtraken of je telefoon wordt gehackt … Zit je ineens in de kou, omdat een grappenmaker je kachel uitdeed. Het is natuurlijk mode om alles aan het internet te hangen; koelkast, oven, koffiezetapparaat en ga zo maar door. Of het allemaal even zinvol is, laat ik natuurlijk aan u over, maar ik heb er zo mijn gedachten over. Het woord is al een keer gevallen, namelijk het hacken. Hoe goed we iets ook beveiligen, het is blijkbaar lastig dat allemaal in één keer te doen. Tel het aantal updates op een standaard windows machine daarbij op en u begrijpt dat het voor Microsoft blijkbaar ook onmogelijk is alles ineens goed te doen. We worden steeds ingehaald door de tijd. Ik noemde mijzelf ook wel een hacker, maar ik weet niet of dat terecht is, als je het zo kleinschalig hebt gedaan als ik. Ja, ik heb het navigatiesysteem van mijn auto gehackt, omdat ik geen 200 euro wilde betalen voor een update, maar voor de rest viel er aan mijn auto weinig te hacken. In voorgaande afleveringen vertelde ik u over de Volkswagensleutels die op kinderlijk eenvoudige wijze gehackt konden worden. Wat ik toen nog niet wist, maar inmiddels ben ik daar beter van op de hoogte, is dat een sleutel hacken wel erg simpel is, maar eigenlijk ook niet noemenswaardig. De huidige moderne auto's zijn rijdende computers met als toppunt de Tesla. Elon Musk (één van de grote geldschieters van Tesla) gelooft heilig in deze duurzame oplossing en als je van mooie spullen houdt, dan zal je ook de fraaiheid van deze superauto onderschrijven. Toch blijft het een auto die je van A naar B moet kunnen brengen. Actieradius wordt altijd als een zwak punt gezien, maar een actieradius van 500 km is voor de meeste mensen natuurlijk ruim voldoende. Mijn zorgen zitten ook niet in de actieradius, mijn zorgen zitten in de veiligheid van de auto. Niet de passieve of actieve veiligheidssystemen, maar de robuustheid van het besturingssysteem van de computer die Tesla heet. Alles in deze auto draait om het centrale computersysteem en het zelfrijdend maken van de auto is niet meer of minder dan het installeren van een update. Wil je een hogere topsnelheid? Update installeren. Wil je een andere kleur op je display? Wederom de update. Of die update nu van Tesla afkomstig is of dat je de update zelf hebt gemaakt, maakt niet uit. Lastiger wordt het als de update door hackers is gemaakt. Terwijl jij voor het stoplicht staat, wordt de update op of in je auto geplaatst door de auto die naast je staat. Jij merkt daar niets van. Het licht springt op groen, jij geeft een straal gas om je buurman te imponeren, maar in plaats van vooruit gaat de auto achteruit. Gevolg: auto 30 cm korter en tot op heden weet je niet hoe dat kan. Zomaar een voorbeeldje, en hackers hoeven onder ideale omstandigheden (voor de hacker dan) geen fysiek contact te hebben met de auto. Een hele geruststelling is dat de fabrieksgarantie vervalt als Tesla merkt dat er geknoeid is met de computer. Hoef je alleen nog maar even aan te tonen dat je auto gehackt is. Sterkte daarmee!

Berry

Certificeren? Dan moet u voldoen aan de norm. DNV GL toetst u snel en goed. Maar iedereen houdt van opstekers, niet van standjes. Daarom kijken we bij certificering ook naar wat goed gaat en zelfs nog beter kan. Op die gebieden die voor uw bedrijf of organisatie belangrijk zijn. Aandachtspunten waarop u zélf beoordeeld wilt worden. Certificering die net even verder voert. Want verbetering zit in een klein hoekje.

U kunt ons bereiken via 010 2922 700 of www.dnvgl.nl

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers