INFORMATIEBEVEILIGING MAGAZINE

Thema: Supply chain management in informatiebeveiliging - deel 1

- Managing Supply Chain Cybersecurity Risk through Life Cycle Modelling
- Tips en tricks voor het MKB om te starten met TPRM
- Security innovation and tech transfer

JAARGANG 24 - 2024 - EDITIE 4

ISOPlanner

Eenvoudig Compliance Management in **Microsoft 365**

Hoe SPIE Nederland de informatiebeveiliging op orde heeft en op toekomstige wetgeving is voorbereid

SPIE Nederland kreeg in korte tijd hun certificeringsproces op orde en stoomde de organisatie klaar voor een ISO 27001 audit.

Door de samenwerking met ISOPlanner:

- ✓ Nam de structuur en overzicht van het certificeringsproject toe.
- ✓ Sorteert SPIE NL nu voor op toekomstige wetgeving.
- ✓ Ervaart SPIE NL veel meer gemak en eenvoud bij certificeringsprocessen.

ISOPlanner is de enige integrale compliance oplossing in Microsoft 365. Uiteraard ook voor de overheid (BIO), NEN 7510 en NIS2.

Snelle implementatie van je ISMS door meegeleverde voorbeeldmaatregelen, templates en voorbeelddocumenten.

SPIE NL IT heeft de ISO 27001 certificering met een positief resultaat doorlopen. Wat mede heeft bijgedragen aan dit mooie resultaat was de inzet van ISOPlanner als ISMS.

Leon van der Valk
SPIE Nederland B.V.

Kijk op **www.isoplanner.app** voor meer informatie en jouw gratis proefperiode.

ISO 27001 2024 COMPLIANT
GDPR 2024 COMPLIANT
PENTEST 2024 SECURE

Dienstmededeling

Chris de Vries

Een 'dienstmededeling' aan onze gewaardeerde lezeressen/lezers. Dit jaar zijn vijf uitgaven gepland van ons magazine, waarbij iB4 (dit nummer) het thema 'Supply Chain' draagt en iB5 het thema 'Quantum Computing'. En zoals het met veel goede plannen gaat: wij als redactie wikken en anderen beschikken. De redactie constateerde dat iB3 'Onderwijs & Onderzoek' een mooi succes bleek te zijn. De 40 geplande pagina's overschreden wij met 12 (+30%) en jullie konden genieten van een extra dik magazine. Daarna weer verder op de oude tour van 40 pagina's en twee uitgaven voor 2024 te gaan.

Maar niet dus. iB4 kent een dermate groot aanbod aan artikelen dat wij wederom op 52 pagina's uitkwamen en dan hadden wij nog niet alle artikelen ontvangen. Wij zagen 16 extra pagina's aankomen. Een uitgave, zoals ons magazine, is aan budgetten gebonden en die limiteren wat wij kunnen en mogen. Dus terug naar 40 pagina's voor iB4, 12 pagina's naar iB5 en dat aangevuld met de nog komende artikelen. Conclusie: wij zijn eigenlijk nagenoeg klaar voor 2024. Een nog nooit eerder vertoond fenomeen! Concreet betekent dit, dat iB4 qua inhoud zal worden gespreid over twee uitgaven; dus iB5 wordt deel 2 over het thema 'Supply Chain'. Het oorspronkelijke thema gaat over naar 2025 en de verwachte 'special' in samenwerking met TNO c.s. komt in 2025 uit. De special 'Quantum Computing' komt in iB2 ter wereld.
Het succes van dit aanbod is niet enkel de redactie toe te schrijven, juist ook de auteurs van binnen alsook van buiten onze vereniging. Onze dank, en wij vertrouwen erop dat wij in 2025 deze mooie ontwikkelingslijn kunnen voortzetten.

