iB

INFORMATIEBEVEILIGING

jaargang 16 - 2016

#8

De Business Continuity Privacy eXperience

Reaching Proactive Security

Enterprise control by design

Risicoanalyse: privacy versus informatiebeveiliging

SECURITY ACADEMY

SECO-Institute Certified Officer Certificering

Ook voor docenten Security Academy

Wij zijn trots op onze docenten. Zij hebben onlangs verschillende SECO-Institute certificeringen behaald binnen disciplines van het **Cyber Security & Governance certification program**. De titels die onder andere zijn behaald zijn **Certified Information Security Officer (S-CISO)** en **Certified IT-Security Officer (S-CITSO)**. Wij willen onze docenten met deze mooie prestatie van harte feliciteren!

De Certified Officer titels zijn internationaal de hoogst haalbare erkenningen binnen het certificeringsprogramma van **SECO-Institute**.

Met dit certificeringsprogramma kunt u binnen verschillende security onderdelen opgeleid worden van **beginner** tot **certified officer**. Bij de **Security Academy** kunt u de juiste opleidingen volgen.

Het programma biedt certificeringen in:

- SECO CERTIFIED OFFICER — INFORMATION SECURITY
- SECO CERTIFIED OFFICER — IT-SECURITY
- SECO CERTIFIED LEADER — ETHICAL HACKING
- SECO CERTIFIED OFFICER — PRIVACY & DATA PROTECTION
- SECO CERTIFIED LEADER — SECURE SOFTWARE
- SECO CERTIFIED OFFICER — BUSINESS CONTINUITY
- SECO CERTIFIED OFFICER — CRISIS MANAGEMENT

Voor meer informatie kunt u terecht op onze website of neem contact met ons op per mail of telefoon.

www.securityacademy.nl
info@securityacademy.nl
+31(0)348-40 80 61

KIES JOUW GROEP

We hebben een jaar van tumultueuze verkiezingsuitslagen achter ons: associatieakkoord Oekraïne, Brexit, president van de VS. En wat we bij deze verkiezingen gezien hebben, is dat samenlevingen zich bij het kiezen laten aandrijven door afkeer, soms zelfs demonisatie van de andere kant. Met andere woorden, de groep waar we onszelf mee identificeren wordt kleiner en genuanceerder.
We hebben ook een jaar van bekendwording van grote security incidenten achter ons. Ik noem Yahoo, het Swift-netwerk, de e-mails van de Democratische conventie, ransomware gericht op ziekenhuizen, DDoS aanvallen gericht op de infrastructuur van het internet. En ik vergeet er zeker nog een paar... En er is een terugkerend thema bij de bekendwording van deze incidenten: de betrokken bedrijven wisten het soms eerder, maar wilden het dan niet openbaar maken ter lering voor de grote groep. Dus ook hier is de groep waarmee bestuurders zich op het vlak van security identificeren klein. Dit wordt gerechtvaardigd door een beetje manipulatie van de waarheid om je reputatie te verdedigen. Zolang als het duurt...
De afkeer en demonisatie die door politici gebruikt worden komen ook voort uit manipulatie van de waarheid om je reputatie te zetten of te verdedigen. Dit is hoe de groepsfocus klein gehouden wordt, beperkt tot landsgrenzen of bedrijven in plaats van Europees of werelds. De professionaliteit van de informatiebeveiligers lijdt hieronder. We krijgen niet genoeg incident-informatie gedeeld en het wordt gemengd met desinformatie. Hierdoor zijn we niet goed geïnformeerd over de collectieve huidige stand van zaken.
Wat is er nodig om dit proces om te keren? Ik zie drie krachten die dit bereiken:

- Bestuurlijke macht: wet- en regelgeving forceert ons om met die deling bezig te gaan. Het is meer de stok dan de wortel, maar het is een goede zaak.
- Transparantie: om succesvol te zijn in een grotere groep, moeten we transparanter durven zijn over wat er binnen de groep gebeurt.
- Professionele passie: we moeten kiezen om verkregen kennis en inzicht te willen delen, omdat dit ons als professionals juist collectief meer macht geeft.

En dit blad is natuurlijk een instrument bij toepassing van die tweede en derde krachten. Deze uitgave weer een aantal artikelen waarbij transparante kennisdeling centraal staat. Kies voor de grotere groep!

Lex Borger, hoofdredacteur

In dit nummer

DE BUSINESS CONTINUITY & PRIVACY EXPERIENCE

Het is de vraag of business-, juridische- en IT-medewerkers elkaar ooit zullen begrijpen. Ze hanteren immers ieder een eigen taal en een eigen begrippenkader. Toch is het essentieel om de brug te slaan tussen deze doelgroepen om de bedrijfscontinuïteit en de bescherming van de persoonlijke levenssfeer (privacy) te borgen. Bij het Ministerie van Buitenlandse Zaken (BZ) is op basis van een evolutionair proces een aanpak ontstaan die deze problematiek adresseert. De ervaring leert dat deze aanpak ook door de betrokkenen als een beleving wordt ervaren. In dit artikel wordt de aanleiding en de werkwijze beschreven die leidt tot dit enthousiasme.

Vanwege de wereldwijde connectiviteit van het internet zijn nationale- en bedrijfsmatige grenzen niet meer relevant vanuit het gezichtspunt van de kwaadwillende. Daarnaast convergeert de fysieke en de digitale werkelijkheid naar één geheel in het kader van 'the Internet of Things'. Tegelijkertijd zijn consumenten, burgers en medewerkers steeds veeleisender ten aanzien van overheidsdiensten. BZ hanteert een door de bestuursraad vastgestelde i-Strategie waarbij de (moderne) diplomaat optimaal digitaal wordt ondersteund, waar dan ook ter wereld.

Problemen

Zoals aangegeven door onder andere het Nationale Cyber Security Centrum (NCSC) professionaliseert de georganiseerde misdaad zich qua cybercapaciteit naar het niveau van statelijke actoren, zoals de veiligheidsdiensten die wereldwijd actief zijn [1]. Daar waar in het verleden een veiligheidsdienst heimelijk probeerde te infiltreren, wordt een cybercapaciteit vandaag de dag steeds meer gezien als een cyberwapen in een permanente wedloop, waarbij een gehele organisatie platleggen als één van de alternatieven wordt gehanteerd. Zowel private bedrijven als overheidsinstellingen zijn regelmatig doelwit van een cyberaanval waarbij de organisatie volledig wordt platgelegd. (zie kader).

De toenemende afhankelijkheid van cyber en de verhoogde capaciteiten van kwaadwillenden maakt dat BZ intensief investeert in haar cyberweerbaarheid. Deze cyberweerbaarheid mag echter niet ten koste gaan van de bescherming van de privacy van burgers en medewerkers van BZ.

Cyberaanval Duitse Bondsdag

In mei 2015 was de Duitse Bondsdag doelwit van een zware, meerdaagse aanval. Het lukte experts niet de aanval af te wenden en daarop heeft de Bondsdag zelf haar systemen platgelegd om te voorkomen dat de aanvallers bij gevoelige informatie konden. De Duitse overheid concludeerde dat het vervangen van hele IT-systeem waarschijnlijk de enige optie is om de hackers volledig naar buiten te werken.

Tegelijkertijd met de toenemende cyberdreigingen zien we een trend naar het gebruik van clouddienstverlening. Ook bij BZ wordt op internet gebaseerde dienstverlening aan burgers en medewerkers beproefd, voor bijvoorbeeld reisadviezen aan burgers, maar ook een wereldwijd systeem voor contract- en relatiebeheer op ambassades. Het spreekt voor zich dat dit ook weer specifieke beveiligingsvraagstukken oproept.

Daarnaast bevindt BZ zich over de hele wereld en betekent beschikbaarheid tijdens openingstijden bij BZ een 24/7 beschikbaarheid, waar dan ook ter wereld. Op dit punt wijkt BZ, maar ook het Ministerie van Defensie, fundamenteel af van andere departementen. De internationale context brengt ook mee dat BZ moet zorgen voor de vertrouwelijkheid van EU- en NATO-berichtenverkeer en daardoor kan BZ zich niet beperken tot de standaard beveiligingseisen die voor de rijksoverheid gelden, de Baseline Informatiebeveiliging Rijksdienst (BIR).

BIR
De BIR biedt één normenkader voor de beveiliging van de informatievoorziening van de Rijksdienst. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. Het zorgt voor één heldere set afspraken.

Bovenstaande ontwikkelingen zijn zo omvangrijk en verstrengeld dat deze problematiek het IT-domein ver overstijgen en een geïntegreerde aanpak noodzakelijk is om risico's in kaart te brengen en waar nodig af te dekken met maatregelen. De beveiligingsfilosofie van BZ wordt daarom via de Business Continuity & Privacy eXperience (BCPX) door de beleidssector gedragen.

Oplossing

Om ervoor te zorgen dat informatiebeveiliging geen exclusieve IT-aangelegenheid wordt, heeft BZ gekozen voor een methodiek waarbij de verantwoordelijke bedrijfsonderdelen middelen tot hun beschikking krijgen waarmee de directies in staat worden gesteld om zelf verantwoordelijkheid te nemen voor het gerealiseerde beveiligingsniveau. Deze middelen bestaan uit methodieken die een directie helpen na te denken over de eisen die zij stellen aan de beschikbaarheid, integriteit en vertrouwelijkheid van hun processen, informatie en systemen.

De directies hoeven deze methodieken niet zelfstandig toe te passen, maar worden in begeleide analysetrajecten hierin meegenomen.

We hebben het hier over een kort, cyclisch analysetraject waarbij de verschillende analyses in een workshopvorm (ook wereldwijd via videoconferencing) worden uitgevoerd. Bij deze workshop werken wij vanuit een creatieve benadering, we werken niet met standaard dreigingenlijsten, maar maken gebruik van de veelzijdige kennis en kunde van de deelnemers aan de workshop.
Om ervoor te zorgen dat de aandacht en betrokkenheid bij dit onderwerp na de workshop niet direct wegzakt, hanteren wij de regel dat als de workshop op dag X plaatsvindt, de directie een dag later het concrete resultaat ziet in de vorm van een rapportage. Deze voortvarende manier van werken sluit goed aan bij de manier van werken van het primaire proces bij BZ. Wat deze methode tevens tot een succes maakt, is dat we deze analyses zo vroeg mogelijk in verander- of ontwikkeltrajecten uitvoeren (continuity, security & privacy by design) en het feit dat we de analyses met een businessinsteek in plaats van een technische insteek uitvoeren.

Verschillende analyses
De verschillende analyses die worden uitgevoerd binnen BZ zijn:
1. Quickscan(s) informatiebeveiliging (Business Impact Analyses)
2. Privacy Impact Assessment(s)
3. Baseline check(s)
4. Aanvullende risicoanalyses (Dreigingen- en kwetsbaarheden analyse)

Iedere analyse leidt tot een geprioriteerd beveiligingsplan voor de directie waar de analyse voor is uitgevoerd. De resultaten




***Irene de Leeuwerk**, Adviseur risicomanagement–BZ, irene-de.leeuwerk@minbuza.nl*
***Edwin Haaring**, Adviseur risicomanagement & compliance–BZ, edwin.haaring@minbuza.nl*
***Maxime Nieuwenhuizen**, Adviseur I-strategie en risicomanagement-BZ, maxime.nieuwenhuizen@minbuza.nl*
***Ben Elsinga**, Adviseur risicomanagement–BZ/Capgemini, ben.elsinga@minbuza.nl of ben.elsinga@capgemini.com*

van alle analyses worden vervolgens centraal samengevat in één spreadsheet voor geheel BZ, met genormaliseerde risico-indicatie. Op deze wijze ontstaat er een centraal overzicht en inzicht en kan over geheel BZ risicogebaseerd worden gestuurd. Dit overzicht kan ook worden ingezet voor de toezichthouders als een belangrijk startpunt voor het verrichten van de interne controles en voor het genereren van managementinformatie over het risicomanagement en de borging van de privacy.

Randvoorwaarden

De BCPX-aanpak wordt niet zomaar een succes in (overheids)organisaties. Er is een aantal randvoorwaarden om deze aanpak tot een succes te maken.

Allereerst is een sponsor op CxO-niveau ten zeerste aan te bevelen om organisatiebreed aandacht te vragen informatiebeveiliging- en privacy. Bij BZ is dit de plaatsvervangend Secretaris-Generaal, die tevens de CIO van BZ is. Uiteraard moet deze sponsor wel een team onder zich hebben die hem adviseert en ontzorgt.

Daarnaast werkt het positief als er voor de directies een duidelijk centraal contactpunt is. BZ voert hiervoor het beleid van de 'one stop shop', de gehele organisatie wordt begeleid door een vast team van risicomanagementadviseurs. Ook van belang is dat de begeleiders voldoende kennis en ervaring hebben en dat zij ook de actualiteiten blijven volgen over bijvoorbeeld nationale en internationale wet- en regelgeving. De begeleiding vanuit het team stopt niet na het uitvoeren van de analyse, maar ook de verslaglegging is onderdeel van de dienst die aangeboden wordt. Zo ontneem je de directie niet alleen veel werk, maar zorg je ook voor uniformiteit in de verslaglegging.

De directies organiseren wel zelf de workshops en nodigen hun eigen vertegenwoordigers uit. Dit is belangrijk voor een hoge opkomst en draagvlak voor het resultaat van de analyses. De verantwoordelijkheid blijft wel liggen bij de directies zelf en het is ook belangrijk dat zij die verantwoordelijkheid niet uit het oog verliezen. De directie zelf is dan ook degene die het verslag ondertekent en deze analyses inclusief beveiligingsplan in het digitale archief archiveert en de uitvoering ter hand neemt.

Governance

Een uitdaging voor de organisatie van IB & privacy van BZ is dat een groot deel van BZ-medewerkers internationaal onverplaatsbaar is en medewerkers letterlijk iedere drie tot vijf jaar een andere functie vervullen op een andere plek in de wereld. Dit maakt de borging van kennis lastiger. Het inzicht en overzicht van de uitgevoerde analyses en de resultaten hiervan ontstaat op basis van de eerdergenoemde spreadsheet en is volledig risicogebaseerd vanuit het oogpunt van continuïteit en borging van de privacy. Denk hierbij ook aan de meldplicht datalekken en de Europese wetgeving rondom de borging van de privacy.

Voor de dagelijkse en periodieke aansturing zijn zowel centrale en decentrale gremia ingericht. De noodzakelijke ondersteuning vindt plaats vanuit het centrale team. Daartoe heeft het team meerdere compliance- en projectadviseurs beschikbaar om de organisatie te ondersteunen en toezicht te houden op het grote aantal externe leveranciers. Daarnaast heeft BZ het plan om op korte termijn de controllers van iedere directie of ambassade een rol te geven bij de periodieke evaluatie en actualisering van IB-plannen en maatregelen.

Succesfactoren

Uit bovenstaand verhaal is een aantal succesfactoren af te leiden dat zorgt voor de juiste BCP eXperience, te weten:

1. Commitment en betrokkenheid vanuit de top en vanuit de directeur van een directie
2. Zorg voor een mix aan competenties binnen het team en tijdens de risicoanalyseworkshops en privacy impact assessments (bijvoorbeeld zowel business-, IT-, IB- en privacy-kennis)
3. Bedrijfscontinuïteit en privacy worden via een geïntegreerde one-stop shop-benadering uitgevoerd
4. Resultaten van risicoanalyseworkshops (opzet) en privacy impact assessments worden direct doorgeleid naar de compliance- en projectadviseurs (bestaan en werking) binnen het centrale cybersecurityteam
5. Vanuit IB niet als politieagent optreden richting directies, maar als hulpmiddel: het ontzorgen van de business en transparant zijn over voortgang en resultaten

Het vervolg

BZ gaat op de ingeslagen weg door om alle bedrijfsprocessen BCPX-compliant te maken. De komende tijd zal ook in het teken staan van het compartimenteren van de informatievoorziening om een eventuele impact van compromitteren te verkleinen. Onderdeel hiervan is een actief Cloud-beleid om de wendbaarheid te vergroten en de risico's over meer onderdelen binnen de informatievoorziening te spreiden. En 'last but not least' een continue aandacht voor het beveiligingsbewustzijn van eindgebruikers. Want cybersecurity is veel meer dan alleen techniek!

Links

[1] NCSC (2016) "Cybersecuritybeeld Nederland 2016: Beroepscriminelen steeds groter gevaar voor digitale veiligheid in Nederland." https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html

IN CONTROL

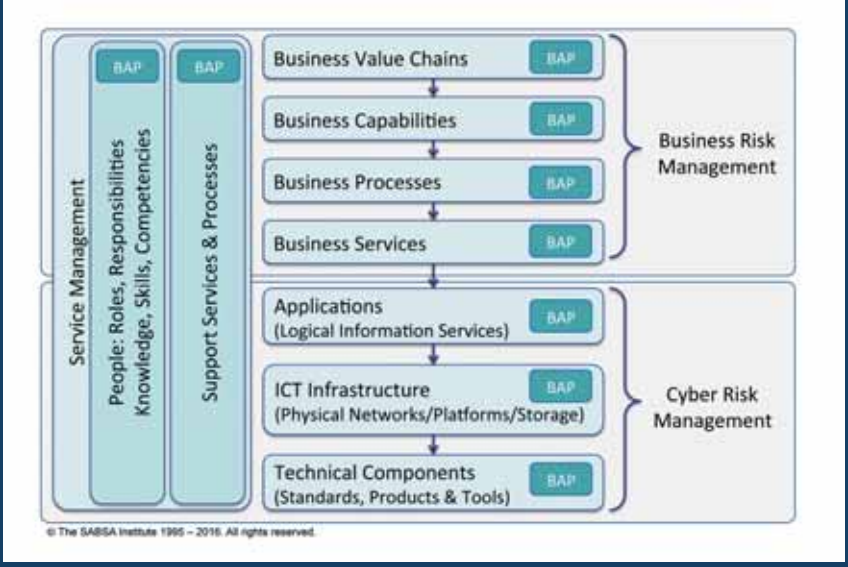
The US Sarbanes-Oxley Act of 2002 has had a huge influence on both American businesses and those in the rest of the world, especially those who want to do business with or in the USA. Section 404 of the act tells us that the management has to be in control, and that the auditors must verify this. A manager must sign a formal statement to declare that he or she is in control.

That immediately begs a question: How can I be sure that I am in control? And more importantly, how can I demonstrate to the auditors that my statement is true? After all, that's what's important with any compliance requirement – being able to show others that you are indeed compliant. Hmmm. That ability to demonstrate being in control might be tough, but don't worry, SABSA can come to your rescue here. Let us first look at what being in control might mean. The Macmillan Dictionary gives us a generic definition: Someone who is in control has the power to make decisions and decide what should happen. Examples: Dr Marion is the person in control of all medical decisions at the hospital. The governing board is in control of the school's budget.

Wikipedia gives a more business-focused definition, in which performance management is introduced:

A management control system (MCS) is a system which gathers and uses information to evaluate the performance of different organizational resources like human, physical, financial and also the organization as a whole in light of the organizational strategies pursued.

These definitions lead us nicely on to the multi-tiered SABSA Business Attribute Profile (BAP) as a means to break down the business into a series of attributes that are the key performance indicators at every level of the Business Stack. The diagram shows this SABSA concept.



The first thing to recognise is that 'to make decisions and decide what should happen' is another way of saying 'manage the business risks'. The diagram shows the way in which risk management (which is at the heart of the SABSA framework and methodology) is distributed through the layers of the stack.

The diagram indicates that a SABSA BAP can be defined at every level. The Business Attribute 'In Control' is one associated with the high level value chain – the business itself, but of course that must be inherited downwards through the stack levels, interpreted into many more specific attributes appropriate to the various levels.

Each attribute is defined within the context of the stack layer, and each one is assigned a measurement approach, a specific metric and a performance target. The attributes are 'proxy assets' for the highest-level asset, Business Value, and the performance targets are an expression of risk appetite with regard to acceptable risk performance of those assets. SABSA defines risk as being the uncertainty of outcome for both grasping opportunities for enhancing business value, and for mitigating threats that might undermine business value. So if you adopt SABSA as your method of controlling, managing and reporting business risk, your done! You're in control and you can demonstrate that by reporting performance.

The Attributer

Reaching Proactive Security

WITH SIEM AND THREAT INTELLIGENCE

The classical reactive posture is no longer sufficient against the current threat landscape and new defense mechanisms are required to deal with Advanced Persistent Threats (APT). Security Information and Event Management (SIEM) systems give a holistic view of an organization's ICT security. Their capabilities provide invaluable help to handle daily security tasks such as anomalous/malicious events detection and investigation, but unfortunately in a reactive fashion. However, to become proactive, we need to consider the overall threat landscape: by knowing exactly what is happening outside our network, we can take the right security measures to harden our infrastructure against future threats. This can be achieved by combining a SIEM solution with Threat Intelligence (TI).

SIEM is a solution that provides a bird's eye view of an IT infrastructure. It fulfills two main objectives: detecting in (near) real-time security incidents, and efficiently managing logs. From a high-level point of view a SIEM collects information, such as logs, events and flows, from various devices on a network, correlates and analyzes the data to detect incidents and abnormal patterns of activity, and, finally, stores the information for later use (reporting, behavior profiling, etc.). When successfully deployed and configured, a SIEM helps organizations by providing the following capabilities:

- Discover internal/external threats.
- Monitor (privileged) user activity and access to resources.
- Provide log management and compliance reporting .
- Support incident response.

For log management, the SIEM will gather logs and events from a heterogeneous collection of data sources which can be grouped into four categories:

- Network devices (routers, switches, etc.)
- Security devices (intrusion detection systems [IDS], firewalls, etc.)
- Servers (Web, mail, etc.)
- Applications

Regardless of the vendor, SIEM solutions present the following architecture, although terminology differs between vendors. For each device, a collector will be used to gather and normalize log information before forwarding the logs to the processing engine — the heart of the SIEM where correlations and analyses take place. Finally, the logs will be stored in a database for a certain amount of time conform to the organization's retention policy. This typical architecture described above can be depicted as shown in figure 1.

The Real Value of Logs, Events, and Flows

A SIEM system can make use of several information types. The primary type is log data, meant for several purposes such as debugging, system administration, and security audits. The most

commonly used standard for logging is Syslog [1]. Depending on the device/technology, the standard can change. For instance, in the case of Web servers, most of them will use the Common Log Format [2] or other proprietary formats.
Another type of information that can be retrieved by a SIEM is event. Events are produced by security devices or controls such as Intrusion Detection/Prevention System (IDPS) or Identity and Access Management (IAM) systems. It can be, for example, input validation failures (e.g. invalid parameter names/value, protocol violations) or application errors and systems events (e.g. runtime errors, connectivity problems, performance issues, etc.). Events can be correlated together with other information to provide higher intelligence into log management.
Finally, the last type of data a SIEM can use is traffic flow [3], providing a good overview of the network activity. The two main standards are NetFlow (RFC 3954) and IPFIX (RFCs 5101 and 5102). These two formats provide information about the lower layers of the OSI model up to the network layer. In order to obtain some visibility on the application layer, some vendors have proposed application-aware flows which help detect threats through the analysis of the packet content, using Deep Packet Inspection (e.g. IBM's QFlow).
The central engine will correlate all of the gathered information by using several algorithms and data-mining techniques. These techniques aim to identify suspicious patterns and behaviors, and provide great help for intrusion detection and auditing. Compared to an ordinary logger, a SIEM system can use various conditions to check whether certain events are matching a rule, and depending on the latter, an alert can be triggered. We can list four categories of conditions:

- **Event Based:** An IDS reports a signature X targeted at host Y and vulnerability scanner knows that Y is vulnerable. It triggers an alert.
- **Rule Based:** If activities X + Y + Z occurs, then do A, or if X repeats more than three times in interval Y then do Z.
- **Anomaly Based:** If the traffic on port X exceeds the standard deviation of historic traffic patterns then trigger an alert.
- **Risk Based:** If attack type is destructive (e.g. buffer overflow versus port scan), and target is a critical asset (production server versus regular workstation), then trigger an alert.

Some event standards have been proposed to improve interoperability and simplify integration of devices. For example, ArcSight came up with the Common Event Format [4], IBM proposed the Log Event Extended Format and Splunk proposed the Common Information Model.

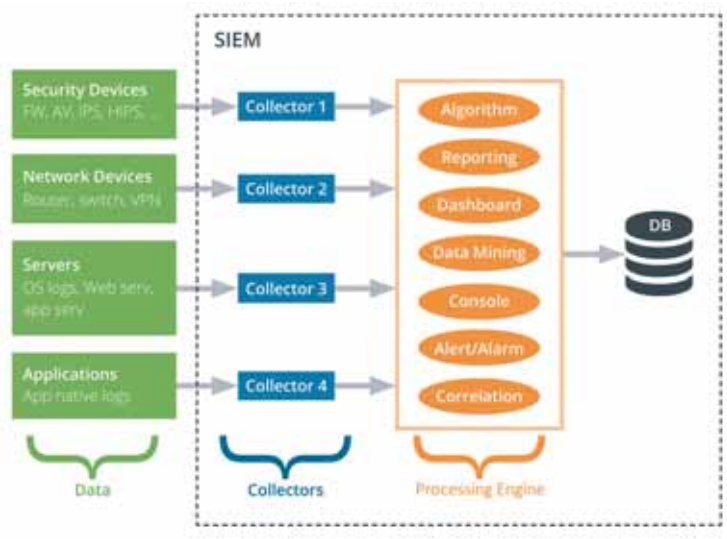


Figure 1 - Typical SIEM Environment

Limitations

Deploying a SIEM solution can be quite complex and expensive: the price of appliances, the time for configuration and tuning, and the expertise required for daily use/maintenance can discourage customers. After purchase and deployment, the recurrent question is "now what do we do?" and enterprises answer that with a 'monitor-and-respond' strategy [5]. By using the SIEM in a signature-based defense approach, the security team (or the security operation center [SOC] team) will monitor activities and regularly update the security devices with signatures of known threats.
Moreover, since the signature-based approach only protects from known threats, the anomaly-based approach, which focuses on detecting abnormal behaviors, should in theory help detect unknown threats, but practically it significantly increases

Guillaume Dupont is a security consultant at Capgemini. His work is focused on SIEM solutions and threat intelligence. He is reachable at guillaume.dupont@capgemini.com.

Once integrated in a security lifecycle, it enhances the security level and awareness of an enterprise and helps business continuity.

the false-positive rate. The direct consequence is the time required by the security team to investigate them, increasing the chance of missing true-positives. In a survey of the Ponemon Institute, they discovered that on average a company will have up to 17,000 alerts per weeks, but only 700 will be investigated!
A Ponemon Institute study [6] found that companies spend $1.27 million annually on average by wasting time responding to inaccurate and erroneous intelligence. In addition, the rise of APTs makes it clear that this traditional reactive security posture is no longer sufficient. With shrinking security budgets [7], companies need to find new efficient ways to defend themselves. The question we have to answer is: How do we get ahead of threats? It is time to become proactive and take a step ahead with Threat Intelligence (TI).

Threat Intelligence - Definition

If we first consider the word 'intelligence' by itself, we start looking at the definition by Edward Waltz [8]:
"The information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding, is the product that provides battle space awareness."
Let's consider now the definition of 'cyber threat intelligence' according to Jon Friedman and Mark Bouchard [9]:
"It is the knowledge about adversaries and their motivations, intention and methods that is collected, analyzed and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise."
In summary, it is important to understand that TI is more than just information: it gives us an analysis of adversaries and their motivations and methods, based on the collection of data that is enriched by using context. Once integrated in a security lifecycle, it enhances the security level and awareness of an enterprise and helps business continuity.

Why Use Threat Intelligence?

TI gives insights on attackers and their capabilities, providing invaluable information to enhance the security level. When companies use and correlate TI provided by external parties with internal information collected by their SIEM solution, defenders have a better vision of attacks in their context and can proactively defend themselves against emerging threats to the business. They can focus their actions on several crucial points to efficiently protect themselves. TI helps in answering the following questions:

- **Who is attacking:** TI helps defenders attribute attacks/malicious activities to certain groups (cyber criminals, hacktivists, government/national agencies, etc.)
- **Why they are doing it:** knowing who is behind an attack helps defenders understand their adversary's motivations, how much effort they would put into an attack (APT vs opportunistic attacks), and how business/industry-specific such attacks could be.
- **What they are after:** with this information, defenders can prioritize their actions based on the importance of the asset or assets the attackers are targeting.
- **How they are proceeding:** the tactics, techniques, and procedures (TTPs) give insight about the way adversaries proceed, the tools and infrastructures they use, and more.
- **Where they come from:** correlating an adversary's country of origin with its geopolitical situation can help defenders understand their enemies.
- **How to recognize the attackers:** also dubbed indicators of compromise (IOC) or artifacts, these technical telltales (IP addresses, hashes, etc.) provide clear information that can be used to detect and signal a malicious presence.
- **How to mitigate them:** information about the steps a company can take to protect itself.

Thanks to the efforts of MITRE, standards have been created to help people retrieve, use, and create TI: Cyber Observable eXpression (CybOX) provides a common structure for representing IOC [10]. Structured Threat Information eXpression (STIX) is a language for the specification, capture, characterization and communication of threat information [11] Trusted Automated eXchange of Indicator Information (TAXII) defines services to leverage the share of threat information [12]. TI can be retrieved from various sources, such as cyber security vendors, independent labs and researchers, open source projects, government and industry groups.

Threat intelligence can be presented at two different levels, depending on the intended audience. On the one hand it can be at a strategic-level: it is human-readable, not too technical, and is meant to be solely processed by humans (e.g. C-suite personnel) to give them insight into the threat impact on business continuity, helping them make the right decisions. Typical formats of strategic intelligence are security industry reports or newsletters for instance. Alternatively, intelligence can also be at the operational-level: once retrieved by SOC analysts, this machine-readable data is consumed by devices to make them able to act upon threats. Operational intelligence is XML-formatted data to ease the processing.

Dismissing Irrelevant Information

There are a number of reasons companies should use TI. One of the most useful is the ability to decrease the amount of time spent on analyzing alerts concerning irrelevant threats (e.g. attackers probing vulnerabilities not present in the network) With good intelligence, an enterprise can easily dismiss irrelevant indicators to weed out false positives and therefore focus on the actual threats it is facing.

If you work for a bank, for example, you could make sure to use TI tailor-made for financial institutions from security vendors or partners (e.g. other banks which may have seen new threats), giving you the right intelligence to defend against business threats. Moreover, you could retrieve generic TI (applicable to any business) to help preventing leaks of intellectual properties or employees' personally identified information (PII). TI also supports vulnerability management, as it provides a way to prioritize indicators and patches, helping IT staff fix the most dangerous vulnerabilities first.

Due to the different types of TI and their broad applications, there are several ways to consume TI. It can be applied from a strategic to an operational level, several groups can benefit from such intelligence and help keep the business running. TI becomes an integrated part of the security lifecycle involving many actors within the enterprise.

SIEM & TI - Security monitoring workflow

Let us consider the flowchart in figure 2 to understand how TI can be combined with a SIEM.

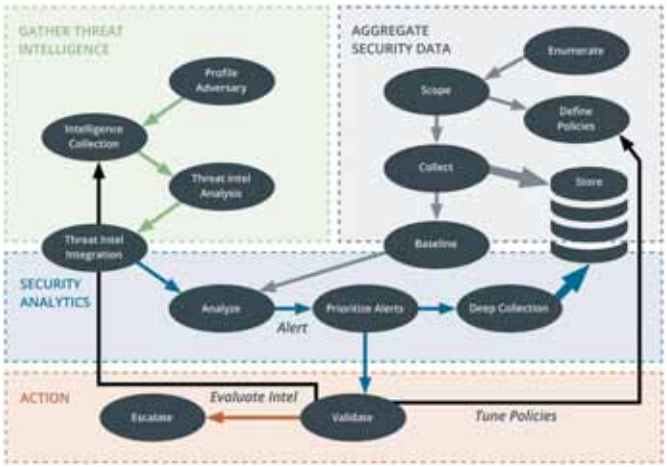


Figure 2 - Security monitoring workflow. (Source: Securosis.com)

We explained the upper right-side of the above diagram in the first section of this article, discussing the reactive security with SIEM. Let's examine the remaining parts.

The upper left-side depicts the collection of TI. Before we can start to collect TI, we first must define and profile our adversaries that play a role in our business risks. Then we can select the right TI feeds that will truly leverage our security posture. Next, we can start collecting and analyzing intelligence, which means reviewing the intelligence to make sure it is actionable. We can now proceed to integrate TI with the SIEM baseline.

In the Security Analytics part of the diagram, we can start analyzing our environment like it is done in the standard SIEM approach, but this time correlating our detection mechanisms (signature and anomaly based) with the TI relevant to our business. Upon detection of an incident, one can prioritize alerts according to the number, the frequency, and the types of indicators which triggered them. According to their priority, we may want to collect deeper — which means collecting more information from the devices involved by querying the databases; this makes it easier for further forensics investigations. Finally, as shown in the Action part, once alerts are reviewed by the security operations team, they can be validated if it's a true positive or discarded in case of a false positive. In the latter case, the intelligence can be evaluated and the policies tuned to avoid further false alerts. After validation, the alerts can be escalated to the incident response team.

Four Qualities of Actionable Threat Intelligence

The advantages of using TI with SIEM is indisputable: nowadays a good SIEM solution ships with support for threat intelligence integration. All vendors are well aware that, to be taken seriously, they have to answer the growing demand for easier and better TI integration. As shown in the flowchart above, the collected TI will have to be assessed in terms of quality and effectiveness. Sergio Caltagirone, Chief Scientist of the Center for Cyber Intelligence Analysis and Threat Research, identified four qualities that intelligence has to meet to be actionable [13]:

- **Relevance:** TI teams must ensure the intelligence is pertinent to the business; measurable by positive hits or real alerts once deployed in the environment.
- **Completeness:** TI must be detailed enough, and provide sufficient context, to guarantee effective detection.
- **Timeliness:** To have a valuable impact, intelligence must be retrieved and processed as fast as possible.
- **Accuracy:** To ensure effective detection, the TI must have few false positives and be highly accurate.

All these aspects can be assessed at different levels by parties involved in a complete security lifecycle, as detailed according to the Active Cyber Defense Cycle [14]. These qualities can be used as criteria to acknowledge the efficiency and usefulness of the retrieved TI.

Finally, by combining internal and external threat intelligence, defenders have a way to empower real-time threat identification; for instance, it now becomes easier to detect malware that is communicating with C&C servers belonging to a certain campaign, to match past/historical internal log data with current threat intelligence, or even to validate correlation rules and improve baselining alerts, therefore reducing false positive and the waste of time and money.

Conclusion

SIEM solutions are great tools but their scope is limited to their internal monitored network. To improve our defense, we also need to consider the overall threat landscape by using TI. It corresponds to detailed and enriched information about current threat actors, their methodologies, tools and motivations, at a worldwide scale. By combining such intelligence with our own internal information from the SIEM solution, we can truly enhance our ability to detect security threats and take proactive defensive measures in accordance with our required security level.

Links

Bibliography

[1] R. Gerhards, "The syslog protocol," March 2009. [Online]. Available: https://tools.ietf.org/html/rfc5424. [Accessed 25 October 2016].

[2] W3C, "Logging control in w3c httpd," July 1995. [Online]. Available: https://www.w3.org/Daemon/User/Config/Logging.html. [Accessed 25 October 2016].

[3] T. Z. a. B. C. ,. O. 2. J. Quittek, "Requirements for IP flow information export," October 2004. [Online]. Available: https://www.ietf.org/proceedings/68/ipfix.html. [Accessed 25 October 2016].

[4] A. Inc., "Common Event Format," 2010.

[5] J. F. a. M. Bouchard, " Definitive Guide to Cyber Threat Intelligence," CyberEdge Press, 2015.

[6] P. I. LLC, "The cost of malware containment," January 2015.

[7] B. Hat, "Black Hat Attendee Survey," July 2015.

[8] E. Waltz, " Information Warfare Principles and Operations," Artech House, Boston, MA, USA, 1998.

[9] J. F. a. M. Bouchard, "Definitive Guide to Cyber Threat Intelligence," CyberEdge Press, Annapolis, MD, USA, 2015.

[10] MITRE, "Cyber Observable eXpression," [Online]. Available: https://cyboxproject.github.io/. [Accessed 1 November 2016].

[11] S. Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression," 20 February 2014. [Online]. Available: http://stixproject.github.io/getting-started/whitepaper/. [Accessed 1 November 2016].

[12] M. D. C. S. Julie Connolly, "The Trusted Automated eXchange of Indicator Information," 2 May 2014. [Online]. Available: http://taxiiproject.github.io/getting-started/whitepaper/. [Accessed 1 November 2016].

[13] S. Caltagirone, "CART: The 4 Qualities of Good Threat Intelligence," 1 July 2015. [Online]. Available: http://www.activeresponse.org/the-4-qualities-of-good-threat-intelligence/. [Accessed 1 November 2016].

[14] R. M. Lee, "Threat Intelligence in an Active Cyber Defense (Part 1)," 17 February 2015. [Online]. Available: https://www.recordedfuture.com/active-cyber-defense-part-1/. [Accessed 1 November 2016].

Mr. Rachel Marbus
@rachelmarbus op Twitter

COMPUTER SAYS NO(2)

Nog niet zo lang geleden tweette mijnheer Akerboom (korpschef Politie Nederland) dat hij zo trots was dat data-analyse het belangrijkste middel zou gaan worden in de opsporing. Het klassieke verhoor, forensisch onderzoek alsmede 'de tap' zouden er allemaal niet meer zo toe gaan doen. Alles met de mooie benaming 'Opsporing 3.0'. Ik ben een groot voorstander van innovatie, maar dit vond ik toch echt eng worden. Data-analyse inzetten als een primair opsporingsmiddel is niet zomaar iets. Zeker als je weet dat dit middel al sinds jaar en dag omstreden is. Voor je het weet word je als vrouw preventief even vastgezet terwijl je terugkomt van je vakantie op de Antillen. Uit onderzoek bleek namelijk dat steeds meer vrouwen in de drugscriminaliteit zitten, met name uit de hoek van de Antillen. Oh, en de cijfers tonen aan dat van alle drugskoeriers 25% vrouw is. En dat was nou net aan dat algoritme toegevoegd. Dat je alleen reisde, gaf de doorslag, want dat doen doorgaans alleen de drugskoeriervrouwen en niet vrouwen die lekker op vakantie gaan.

Hoe weet je nu eigenlijk of die cijfers allemaal wel kloppen? En hoe moet je dat dan gaan toepassen? Kun je dat soort cijferkunde eigenlijk wel toepassen op iedereen? En hoe ga je dat dan in algoritmes stoppen? En hoe gaat die dan een berekening uitvoeren ofwel, op welke data wordt dat dan toegepast? Dat zijn nogal wat fundamentele vragen waarbij het antwoord niets anders kan zijn dan: dat weten we eigenlijk nooit helemaal zeker. En dan heb ik het nog niet eens gehad over wat dan bij de opsporing bedoeld wordt met het begrip data-analyse.
Niet voor niets kent de Wet bescherming persoonsgegevens een bepaling die stelt dat geautomatiseerde beslissingen niet zonder meer toegestaan zijn. Ik citeer: "Niemand kan worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking van persoonsgegevens bestemd om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid." Onder de verordening wordt dat nog verder aangescherpt. Er moet een mens van vlees en bloed aan te pas komen.
Mensen zijn bevooroordeeld. Mensen hebben een eigen normatief kader. Mensen schrijven code. Mensen geven input. De computer rekent het uit. Niets in deze keten is objectief. Data is niet objectief. Een berekening ook niet. De uitkomst ook niet. En dit is niets nieuws! Jaren geleden al toonden onderzoekers aan dat het ontwerp van de toen veel gebruikte games zeer gekleurd was. Sterker nog: het was eigenlijk helemaal niet gekleurd. In praktisch alle games waarbij avatars konden worden gekozen, bestond slechts een optie voor 'andere huidskleur dan wit' (een rastafari) en waren vrouwen doorgaans altijd 'sletten'. Wat wilde het geval? Dé gamedeveloper was wit, rond de 25-30 jaar, van westerse afkomst en man. Nu is daar gelukkig wel verandering in gekomen in de loop van de jaren, echter de kern van de bevindingen staat nog steeds overeind. Mensen zijn bevooroordeeld en werken vooral vanuit het kader dat zij kennen zelfs zonder dat zij zich daarvan bewust zijn, die bevooroordeeldheid stoppen zij in code. En om nou in de opsporing primair in te gaan zetten op bevooroordeelde data-analyses? Dit is echt geen spelletje, maar gaat om zaken van levensbelang waar grondrechten onder druk staan.

Control by design in het verkeer.

ENTERPRISE CONTROL BY DESIGN

De alignment van veranderingen

Dit artikel schetst de borging van enterprise control by design. Sleutelbegrip is alignment, dit alignment wordt in opzet bereikt door strategisch plan, business model, enterprise capability architectuur en zogenoemde business capability stories te annoteren met op elkaar afgestemde en telkens meer in detail uitgewerkte control requirements. Kernbegrippen in dit artikel zijn strategic destination statements, Business Model Canvas, enterprise capability maps, touchpoints en business capability stories. Het artikel is niet bedoelt als voorschrift, maar deelt een zienswijze die de auteur op verschillende projecten met voordeel heeft ingezet.

We mogen constateren dat de digitale technologieën steeds meer impact hebben op onze maatschappij. Innovaties zoals Distributed Ledger Technologies, autonome gedistribueerde organisaties, Industry 4.0 en Cyber Physical Systems maken dat er genoeg redenen zijn om enterprise control requirements steeds meer a-priori en dus by design in de levenscyclus van een concern te willen integreren. Het achteraf herstellen van vooraf vermijdbare tekortkomingen wordt terecht gezien als ongewenst en is in sommige gevallen zeer kostbaar. Tevens geldt dat door het steeds snellere tempo waarin de enterprise omgeving verandert transformationele inertie in de enterprise steeds meer als een significantie kwetsbaarheid gezien wordt. Verandering is continu en enterprise control zal ook tijdens verandertrajecten op een aanvaardbaar niveau gehandhaafd moeten worden. Dit artikel schetst op hoofdlijnen een aanpak om enterprise control by design te realiseren dat verandering omarmt. Zelf ben ik vaak onder de indruk geweest van de wijze waarop in het verkeersnet wordt omgegaan met de requirement om de vervoerscapaciteit van snelwegen te optimaliseren en ook de noodzaak om met voldoende veiligheid verkeersbewegingen mogelijk te maken. Het is een leuke exercitie om control requirements en maatregelen in deze context te herkennen en op een rijtje te zetten. We vermijden open deuren door hier in dit artikel niet verder op in te gaan.

Strategic destination statement

De ambitie om enterprise control by design te realiseren begint volgens dit artikel op het niveau van de enterprise strategie. Alignment met enterprise strategie is een rode draad in dit artikel. Visie, missie, waarden stelsel, omgeving, strategic destination statement en de strategy map worden in [1] als kern bouwstenen van een bedrijfsstrategie beschouwd. Deze kunnen op gestructureerde wijze worden uitgewerkt via de inzet van technieken zoals SWOT, PESTLE, 5 Forces, Business Scorecards, en dergelijke. Aansluitend op deze bekende en ook in [1] gepresenteerde concepten is de Strategic Destination Statement (SDS) voor de doelstellingen van dit artikel het belangrijkste bouwblok. De SDS geeft SMART aan wat de strategische doestelling van een bedrijf is voor een bepaalde tijd. Een voorbeeld van SDS: Door overnames van geschikte partners zal ons bedrijf binnen vijf jaar de grootste koekenbakker van Nederland zijn voor ouderen.

Het business model

De volgende stap in de realisatie van een enterprise strategie is de keuze voor een geschikt businessmodel dat de realisatie van het beoogde strategie optimaal faciliteert. Het middel bij uitstek voor het uitwerken van businessmodellen is het Business Model Canvas [2]. De opzet van een Business Model Canvas wordt in figuur 2 getoond.

Figuur 2 - Opzet Business Model Canvas
Bron: Business Model Generation

Het Business Model Canvas brengt het bedrijfsmodel van een concern in beeld waarmee het SDS te realiseren is. Voor uitweiding over het Business Model Canvas wordt u naar andere bronnen verwezen. Alignment tussen strategische doelstellingen en het businessmodel is een key succes factor voor enterprise control by design. Dit alignment waarborgt dat we met de juiste dingen bezig zijn. Alle bouwblokken van het businessmodel zullen met gepaste control requirements geannoteerd dienen te worden. Bijvoorbeeld, welke toezichthouders bewaken de belangen van klantsegmenten? Of aan welke regelgeving zijn onze waarde proposities onderhevig?

Business capability map

Alignment tussen businessmodel en business architectuur is de volgende vereiste voor enterprise control by design. Een belangrijk bouwblok van business architectuur is de business capability. Een business capability is een logisch samenstel van rollen, processen, technologie, informatie en andere concepten die nodig zijn om waarde te leveren aan de klant.

Ing. Maurice Gittens, CRISC, CGEIT, CISA, CISM. Maurice werkt momenteel als Capability Architect bij de overheid. Hij is bereikbaar via maurice@gittens.nl.

In opzet benut een business capability, building blocks uit het Business Model Canvas (zoals key activities, key resources) om bij te dragen aan value propositions die volgens het Business Model Canvas aan klantsegmenten geleverd wordt. Business capabilities zullen in het algemeen uit sub-capabilities bestaan. Een business capability map benoemd capabilities, die in opzet nodig zijn om bij te dragen aan de realisatie van het businessmodel en in het verlengde daarvan de bedrijfsstrategie. Ook willen we opmerken dat strategische transformaties door veranderende omstandigheden telkens een noodzaak zijn voor een duurzaam bedrijf. In verschillende stadia van strategische transformatie trajecten zullen met name de inrichting van business capabilities zich transformeren om voor de verschillende transitie stadia de benodigde functionaliteit te leveren. Ieder transitiestadium zal een corresponderende transitiearchitectuur hebben die de samenhang tussen business capabilities voor het betreffende stadium in kaart brengt. Business capability planning wordt in gezet om het transitietraject naar de beoogde eindsituatie in kaart te brengen. Voor enterprise control by design geldt als invariant dat alle stadia van het transitie traject capability control requirements per capability geborgd dienen te zijn. En passant vermelden we dat de business capability map en de corresponderende business capabilities misschien wel ideale kapstokken voor scenario modelling, business impact analyses, risk assessments en dergelijke aan te koppelen.
In de volgende stap gaan we in op het systematisch afleiden van control requirements voor de capability constituenten zoals processen, mensen, technologie en informatie.

Touchpoints en user-stories

De volgende stap van de realisatie van enterprise control by design willen we twee concepten uit het domein van integrated market communication en Agile/Scrum benutten. Deze concepten zijn respectievelijk touchpoints en user stories. Touchpoints zijn in oorspronkelijke context de interactiepunten van een klant met een bedrijf. Die punten waar de klant en het bedrijf elkaar 'raken' als het ware. Voorbeelden zijn web portals, mobile apps en retail outlets en dergelijke. Het ligt voor de hand dat er een correlatie te leggen is tussen touchpoint architecture en user experience modelling. Voor meer informatie over touchpoints wordt de lezer via een search-engine naar ander bronnen verwezen. We benutten het touchpoint concept door te herkennen dat ook business capabilities touchpoints hebben. Deze touchpoints kunnen natuurlijk via technische media en menselijke interactie gerealiseerd worden.
Op analoge wijze stellen we dat building blocks van het Business Model Canvas op zijn minst in abstracte zin ook touchpoints hebben. User stories kunnen heb ik in de context van Agile/Scrum leren kennen. Bij het ontwerpen van security controls blijken user stories uiterst bruikbare bouwstenen. Voor onze doelstelling zien we Agile/Scrum user stories als eenheden van functionaliteit.
Voor de doelstelling van dit artikel heeft een user-story de vorm:
As a <role> I want to <action> to achieve <benefit>

Een user story is een prima aanknopingspunt voor control requirements die met het oog op enterprise control by design gewenst zijn. User story control requirements zullen in het algemeen verschillend van aard zijn. Denk hierbij bijvoorbeeld aan: business performance requirements, information security requirements, data quality requirements. Voor het perspectief van informatiebeveiliging is de link tussen user-stories en abuse-stories gauw gelegd. In dit artikel gaan we hier niet verder op in.

Business capability story map

Analoog aan user stories in de context van Agile/Scrum wil ik in dit artikel het concept van een business capability story introduceren. Het idee is om het principe achter Agile/Scrum user stories toe te passen op business capabilities. Een voorbeeld zinstructuur voor een business story is:
Stakeholder leverages the Capability Touchpoint of the Capability to deliver Benefit to Recipient under Terms.
Deze zinsstructuur kan zoals bovenstaand in tabelvorm worden weergegeven. De business capability story uit het bovenstaande voorbeeld lezen we als:

Stakeholder	Touchpoint	Capability	Benefit	Recipient	Terms
Hiring manager	request resource	Internal Staffing	Project SME	Project x	standard-temp-hr
Sales Department	DR Advisory	BCM	DR Plan	Sales Department	standard-bcm
Retail products Dept	SIEM Services	SOC	SIEM Services	Consumers Portal	standard-24-7

De placeholders of variabelen van de business capability story noemen we de constituenten van de business capability story. Op de constituenten van business capability stories kunnen we afzonderlijk en in combinatie control requirements plaatsen. Denk hierbij aan:

- autorisatie requirements voor capability touchpoints die bepalen welke stakeholders een capability touchpoint mogen benutten
- legal, compliance en data quality control requirements op de contractvoorwaarden van de capability touchpoint
- business requirements op de benefits recipient van de business story

De bovenstaande beschrijving van business capability stories zijn voor de doelstellingen van dit artikel voldoende. Toekomstige artikelen zullen mogelijk over dit onderwerp verder uitweiden. In dit artikel wordt gesteld dat enterprise control by design gaat over alignment. De alignment van control requirements is geschetst vanaf strategische control requirements, via businessmodel control requirements en control requirements voor capabilities van de business capability map. Als laatste is geschetst hoe control requirements aan business capability stories te koppelen zijn. De laatste stap zijn control requirements op het operationele niveau van processen, technologie, mensen en dergelijke. In dit artikel gaan we hier niet verder op in. Wel gaan we nog in op een belangrijk aspect van enterprise control by design dat we nog niet hebben besproken. Het betreft de alignment van veranderingen in de organisatie.

The enterprise gait: moving to the beat

De meidengroep Sizzle Frizzle had in de jaren tachtig een leuk hitje met als titel 'Alles heeft een ritme'. De titel van dit liedje sluit goed aan op mijn opvattingen over verandering ook in de context van een bedrijf. Het Engelse woord gait wordt vertaald met begrippen als het looppatroon, de gang of de tred. Ik stel dat een bedrijf ook een tred heeft. Om in control te zijn van veranderingen is het wat mij betreft nodig om alignment in tijd tussen veranderingen op verschillende niveaus in een bedrijf te realiseren. Ik zie het graag als een dans. Als tijdens een wals de dame en heer qua tempo niet op elkaar afgestemd zijn is het resultaat doorgaans ongewenst. Een fijne dans ontstaat juist wanneer de positionering van lichaamsdelen in de tijd en ruimte op elkaar zijn afgestemd. Er zijn wat mij betreft veel parallellen te trekken tussen dit voorbeeld en veranderingen in de context van een enterprise. Onderstaande tabel geeft een schets van een mogelijk cadans van veranderingen op verschillende niveaus in een bedrijf.

We stellen dat t = 0 de huidige periode is. Natuurlijk zal dan t+1 met een periode in de toekomst corresponderen en t+2 twee perioden in de toekomst. P:t+x correspondeert met de capabilities die in periode x in productie zijn. Wordt op t=0 aan een strategische verandering gewerkt dan zal volgens het bovenstaande tabel pas in periode t+5

Strategie	S:t+5	S:t+6	S:t+7	S:t+8	S:t+9	S:t+10
Business Model	B:t+4	B:t+5	B:t+6	B:t+7	B:t+8	B:t+9
Business Capability Architectuur	A:t+3	A:t+4	B:t+5	A:t+6	A:t+7	A:t+8
Capability Solution Design	O:t+2	O:t+3	O:t+4	O:t+5	O:t+6	O:t+7
Capability Increment Realisatie	V:t+1	V:t+2	V:t+3	V:t+4	V:t+5	V:t+6
Productie	P:t+0	P:t+1	P:t+2	P:t+3	P:t+4	P:t+5

de betreffende capability increment in productie landen. Een enterprise die in control is zal in staat zijn om met een hoge mate van voorspelbaarheid capability increments in productie af te leveren met alignment in de tijd en aan de enterprise strategie. Alignment van control requirements tussen de verschillende niveaus is sleutel tot succes. Het maakt mogelijk dat op ieder niveau, van conceptie naar realisatie, aan de juiste dingen gewerkt wordt terwijl het zich niet uit laat over hoe de capability increments gerealiseerd dienen te worden. Alignment reduces waste! De invloeden van Agile, Lean, Operational Excellence en dergelijke mag op de uiteenzetting in dit artikel duidelijk zijn.

The tragedy of the commons

Enterprise control by design zie ik als een noodzaak voor bedrijven die met vertrouwen de toekomst tegemoet willen treden. Voor het benutten van opportunities en het beperken van risico's is een beperkte hoeveelheid geld beschikbaar. Opportunity control en risk control als aparte disciplines zien, leidt er ertoe dat synergievoordelen niet optimaal benut worden. Verzuiling tussen risk management en opportunity management leidt wat mij betreft tot een verschijnsel dat in de economie bekend staat als 'the tragedy of the commons'. We halen er niet uit wat erin zit. Laten we de volgende vraag beschouwen:

Welke business opportunities worden door informatiebeveiliging mogelijk gemaakt?

De beloning voor een specifiek antwoord op deze vraag zal vaak genoeg een realisatiebudget zijn. Het specifiek kunnen beantwoorden van vragen als de bovenstaande is een voorbeeld van wat enterprise control by design mogelijk maakt. In dit artikel is een schets gegeven van een aanpak voor enterprise control by design. De rode draad is alignment. Alignment van control requirements van conceptie tot realisatie en de alignment van veranderingen in de tijd over verschillende niveaus. Misschien heeft alles inderdaad een ritme.

Referenties

[1] Balanced Scorecards & Operational Dashboards, Ron Person, Wiley Publishing, 2009.

[2] Business Model Generation, A. Osterwalder, Yves Pigneur, Alan Smith, and 470 practitioners from 45 countries, (2010).

Achtergrond

Economics of Organizations and Markets, S. Onderstal (2014).

Artikel in Informatiebeveiliging: "Tethering Enterprise Interests", gepubliceerd in IB1 2014.

Artikel in Informatiebeveiliging: "Accual Based Risk Management" gepubliceerd in IB2 2012.

Artikel in Informatiebeveiliging: "Threat Scenario Modelling I" gepubliceerd in IB6 2015.

Artikel in Informatiebeveiliging: "Treating Risk Prospectively in IB1 2015.

Artikel in Informatiebeveiliging: "Requirements dependency analysis" in IB3 2015.

RISICOANALYSE: PRIVACY VERSUS INFORMATIEBEVEILIGING

Bijna dagelijks worden we in de media geconfronteerd met een situatie waarin gevoelige gegevens zijn gelekt of gehackt. Het belang van informatiebeveiliging en privacy lijkt hierdoor steeds meer tot organisaties door te dringen. Zij maken zich zorgen over welke gegevens zij eigenlijk vastleggen van personen en hoe goed ze die gegevens hebben beveiligd.

Naast een beroep op de 'maatschappelijke' verantwoordelijkheid worden organisaties ook op andere manieren gestimuleerd om serieus met hun informatiebeveiliging en privacy om te gaan. Zo kunnen organisaties die maatregelen willen nemen om de informatiebeveiliging beter te borgen de ISO27001 standaard voor informatiebeveiliging gebruiken. Deze geeft aan op welke wijze organisaties hun informatiebeveiligingsproces moeten inrichten en uitvoeren. Organisaties kunnen zich tegen deze standaard laten certificeren en tonen daarmee aan klanten en toezichthouders dat zij de informatiebeveiliging onder controle hebben.

Voor privacy heeft de wetgever het belang van de burger vertaald in sterk aangescherpte (Europese) wetgeving. Organisaties die persoonsgegevens vastleggen dienen maatregelen te nemen om de privacy van persoonsgegevens te beschermen op straffe van hoge boetes. Daar waar bij informatiebeveiliging er vooral een business case moet zijn voor het nemen van beheersmaatregelen, is voor beheersmaatregelen ten aanzien van privacy ook de public case aan de orde.

Vraagstelling

Organisaties die hun informatiebeveiliging willen organiseren volgens de ISO 27001 standaard worden geacht risicoanalyses uit te voeren op hun kritische processen. In het kader van de nieuwe privacywetgeving worden diezelfde organisaties ook verplicht om voor hun persoonsregistraties de privacy risico's af te wegen in een Privacy Impact Assessment. Beide domeinen, informatiebeveiliging en privacy, liggen dicht tegen elkaar aan. De vraag die in dit artikel centraal staat is daarom:

In hoeverre is het mogelijk om de risicoafweging op de aspecten informatiebeveiliging en privacy te combineren?

Informatiebeveiligingsrisicoanalyse

Een belangrijke element van informatiebeveiliging is de informatiebeveiligingsrisicoanalyse (IBRA). Organisaties dienen in een Business Impact Analyse vast te stellen wat de eisen zijn die zij stellen aan de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie. Vervolgens moeten zij vaststellen welke risico's deze belangen bedreigen en dienen zij een risicobehandelplan op te stellen.

Privacy Impact Assessment

De aangescherpte privacywetgeving vereist dat organisaties die persoonsgegevens willen gaan verwerken een Privacy Impact Assessment (PIA) uitvoeren. In deze PIA wordt veelal op basis van een uitvoerige vragenlijst vastgesteld welke risico's een organisatie loopt bij de verwerking van persoonsgegevens. De privacyprincipes die een rol spelen zijn onder andere: doelbinding, rechtmatige grondslag, dataminimalisatie, profilering, datagebruik, informeren van betrokkenen, rechten van betrokkenen, bewaartermijnen en beveiliging van de gegevens.

De PIA is er onder andere op gericht om, met de WBP en haar boetebepalingen op de achtergrond, op een juiste wijze het belang van de betrokkene (de public case) in de risicoafweging mee te nemen.

De combinatie van PIA en IBRA in de praktijk

In mijn werk heb ik voor de Hanzehogeschool Groningen een PIA gecombineerd met een IBRA. De scope van het onderzoek betrof het CRM-systeem dat Hanzehogeschool gebruikt ter ondersteuning van de instroom van (aspirant) studenten,

regelen van stage-opdrachten en uitstroom van studenten (alumni). Het traject heeft niet alleen succesvol de informatiebeveiligingsrisico's en de privacy-risico's inzichtelijk gemaakt, het heeft ook veel interessante inzichten opgeleverd.

Gemeenschappelijke aanloop

Om de risico's te kunnen beoordelen is informatie nodig. Voor beide analyses IBRA en PIA gaat het daarbij om grotendeels de zelfde informatie:

- **Gegevensinformatie:** Welke persoonsgegevens worden vastgelegd?
- **Procesinformatie:** Welke bedrijfsprocessen worden uitgevoerd met de persoonsgegevens? Met welk doel worden deze processen uitgevoerd?
- **Informatiearchitectuur:** In welke informatiesystemen worden gegevens vastgelegd en tussen welke organisaties en applicaties worden persoonsgegevens uitgewisseld?

Uit het oogpunt van efficiëntie is het slim om deze informatie één keer op te vragen en voor beide analyses te gebruiken.

Verschil in aanpak

ISO27001 schrijft organisaties niet voor hoe zij een risicoafweging doen, net zomin als de Wbp voorschrijft op welke wijze een Privacy Impact Assessment moet worden uitgevoerd. In de praktijk is er natuurlijk al wel invulling gegeven aan beide risicotrajecten. Security officers hebben op basis van best practices invulling gegeven aan de IBRA, waarbij de rode draad is: Business Impact Analyse • Kwetsbaarheden • Risico's • Beheersmaatregelen.

VOORBEELD IBRA

Scope:	Customer Relation Managementsysteem (CRM).
BIA:	De classificatie op Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) wordt vastgesteld op respectievelijk Midden, Midden en Hoog.
Kwetsbaarheid:	Gebruiker kan eenvoudig gegevens uit het systeem halen.
Risico:	Ongecontroleerd gegevens worden verstrekt (of gelekt).
Maatregel:	Beperk de mogelijkheid tot exporteren van gegevens uit CRM.

VOORBEELD PIA

Scope:	Customer Relationship Managementsysteem (CRM).
PIA-principe:	Doelbinding: Worden de gegevens voor het juiste doel gebruikt (en niet ook voor iets anders)?
Risico:	Medewerkers gebruiken de gegevens voor andere doeleinden.
Maatregel:	Formuleer doeleinden voor de verwerking van persoonsgegevens voor CRM en informeer de betrokken medewerkers hierover.

NOREA heeft een PIA-instrument ontwikkeld om invulling te geven aan de wettelijke vereisten: een vragenlijst waarin acht privacyprincipes worden getoetst en waarbij per principe vooral de juridische risico's worden benoemd en gewogen.

Organisatiebelang versus belang van betrokkene

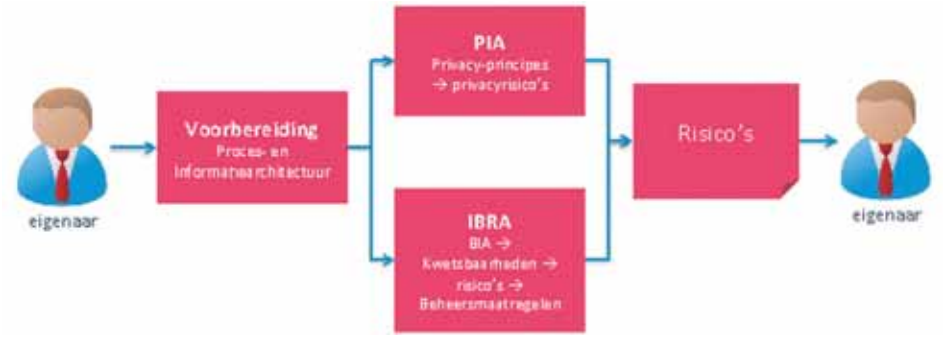
Los van deze praktische verschillen in aanpak is er ook een belangrijk verschil in benadering. De IBRA neemt de Business Impact als uitgangspunt: het belang van de organisatie. De PIA neemt de Public Impact als uitgangspunt: het belang van de betrokkene. Het liefst hebben we natuurlijk dat een organisatie het belang van de betrokkenen (vaak haar klanten) als haar eigen belang ziet. Toch was er een wetswijziging voor nodig om organisaties te dwingen het belang van de betrokkene serieus te overwegen.

Wie bepaalt de risico's?

Het onderscheid in benadering is ingegeven door de constatering dat organisaties over het algemeen niet in staat of bereid zijn om de privacyrisico's van de betrokkenen in te schatten. Organisaties hebben daar hulp bij nodig van een privacyspecialist. De ervaring met de case was dat de (externe) privacyspecialist de rol van betrokkene invult, de privacyrisico's benoemt en ook de ernst van deze risico's aangeeft.

Bij de IBRA is in de case ook gebruik gemaakt van een extern adviseur, maar die vervulde veel meer de rol van facilitator. De medewerkers van de organisatie stellen zelf de risico's vast en verklaren de beheersmaatregelen van toepassing.

Peter Kampman is adviseur bij Insite Security. Peter is bereikbaar via pkampman@insitesecurity.nl.



Figuur 1 - Aanpak voor gecombineerde PIA-IBRA

Beheersmaatregelen
Het gebruik van het PIA-instrument borgt dat organisaties nadenken over de privacy van de betrokkenen waarvan zij gegevens opslaan en het leidt tot de vaststelling van de risico's die een organisatie loopt. De beheersmaatregelen om die risico's te mitigeren liggen vaak wel voor de hand, maar de PIA dicteert niet welke beheersmaatregelen moeten worden genomen.

De IBRA op basis van ISO27001 is wat strakker in het benoemen van beheersmaatregelen. Op basis van de BIA en de kwetsbaarheden dient de organisatie beheersmaatregelen 'van toepassing te verklaren'. De organisatie kan daarbij putten uit een lange maar eindige lijst van redelijk concrete beheersmaatregelen uit de bijlage van de ISO27001 standaard. Met enige begeleiding van een informatiebeveiligingsconsultant wordt de organisatie naar de beheersmaatregelen geleid. Daarmee is strak gedicteerd welke maatregelen van toepassing zijn. De afweging om de beheersmaatregelen ook werkelijk te implementeren is aan het management.

PIA en IBRA leiden tot één risicotabel
Hoewel de weg ernaartoe dus verschilt is het eindresultaat van zowel PIA als IBRA een overzicht van risico's. Ervan uitgaande dat de scope een afgebakende persoonsregistratie of informatiesysteem of bedrijfsproces is, waarbij er één eigenaar is toegewezen, is het voor deze eigenaar zinnig om de privacy- en IB-risico's in één overzicht te verzamelen.
Als een organisatie een Plan-Do-Check-Act cyclus heeft ingericht voor informatiebeveiliging is het ook verstandig om de privacyrisico's daarin mee te nemen.

PIA is een projectinstrument, IBRA een beheerinstrument
In opzet is de PIA een instrument dat organisaties kunnen gebruiken als zij een project starten voor een nieuwe verwerking van persoonsgegevens of voor een belangrijke wijzigingen op een bestaande verwerking. In ieder geval is dat wat de nieuwe privacywetgeving voorschrijft: Als een organisatie het voornemen heeft om een persoonsregistratie aan te leggen moet zij een PIA uitvoeren. Privacyprincipes als dataminimalisatie en doelbinding leiden mogelijk tot maatregelen die in dat stadium nog effectief kunnen worden afgewogen en geïmplementeerd.

Veel organisaties zullen eerst een inhaalslag moeten maken en zullen PIA's uitvoeren op bestaande verwerkingen van persoonsgegevens. Een PIA kan in dat geval leiden tot beheersmaatregelen die het karakter hebben van een achteraf reparatie. De ervaring in andere branches leert dat reparatie achteraf erg kostbaar kan zijn.

Een IBRA is natuurlijk het meest effectief als deze bij de start van de implementatie wordt uitgevoerd, maar de benadering van een IBRA is meer dat de risico's worden vastgesteld die volgen uit de mate waarin bepaalde beheersmaatregelen zijn geïmplementeerd.

Bewustwording
De ervaring met de case vertelt ons dat zowel bij de IBRA als bij de PIA bewustwording erg belangrijk is. Met name als er wordt gekozen voor een workshopvorm zien we dat de deelnemers zich bewust worden van wat informatiebeveiliging en privacy eigenlijk inhoudt, dat zij de risico's snappen en dat zij daarom ook snappen waarom er beheersmaatregelen nodig zijn.

Gebleken is wel dat het borgen van de privacy van personen en het beveiligen van informatie twee wezenlijk verschillende onderwerpen zijn en dat het goed is om de dialoog over beide onderwerpen gescheiden te houden.

Conclusie
Op basis van bovenstaande ervaringen is de conclusie dat de IBRA en de PIA als instrument dermate van elkaar afwijken dat

het niet verstandig is om ze volledig te combineren. Met name het verschil in benadering (business case versus public case) maakt dat we ze niet over één kam moeten scheren.

Aan de voorkant en aan de achterkant van de analyses is echter wel efficiëntie te behalen. Aan de voorkant door bijvoorbeeld eerst de IBRA te doen, waarin informatie over het proces- en de informatiearchitectuur wordt uitgevraagd en vastgelegd. De PIA kan gebruik maken van de deze informatie en hoeft deze dus niet opnieuw uit te vragen.
Aan de achterkant is het verstandig om de risico's uit beide analyses te verzamelen in één risicotabel en aan te bieden aan de systeem- of proceseigenaar en op te nemen in één planning- en control cyclus.

Het is goed om het vaststellen en wegen van de risico's en het bepalen van de beheersmaatregelen voor informatiebeveiliging en privacy in separate workshops of gesprekken plaats te laten vinden.

In de privacyworkshop is aan te bevelen om iemand aan te wijzen die het publieke belang vertegenwoordigt.

PIA-principes:

1. **Dataminimalisatie.** Limitering van het verzamelen van gegevens. Het verminderen van de hoeveelheid gegevens, door de gegevens niet op te slaan of niet te bewaren.
2. **Gegevenskwaliteit.** Introduceren van (geautomatiseerde) controles op gegevens.
3. **Doelbinding.** De doelen voor het verzamelen en de verenigbaarheid van verdere verwerking nader specificeren en hierover communiceren.
4. **Limitering van gebruik van gegevens.** Het beperken van de mogelijkheid om grote hoeveelheden gegevens in een keer binnen en buiten de organisatie te verspreiden door gefragmenteerde opslag in plaats van concentreren van alle gegevens in één database.
5. **Beveiliging van gegevens.** Het toepassen van encryptie en logische toegangsbeveiliging.
6. **Transparantie.** Het opstellen van een privacybeleid, gedragscode of het laten certificeren van de verwerking.
7. **Rechten van betrokkenen.** Betrokkenen zeggenschap geven over zijn gegevens. Hieronder valt ook het recht om vergeten te worden.
8. **Verantwoordelijkheid en Verantwoording.** Invoeren van periodieke externe controle.

Van links naar rechts: Rinke Zonneveld, Eveline Steenbergen, Ingrid van Engelshoven en Richard Franken.

HSD OPENT INTERNATIONAL CENTRE IN WTC DEN HAAG

Hoofddoel is internationale samenwerking

De bovenste etage van toren C van het World Trade Center in Den Haag was op 26 oktober het toneel van een officiële openingsceremonie. Op deze etage is de eerste uitbreiding van The Hague Security Delta (HSD) gehuisvest onder de naam HSD Campus International Centre. Naast de reeds langer in gebruik zijnde etages in het ICTU gebouw is deze nieuwe ruimte vooral gericht op internationale samenwerking. Daarvoor is het WTC Den Haag een logische keuze met z'n vijf torens met totaal 60.000 m^2 vloeroppervlak en een breed scala aan ondersteunende faciliteiten.

Nu is HSD al het grootste security cluster in Europa met meer dan 230 partners, maar samenwerking met de rest van de wereld is een van de speerpunten.

In zijn openingsrede gaf Richard Franken (Algemeen Directeur HSD) aan dat via deze nieuwe ruimte beter en sneller internationale contacten gelegd kunnen worden met als bedoeling HSD verder buiten Nederland uit te breiden. Nu is HSD al het grootste security cluster in Europa met meer dan 230 partners, maar samenwerking met de rest van de wereld is een van de speerpunten.

Eveline Steenbergen (General Manager WTC Den Haag) memoreerde de recente verbouwing van het WTC, waardoor dit nog beter in staat is als internationaal handelshuis en ontmoetingsplek te fungeren. WTC zorgt voor de ondersteunende faciliteiten, waardoor huurders (zowel gerenommeerde bedrijven en organisaties als start-ups) zich volledig kunnen concentreren op het aangaan en uitbouwen van samenwerkingsverbanden.

Rinke Zonneveld (Directeur Innovation Quarter, de regionale ontwikkelingsmaatschappij voor Zuid-Holland) vertelde al zo'n 40 start-ups te hebben geholpen met innoveren, investeren en/of vestigen. Hij verwacht veel van de samenwerking met HSD, en gaf aan dat door de opening van deze etage in het WTC de aantrekkelijkheid voor het buitenland nog verder vergroot zal worden.

De officiële opening werd verricht door Ingrid van Engelshoven (wethouder Kenniseconomie, Internationaal, Jeugd en Onderwijs, en eerste locoburgemeester). Den Haag is de stad van Vrede en Veiligheid, en heeft al verschillende instanties op dat gebied binnen de gemeentegrenzen (denk aan het Vredespaleis, het Internationaal Gerechtshof, het Internationaal Strafhof, het Joegoslavië Tribunaal, de Organisatie voor het Verbod op Chemische Wapens, maar ook bijvoorbeeld Europol). Middels de HSD wil Den Haag de toegang tot Europa zijn voor internationale bedrijven en organisaties op het gebied van cybersecurity. Daarbij wordt vaak de term 'triple helix' gebruikt, hiermee wordt de samenwerking tussen overheid, bedrijfsleven en kennisinstituten bedoeld.