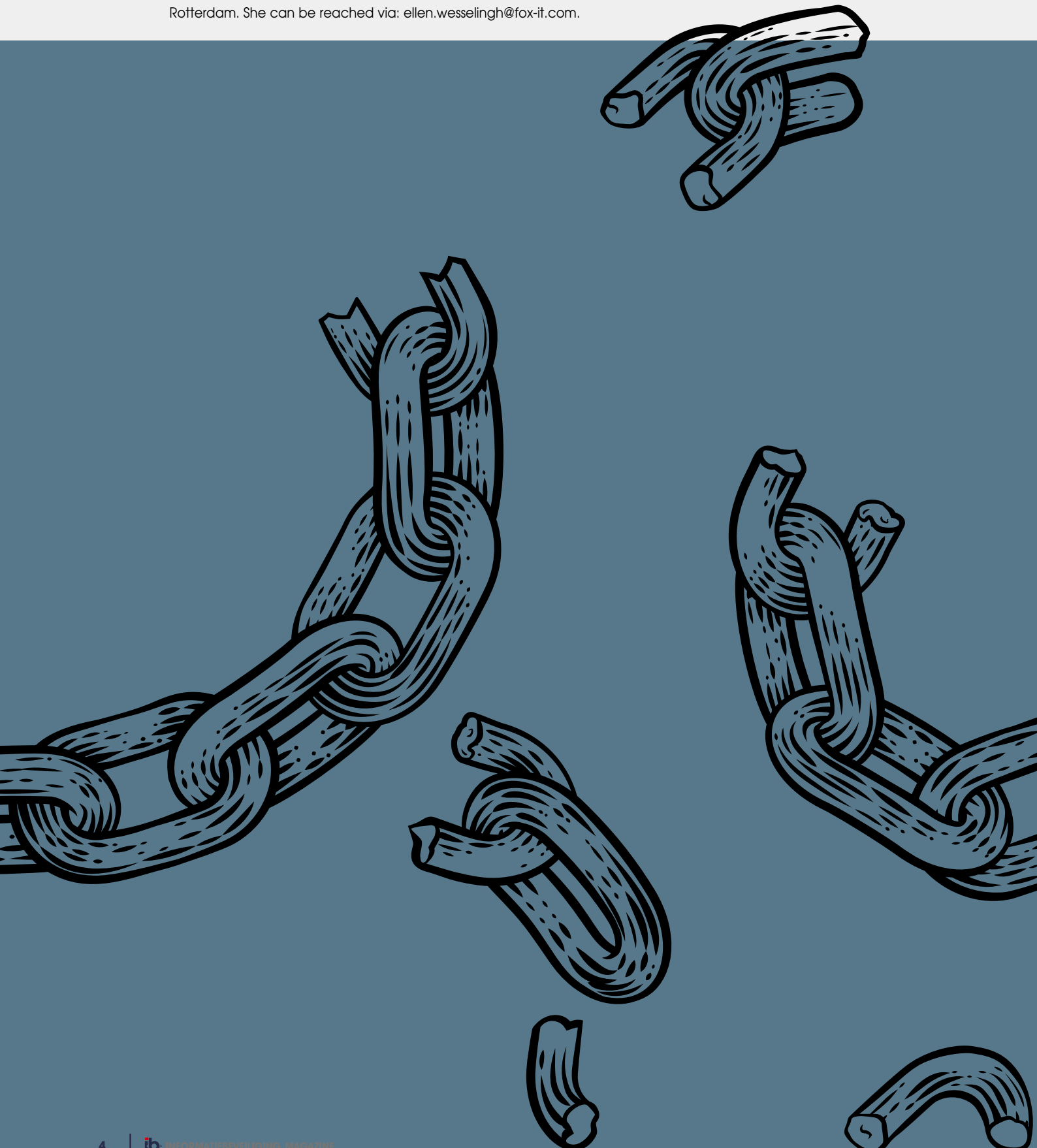
In deze uitgave vraag ik bijzondere aandacht voor het artikel: 'Managing supply chain cybersecurity risk through life cycle modelling' van Ellen Wesselingh. Ook het lezenswaardig en instructief verhaal van Ronald Eygendaal met als uitdagende titel: 'Bye Bye Chinees, welkom Pool' plaatst zich in ons blikveld. Kijken, hoezeer jullie je herkennen in zijn ervaringen.
Onze vaste columnist Martijn Hoogesteger kaart het thema ransomware aan en dat gericht op de supply chain. Hij laat zien hoe ransomware een puur zakelijk bedrijfsmodel is, van herinvestering van afgeperste gelden (in 2023 3 miljard US dollar) in professionalisering van hun misdadige sector. Aardig gedachte-experiment: is een zakelijk bedrijfsmodel misdadig of een misdadig bedrijfsmodel zakelijk? Iets voor de creatievelingen onder ons: doe het niet of doe het wel. En een stap verder: onze tegenmaatregelen, hoe definiëren wij die?

En neem dan eens de column van Lex Borger onder ogen met de uitdagende titel: 'De keten platslaan'. Zijn terugblik op 24 jaar informatiebeveiliging en op de rolverwisselingen tussen beheerder en gebruiker geeft een andere invalshoek op voorgaande, uitgelichte artikelen.
De redactie wenst jullie allen een boeiende leestijd toe.

Chris

IN DIT NUMMER

Author: Ellen Wesselingh is senior with subject matter expertise in product security certification, Member Workfield Committee HBO-ICT bachelor NSE program in Delft and Member Workfield Committee HBO-ICT bachelor Computer Science program in Rotterdam. She can be reached via: ellen.wesselingh@fox-it.com.



Managing Supply Chain Cybersecurity Risk through Life Cycle Modelling

Eliminating the weakest link

In recent years, supply chain issues for products with digital elements have increased, which poses a problem for the assurance of the Integrity of these products and the confidelity of the data contained in these products. To illustrate the problem, this article provides a number of examples of supply chain attacks that have happened over the last couple of years. The article also provides a model for supply chain risk analysis. This model is based on an existing model from 2013, which is amended with a level of abstraction to ensure the model is as complete as possible. A risk analysis that has been conducted with the support of this model, complemented with an additional analysis of the remaining risk, should provide a sufficient argument that the supply chain is secure enough for its purpose.

This article discusses recent developments in products with digital elements that may lead to security issues when systems with these elements are deployed. It also discusses possible solutions. One problem is not addressed: misinformation. While a major problem, misinformation makes the product less reliable in the eyes of the beholder. That means it is not the target of this model, because it does not address the security of the system. Misinformation however, may lead users of the system to less secure choices.

It is recommended to use (internationally recognised) standards for interoperability, industry standard development tools for quality assurance, and to re-use architecture, designs, firmware, and software for cost efficiency and development time reasons. However, since the (re-)use of these components expands the supply chain to a great extent, this leads to a higher possibility of supply chain attacks.

In the past ten years, supply chain problems have become more apparent. This can be seen from examples such as Meltdown and Spectre, which have shown hardware architecture choices can introduce the possibility of sophisticated hardware attacks. Kaseya and Solarwinds have shown a similar introduction of attack possibilities through supporting services. Another seminal example is the Dutch case of Diginotar, in which a certificate issuing service was hacked. These examples have made it clear that hackers can attack potentially interesting targets through their supply chains. This is especially true for high assurance products that are potentially interesting targets for Advanced Persistent Threats (APTs), also known as state actors. Such targets with much exposure include industries such as the energy, the financial and the military sector.

Hardware supply chain attacks can be distinguished into two categories. The direct hardware supply chain attacks are executed by actively inserting backdoors and/or trojans in hardware, while the indirect hardware supply chain attacks, such as Meltdown and Spectre, result from genuine design decisions with adverse security consequences. Similar considerations have to be made for firmware and software, with the distinction that