Ter illustratie van het soort bedrijven en organisaties dat op deze nieuwe etage van HSD samenwerkt, liet Jochem Streekstra (Campus Manager HSD) een aantal van hen de 'zeepkist' beklimmen om in twee minuten uit te leggen waarom zij partner zijn in HSD. Ook Women in Cybersecurity (WiCS) komt regelmatig bij elkaar op de HSD Campus, en illustreerde dit met een leuke film.

Tot slot was er (recht doend aan de missie van HSD) ruimschoots gelegenheid om met een hapje en een drankje met elkaar te netwerken, nieuwe mensen te leren kennen, en bij te praten met oude kennissen.

Links

The Hague Security Delta (HSD):
https://www.thehaguesecuritydelta.com/
HSD Campus:
https://www.thehaguesecuritydelta.com/about/hsd-campus
HSD Campus International Centre:
http://www.wtcthehague.com/nl/hsd-campus-international-centre
WTC Den Haag:
http://www.wtcthehague.com/nl
Innovation Quarter:
http://www.innovationquarter.nl/
Den Haag, Internationale stad van vrede en veiligheid:
http://www.denhaagvrederecht.nl/vrede-en-recht.htm
Women in Cybersecurity:
http://wics.online

Lex Dunn is adviseur op het gebied van informatiebeveiliging en compliance. Hij is te bereiken via lex@selexity.nl.

CYBERSECURITYBEELD NEDERLAND 2016

Jaarlijks brengt het Nationaal Cyber Security Centrum (NCSC), samen met meer dan 80 partnerorganisaties de stand van zaken op het gebied van cybersecurity in Nederland in kaart. Deze samenwerking resulteert in het Cybersecuritybeeld Nederland (CSBN). Hierin worden de belangrijkste en meest opvallende ontwikkelingen besproken in termen van manifestaties, belangen, dreigingen en weerbaarheid. Deze ontwikkelingen van de dreiging wordt ingeschaald en gecategoriseerd op basis van malafide actor en doelwit en wordt gepresenteerd met een dreigingsmatrix.

Een selectie uit de dreigingsmatrix van het CSBN 2016 is weergegeven in tabel 1. Deze matrix kan beleidsmakers (bijvoorbeeld CISO's) helpen bij het uitvoeren van risicoanalyses en, vervolgens, met het prioriteren van maatregelen en overige securityinvesteringen.

	Doelwitten		
Bron van Dreiging	Overheden	Private organisaties	Burgers
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie
	Manipulatie van informatie	Manipulatie van informatie	Manipulatie van informatie
	Verstoring van ICT	Verstoring van ICT	Verstoring van ICT
	Overname van ICT	Overname van ICT	Overname van ICT
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten	

Tabel 1 – Selectie uit de dreigingsmatrix van het CSBN2016

Om te komen tot een cybersecuritybeeld wordt samengewerkt met organisaties ondersteunend aan vitale processen, de academische wereld, belangengroepen en private cybersecuritybedrijven. De informatie van deze partijen wordt samengebracht, voornamelijk per sector. Er worden diverse expertsessies georganiseerd rond bepaalde sectoren en thema's. Uit deze sessies blijken sommige organisaties veel meer last van specifieke problemen te hebben dan andere organisaties. Uiteindelijk wordt er gewerkt naar één beeld dat de staat van cybersecurity en ontwikkelingen op dat gebied in Nederland over het afgelopen jaar weergeeft. Een selectie uit de ontwikkelingen die bijzondere aandacht verdienen, wordt hieronder samengevat.

Beroepscriminelen voeren langdurige, hoogwaardige en geavanceerde campagnes uit.
Campagnes van beroepscriminelen worden steeds geavanceerder. In het verleden waren de digitale aanvallen en bijbehorende campagnes van criminelen vaak van korte duur en gericht op snel geld verdienen door veel partijen te benadelen. Criminelen hebben het afgelopen jaar een aantal campagnes uitgevoerd waarvoor hoge investeringen zijn gedaan en waaruit een hoge organisatiegraad blijkt. Deze criminele organisaties zijn professioneel georganiseerd en zijn gericht op winst op langere termijn. De focus ligt bij deze criminelen vaker op een klein aantal vermogende doelwitten dan op een breed publiek. Bovendien worden technieken als spearphishing door criminelen steeds verfijnder ingezet en daarmee geloofwaardiger voor slachtoffers. Spearphishing is zo steeds lastiger te bestrijden met beveiligingsbewustzijn: wanneer phishing dusdanig geraffineerd is, kunnen maatregelen om beveiligingsbewustzijn te verhogen hier niet altijd bescherming tegen bieden. Langdurige campagnes met grote investeringen en geavanceerde spearphishing waren in het verleden het terrein van statelijke actoren.

Ransomware is gemeengoed en is nog geavanceerder geworden.
Het gebruik van ransomware door criminelen is het afgelopen jaar gemeengoed geworden. Besmettingen zijn aan de orde van de dag en raken de gehele samenleving. Vorig jaar werd ransomware in het CSBN al genoemd als het cybercriminele businessmodel bij uitstek. Die waargenomen trend heeft zich het afgelopen jaar voortgezet: organisaties die onderdeel uitmaken van vitale processen en binnen de overheid geven aan het afgelopen jaar te maken gehad hebben met meer infecties met ransomware dan in eerdere jaren. Waar in het verleden dezelfde prijs betaald moest worden per besmetting, wordt nu soms een prijs bepaald aan de hand van het type getroffen organisatie. Criminelen verhogen hun losgeldeis gebaseerd op de verwachte financiële draagkracht van het slachtoffer. Bovendien is de malware zelf verfijnder: naast bestanden op de lokale schijf worden tegenwoordig ook databases, back-ups en bestanden op netwerkschijven versleuteld. Voor organisaties betekent dit dat de impact van een besmetting groter kan zijn en dat herstel lastiger wordt.

Advertentienetwerken zijn nog niet in staat gebleken om malvertising het hoofd te bieden.
Het verspreiden van malware via advertenties op grote websites is een probleem. Ook dit jaar kwam het regelmatig voor dat bezoekers van reguliere websites geconfronteerd werden met malware in de getoonde advertenties. Door het brede bereik van deze advertentienetwerken vormen ze een voor criminelen interessant kanaal om malware te verspreiden. Gebruikers met niet bijgewerkte software zijn daarbij vooral het doelwit. Dit komt niet alleen voor in obscure hoeken van het internet, maar ook op zeer populaire Nederlandse websites. De werkwijze bij deze aanvallen suggereert dat de daders meestal beroepscriminelen zijn. De advertentienetwerken zijn nog niet in staat gebleken dit probleem het hoofd te bieden. Het brede bereik van advertentienetwerken zorgt, samen met het grote aantal systemen waarop de laatste updates ontbreken, voor een groot aanvalsoppervlak. Beheerders van deze websites en de advertentienetwerken zelf hebben geen volledige controle over de advertenties. Dit zorgt ervoor dat malware zich kan verspreiden. Het volledig blokkeren van advertenties in de browser raakt aan het verdienmodel van website-eigenaren. Om gebruikers te beschermen tegen malvertising zonder alle advertenties te blokkeren zijn fundamentele wijzigingen nodig in de manier waarop deze netwerken werken.

Op 5 november is het CSBN-2016 met een beleidsreactie naar de Tweede Kamer verzonden. De volledige documenten vindt u hier: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html.

Het Nationaal Cyber Security Centrum (NCSC) draagt bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein. De primaire doelgroep van het NCSC is de rijksoverheid en de vitale infrastructuur. Meer informatie vindt u op: https://www.ncsc.nl.

VERSLAG CISO 13

ANDERS OMGAAN MET RISICOMANAGEMENT

Er verscheen een oproep op LinkedIn. Een citaat: "Er wordt veel van overheidsorganisaties gevraagd. Om hun maatschappelijke taak te vervullen, transparant te zijn én in control, terwijl de omgeving steeds sneller en onvoorspelbaarder verandert en de maatschappelijke en politieke tolerantie voor fouten en tekortkomingen laag is". De oproep kwam van Marlies Ypma die voor de ADR actief is bij het ondersteunen van risicomanagement. Zij was benieuwd naar ervaringen van anderen.

Drs. Marlies Ypma is Auditmanager Verandermanagement en Organisatiegedrag bij de Auditdienst Rijk (ADR). Ze helpt (top)managers gedragspatronen die het bereiken van organisatiedoelen in de weg staan te begrijpen en te beïnvloeden. Tijdens deze CISO-bijeenkomst was zij onze inleidster. En al direct begon het veranderen, de opstelling werd aangepast waardoor een minder formeel en statisch geheel ontstond.

De vraag die de (toen) nieuwe leider van ADR aan Marlies stelde, luidde: "Hoe risicomanagement bij de overheid tot leven te wekken?". In plaats van de gebruikelijke lijstjes met risico's, samengesteld volgens geijkte methodieken, wilde hij een goed gesprek over risico's in de organisatie. Geen administratieve handeling maar een manier van risicomanagement die aansluit op de dagelijkse werkelijkheid van betrokkenen.

Het is duidelijk dat risicomanagement 'moet' bij de overheid. Maar iedere organisatie richt dat weer op een eigen manier in. De diensten die ADR hierbij aanbiedt, zijn gebaseerd op 'het goede gesprek'. Daarvoor is samenwerking nodig en vertrouwen. De sessies zijn daarom gericht op het verkrijgen van vertrouwen, een open sfeer waarin onderling contact gedijt. Het menselijke gedrag staat centraal en verbeeldingskracht wordt naast de dagelijkse praktijk gezet. Hierbij blijkt dat ook onderlinge nieuwsgierigheid van invloed is. Hoe kijken anderen naar risico's? Hoe reageren anderen op reacties van deelnemers? Doel van de sessies die ADR aanbiedt, is duidelijk maken dat het gaat om de wil om risico's te beheersen, dus weg van het moeten. Daarbij draait het om de eigen rol van de deelnemers in hun werk, hun opvattingen vanuit hun taak en de werksfeer.

ADR als auditdienst heeft de (controlerende) naam tegen als het gaat om het betrekken van mensen in een goed gesprek. Daarom maakt Marlies gebruik van 'ambassadeurs' die als onderdeel van de organisatie sneller vertrouwen krijgen. Menselijk gedrag is van belang omdat dit een onvoorspelbaar fenomeen is. Voorbeelden van gedrag van 'bekende personen' laten zien dat gewoontes, gemak, overschatting en

Menselijk gedrag is van belang omdat dit een onvoorspelbaar fenomeen is.

onderschatting, de directe omgeving en andere persoonlijke factoren het gedrag bepalen, ook als het bekend is dat dit gedrag niet verantwoord is.

Discussie

In de praktijk bestaan er risicomijders en risiconemers. Hoe kan je daarmee omgaan in een per definitie risicomijdende organisatie? Marlies gebruikt in haar sessies vaak hulpmiddelen waarmee zij bijvoorbeeld de persoonlijke risk appetite laat bepalen. Daarmee is het mogelijk te praten over een persoonlijk gevoel voor risico en wat de groep daarvan vindt.

Een ander thema is het verschil in beoordeling van een risico op verschillende niveaus in de organisatie. De kern hiervan is dat men op een hoger niveau gerust is "want wij hebben goede mensen aan het werk", terwijl die mensen dicht op het vuur zittend de kansen beter kunnen inschatten. Die zien wel de zwakke plekken, maar overzien de gevolgen minder. Daarvoor moet je dan weer bij de top zijn.

Vanuit de psychologie is bekend dat mensen slecht met risico's kunnen omgaan. De subjectieve, emotionele benadering maakt dat gesprekken met anderen daarover noodzakelijk zijn. In de discussie werd opgemerkt dat er een natuurlijke tegenstelling is tussen het rationeel benaderen van risico's en het gevoelsmatige van risico's. NIST (National Institure of Standards and Technology) werd genoemd dat laatst melde dat er sprake is van 'security moeheid'.

Een goed gesprek kan leiden tot meer bewustwording en betere keuzes. Beelden en verhalen zijn daarbij een belangrijk hulpmiddel. Wordt de pijn begrepen en gevoeld? Waar ligt men wakker van? Wetgeving kan de impact van een gebeurtenis behoorlijk vergroten en daarmee de top aan het denken zetten. Recente wetgeving tegen datalekken is daarvan een voorbeeld. Het is duidelijk dat 'anders omgaan met risico's', gebaseerd is op een goed gesprek. Dat betekent ook dat er geluisterd moet worden. De aanpak werkt breder dan alleen voor risicomanagement. Marlies faciliteert de goede gesprekken, waarbij de meerwaarde wordt gezocht in de terminologie 'van de ander'. Ja, vaak wordt het lastig gevonden om moeilijke dingen aan de orde te stellen. Daarom had Marlies nog een leestip: Arend Ardon, Doorbreek de cirkel.