Supply chain attacks are a real risk, especially for high assurance products

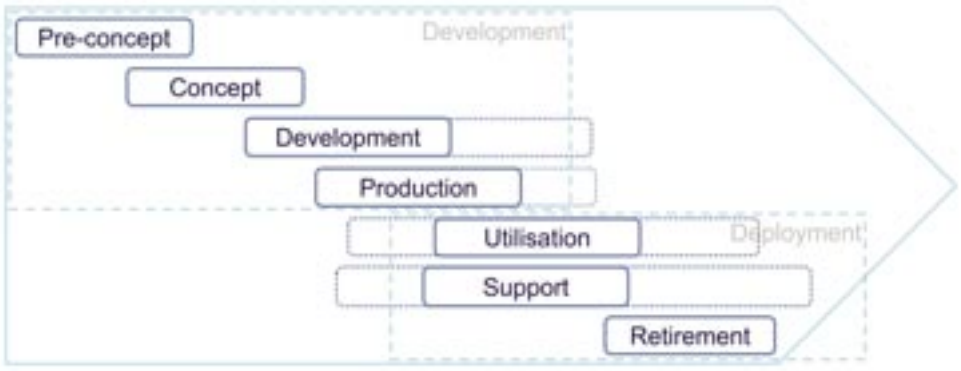


Figure 1: Life cycle model.

these may be updated on production systems, whereas that is usually not possible for pure hardware systems such as IC and ASIC.

A target can be the supply chain for direct organisational operations, such as the production supply chain. But indirect supply chains can also be targeted, affecting services that an organization uses for marketing research. Other similarly indirect operations, such as a financial backend, or a Human Resources Management (HRM) system, may be just as vulnerable. The bottom line is that organisations should be aware of all their supply chains and the way these elements may interfere with critical business operations, even when they are perceived remote elements of the complete operation with all its supply chains.

The primary focus of this article is to develop a supply chain attack framework that addresses the primary process in which a product with IT components is produced. Such products may consist of hardware, firmware and software, a combination of these three or (development) system information or other product data. Supply chain issues that affect the systems which support the development environment are also addressed.

Secondary services such as the supply chain of other office processes or communication processes are not in scope, but may be addressed in future work. The same holds for supply chains of services that are provided to customers.

Methodology used

The research was inspired by a presentation from Andrew Huang for a Blue Hat conference. In his presentation, Huang mentioned a number of attacks for which the articles describing those attacks were analysed for further ideas and references (snowball method). Subsequently, a search for (hardware) supply chain attacks with more generic keywords was conducted to find other supply chain hardware attacks. These attacks were then analysed. No specific search for software issues was done in this phase because of the overwhelming amount of software security problems.

Once a list of relevant hardware supply chain attacks was compiled, a search was conducted to find existing life cycle frameworks and supply chain frameworks. This search yielded a list with possibly relevant frameworks from credible institutions such as ISO, MITRE, NATO, NIST. Once the list was compiled, the most relevant existing framework was chosen. The ISO, NATO and

NIST frameworks mainly address single organisations, and tell how to fix problems in a standardised way. The MITRE framework shows what can go wrong and what the possible solutions can be.

The existing framework used a different life cycle model and was therefore transformed to the life cycle model in use at this company. The chosen framework provided a list of attacks in the various life cycle stages and a list of countermeasures that may be taken against the attacks. The new model was amended with an attack in the retirement stage, the new life cycle model is shown in figure 1.

The model was then validated for usability by applying it to an actual supply chain situation from the stakeholder. Following the application, several new countermeasures were added, and the model was introduced to colleagues. It has since then been used on actual supply chain situations multiple times.

This article describes how the model was re-worked by rearranging the attacks and countermeasures. The framework was developed in several stages. In each stage, the model was validated by peer review with expert colleagues internally. In between those stages, the framework was applied to actual project questions, leading to validation of the model.

In the course of writing this article, information on supply chain attacks and vulnerabilities for firmware and software was sought. One of the examples that was found is Log4J, an Open Source Software (OSS) component widely used in many IT systems, of which the administrators and users were often unaware that it was used in their applications.

Further, an overarching layer of abstraction was added to show more convincingly model completeness. Finally, the model was validated by giving presentations to peers in the field, leading to useful feedback.

Updated model

Figure 2 shows the highest abstraction layer of the model. The model contains different layers of abstraction of the product. The development environment is modelled as relevant for all stages of development: standard, architecture, hardware, firmware, software. Secondary services such as financial backend or HRM system are out of scope for this model.