Cees Coumou is sinds medio 2003 gepensioneerd als senior EDP Audit manager bij KPMG. Sindsdien is hij onafhankelijk adviseur en docent aan de IT-Audit Master van de Vrije Universiteit, de opleiding Master of IT auditing van de Universiteit van Amsterdam. Zijn werk op het gebied van organisatieadvisering betrof de laatste decennia met name onderwerpen als risicomanagement, continuiteitsmanagement en informatiebeveiliging. Tussen 2005 en 2012 redigeerde hij voor PvIB 8 boeken over trends in IT-beveiliging op basis van gesprekken met vele verschillende professionals.Hij is bereikbaar via cees.coumou@planet.nl.

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.

MELDING DATALEKKEN

Recent zijn er weer wat berichten in het nieuws verschenen over de meldplicht datalekken. De Autoriteit Persoonsgegevens heeft dit jaar tot nu toe 'slechts' 4.000 meldingen binnen gekregen. Dat is een opmerkelijk gering aantal omdat we zo'n 130.000 organisaties hebben die privacygevoelige persoonsgegevens verwerken. Men had minstens 60.000 meldingen verwacht. Een ander bericht verscheen in het FD, waarin een advocatenkantoor (Aldo Verbruggen, ex-officier van justitie) adviseert om een datalek niet altijd te melden maar het in alle stilte te repareren omdat een aangifte en melding 'grote materiële schade' zal opleveren. Dus kan het lonend zijn een boete maar op de koop toe te nemen. Zou dergelijk gedrag nu al spelen gezien het geringe aantal meldingen? Onze redacteuren geven hun mening.


Tom Bakker


Maarten Hartsuijker


Lex Borger

Tom Bakker

Het lage aantal meldingen zal denk ik wel voornamelijk te maken hebben met onwetendheid. Het is niet geheel duidelijk wat en wanneer er nu wel of niet gemeld moet worden. Een IT-afdeling zal bij een incident proberen het probleem zo snel mogelijk op te lossen en er niet bij stilstaan dat er ook een formele melding gedaan moet worden. Wellicht zijn de processen hiervoor ook nog niet ingericht. Een voorbeeld: als een penetratietest wordt uitgevoerd en er worden zwakheden ontdekt die kunnen leiden tot een mogelijk datalek van persoonsgegevens, moet dat dan ook gemeld worden? Als de AP dit soort 'incidenten' ook meetelt bij hun verwachting dan is het verschil tussen de verwachting en de daadwerkelijke meldingen waarschijnlijk wel verklaarbaar. Zo zijn er nog wel een paar voorbeelden te verzinnen.

Er is een onderzoek geweest van Palo Alto (https://executive-people.nl/564748/rapporteren-van-cyberincidenten-bij-senior-management-leidt-tot-spanningen.html) waaruit blijkt dat incidenten met cybersecurity soms aan het senior management worden verzwegen om erg ongemakkelijke gesprekken te vermijden (mogelijk ontslag?). Juist omdat men vindt alle preventieve maatregelen genomen te hebben en dan gebeurt het toch dat data gelekt wordt. Meestal door menselijk falen. Bestuurders zijn over het algemeen niet 'enthousiast' om lekken te melden juist vanwege in hun ogen de mogelijke publiciteit en reputatieschade. Zo wordt bij fraudegevallen ook om dezelfde redenen niet altijd aangifte gedaan. Senior management snapt niet altijd dat een lek altijd kan gebeuren (100% beveiliging bestaat niet) en dat een juiste respons ook tot de maatregelen behoort.

Het bewust niet melden van een datalek is sowieso geen optie (en de boete) omdat het gewoon een overtreding van de wet is. Als dat later toch nog aan het licht komt is de reputatieschade nog veel groter. Hoe hoog de boetes zullen uitvallen is nog onzeker maar de bedragen die genoemd worden zijn maximum bedragen en dan moet je het wel heel bont gemaakt hebben.

Lex Borger

Er zijn vele andere redenen waarom het aantal meldingen nog niet op het verwachte peil zou kunnen zijn. De meldplicht is nog maar net ingesteld. Ook al is het een plicht, er zal zeker sprake zijn van een mate van gewenning. Ten eerste moet je kunnen detecteren dat er gelekt is. En na detectie moet er het bewustzijn zijn dat dit gemeld moet worden en er moet een proces zijn waaronder gemeld wordt. Dit vindt plaats in een bestuursomgeving die eigenlijk van geen lekken wil weten en deze liever ook niet meldt. Je gaat liever afwachten wat een ander doet of wat een ander overkomt. Dit heeft niets te maken met het bewust niet melden, het is meer 'niet erg vinden' dat men onbewust onbekwaam is...

Bewust ontduiken doen bestuurders liever niet. Als men bij de Autoriteit Persoonsgegevens daarachter komt, dan heb je echt een probleem! En je moet je hierbij voorstellen dat het ook nog niet duidelijk is wanneer de AP overgaat tot boetes en hoe hoog die dan zullen worden.

Hier zal de AP het echt moeilijk hebben. Aan de ene kant moeten ze klaar zijn voor de grote aantallen mogelijke meldingen, maar aan de andere kant zullen ze moeten dulden dat het langzaam zal gaan om die grote aantallen te bereiken. Het beste wat de AP kan doen, is het publiek inzicht geven in de meldingen die gedaan worden. Analyseer ze, categoriseer ze en meldt de aantallen en de statistieken. Dit zal het nodige bewustzijn creëren met twee effecten: ten eerste went het publiek aan de verschijnsels datalek en meldplicht, de grote imagoschade na melding blijft dan uit. En ten tweede weten bestuurders zo wat hun risico is: de kans om gepakt te worden maal de hoogte van de boete.

Maarten Hartsuijker

Bij nieuwe wetgeving is het voor organisaties altijd aftasten wat de reikwijdte en de grenzen van de wet zijn. Dit geldt ook voor de wet datalekken. Want wanneer is iets eigenlijk een inbreuk op de beveiliging (datalek)? En wanneer "slechts" een geconstateerde kwetsbaarheid? Moet je bijvoorbeeld een beveiligingslek als datalek melden als je vanuit eigen audits vaststelt dat klantdata onvoldoende beschermd is geweest? Met welke mate van zekerheid mag je op basis van logs uitsluiten dat een kwetsbaarheid niet uitgebuit is geweest? Ik zie verschillende juristen hier momenteel verschillende afwegingen maken. En dat is niet vreemd. Want naast de wet zijn er weliswaar zienswijzen en toelichtingen gepubliceerd, maar er zijn naar mijn weten nog geen boetes opgelegd. Noch zijn opgelegde boetes getoetst bij een rechter. En dergelijke jurisprudentie is voor bedrijven erg belangrijk om een goede risicoafweging te maken. Op dit moment weet je als organisatie immers zeker dat een melding kan leiden tot reputatieschade, maar weet je in heel veel kleinere gevallen nog niet zeker of een incident ernstig genoeg is om voor melding (bij de AP en/of betrokkenen) in aanmerking te komen. Sommige organisaties kiezen er daarom voor om het zekere voor het onzekere te nemen: alles wordt gemeld. En andere organisaties kijken de kat nog even uit de boom totdat ze zeker weten hoe ze hier op een passende wijze mee om kunnen gaan.

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
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
MOS bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn
Maarten Hartsuijker (Classity)
Rachel Marbus (KPN)
Bart van Staveren

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
T (033) 247 34 00
ibmagazine@pvib.nl

VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

UITGEVER
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
e-mail: secretariaat@pvib.nl
website: www.pvib.nl

ABONNEMENTEN 2016
De abonnementsprijs in 2016 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

VERDRAAIDE FEITEN

We gaan het niet meer hebben over de autofabriek uit Wolfsburg. Het is verleidelijk om de ingenieurs daar nog eens onder uit de zak te geven, maar die arme jongens hebben genoeg ellende over zich uitgestort gekregen. Nee, ik ga een paar jaar terug, terug naar de periode dat de regering bedacht dat zuinige auto's minder wegenbelasting/bijtelling (of helemaal niets) hoefden te betalen. Daarmee werden deze auto's ook zeer populair in de lease.

Om een lang verhaal kort te maken; mijn vrouw kreeg een auto met het zogenaamde A-label uit het land waar de maffia huist. Vrij van wegenbelasting en ontzettend zuinig. Met dat karretje zouden we maar liefst 29,7 kilometer kunnen rijden voordat de eerste liter benzine verbrand was. Dat is echt veel en de auto is dus erg zuinig. Trots als een pauw rijdt mijn vrouw in haar auto.

Na een paar week meldt ze dat het 'tank is leeg'-lampje brandt. "Hoeveel kilometer heb je gereden?", vraag ik. Ze antwoordt "zeshonderd". Ik geef haar aan dat ze twaalfhonderd kilometer op een tank kan rijden. Ze vindt het vreemd dat de auto desondanks aangeeft dat hij weer volgegooid wil worden. Ik geef haar deze keer gelijk. Ik gooi hem vol en rijd direct door naar de garage die me deze auto heeft verkocht. Ik wacht geduldig op mijn beurt en begin verhaal te halen bij de verkoper. Bij het aanhoren van mijn verhaal ontstaat een grijs op zijn gezicht. Aan mijn reactie merkt hij wel dat ik een ander gezicht van hem verwacht.

Hij vertelt mij hoe dat gemeten wordt, met aparte banden, airco uit, radio uit, alle spiegels eraf, randen afgeplakt en een chauffeur van 40 kilo die getraind is om het parcours zo zuinig mogelijk af te leggen. De buitentemperatuur moet tussen de twintig en vijfentwintig graden liggen en het is altijd windstil. Hij voegt toe dat de auto zelfs apart wordt afgesteld voor de proef. Ik ben blij dat ik een riem om heb anders zou de broek afgezakt zijn. "Maar wat bedoelen jullie dan met die 29,7 kilometer?", vraag ik hem. Met name de 'komma 7' geeft toch aan dat het een erg precieze test is, anders noteer je geen decimalen. Ik vertel hem dat ik nog geen vijftien kilometer op een liter kan rijden.

De man complimenteert mij met dit mooie verbruikscijfer en geeft dan aan dat ik dan wel heel erg zuinig kan rijden. Ik doe mijn handen gauw in de zak om mijn eerste neiging te onderdrukken. Dit durf ik diefstal bij daglicht te nomen. Oké, ik hoef geen wegenbelasting te betalen, maar op basis waarvan? Op basis van onhaalbare verbruikscijfers? Waar is de integriteit?

Het resultaat van de belastingmaatregel was duidelijk, met name de A-label diesels waren niet aan te slepen. De hybride auto's idem dito. En de lage verbruikscijfers werden niet gehaald. Dit soort flauwekul met belastingvoordeel is inmiddels achter de rug en het resultaat is dat de A-label auto's veel minder verkocht worden en snel in waarde dalen. Miljoenen minder belasting is er gevangen en wat levert het nu op? Tja, wie het weet, mag het zeggen.

Berry

SecureLink als Managed Security Services partner.

"Onze cybersecurity specialisten staan 7*24 vanuit het Security Operations Center klaar om u te helpen. Resultaatgericht, met een no nonsense mentaliteit en ruime expertise op het vlak van security en infrastructuur."

Peter Mesker • CTO SecureLink Nederland

Safely enabling business

De continue monitoring en detectie en de daaropvolgende actie zijn van cruciaal belang om een security breach te voorkomen. Met het hebben van de juiste security componenten in de infrastructuur ben je toch veilig?

Niets is minder waar! Het vereist frequente aanpassingen van de security policies maar ook continue monitoring en analyse om te kunnen detecteren waar eventueel geïnfecteerde endpoints zich bevinden. Een Managed Security Service welke niet alleen voorziet in monitoring en alarmering maar die daadwerkelijk ook analytics, forensics en dus incident response biedt, is essentieel bij het verhogen van uw security niveau.

www.securelink.nl

SecureLink Infrastructure Security Solutions