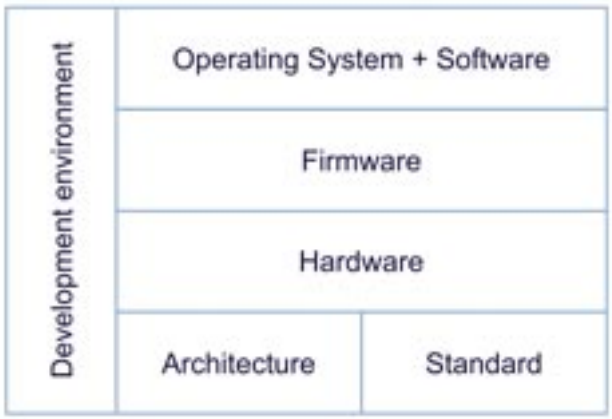


Figure 2: Attack surface categories.

Figure 2: Attack surface categories defines the attack categories in which various attack types can be identified. They also provide specific examples of such attack types. Below is a list of attack types and examples in each category:

- Architecture: attacks as a result of architectural design choices. Examples are Meltdown and Spectre, which may be categorised as either Architecture or Hardware.
- Standard: attacks as a result of vulnerabilities in the standard that is used. An example is Terrestrial Trunked Radio (TETRA). Parts of the TETRA standardised protocol contain vulnerabilities due to government restrictions on the cryptography used.
- Hardware: attacks based on genuine design choices like Meltdown and Spectre. Other examples include attacks based on malicious additions to the design in pre-concept, concept, development and production stages.
- Firmware: attacks based on genuine design issues, such as the Joint Test Action Group (JTAG) interface. This interface is necessary for testing during development and production and to provide updates during support. Other examples are attacks based on malicious additions to firmware design in concept, development, production or utilization/support stages of which Stuxnet is an example. Note that the firmware definition used is the following: makes a generic component a fixed function device. This fixed function device can still be updatable.

- Software: attacks based on genuine design issues such as Log4J, an OSS Java-based logging utility often used in web applications, which had multiple vulnerabilities due to programming issues. Other examples are attacks based on malicious additions to the design in pre-concept, concept, development, production and utilization/support stages, such as typosquatting or dependency confusion. In this article, software consists of operating system and any application running on that operating system.
- Development environment: attacks on data and/or systems, based on genuine design issues in the supplied systems like Kaseya and Solarwinds. Other examples are attacks based on malicious additions in the supplied systems (backdoors, ransomware, trojans, viruses). These issues may also arise in the production environment. On 29 March 2024, a new attack vector in the development environment emerged: the human factor.

The categories, including attack types, are combined with the chosen life cycle model. This life cycle model has seven stages, described below. It is important to note that the stages are not linear.

1. Pre-concept, in which generic (market) research is performed to find the customer needs, requirements and wishes.
2. Concept, in which a Proof Of Concept (POC) is developed to validate the results of the pre-concept research.
3. Development, in which the POC is developed to a Technological Readiness Level (TRL) for production.
4. Production, in which the developed system is produced and delivered to the customer.
5. Utilisation, in which the system is deployed, this stage incorporates the acceptance and installation.
6. Support, in which the deployed system is being maintained in an operational and secure state.
7. Retirement, in which the deployed system is securely destroyed to prevent persistent data leakage.

Note: the development and production stages run parallel in part, and the stages utilisation and support stages run largely parallel. In the definition of the Common Criteria standard, the production stage is considered part of the family Development Security (ALC_DVS).

For each attack type as listed, they are projected on the life cycle stages. Subsequently, the corresponding countermeasures for each attack are added to the model. All countermeasures are categorised by their applicability to the various attack types.

Combined, the attacks and countermeasures provide a model which can be used for supply chain attack risk analysis. This method is a qualitative method, which means that it does not calculate the risk that an attack is feasible. However, it shows any remaining risk in the supply chain that can either be accepted or mitigated with measures such as insurance. A simplified model is presented in Figure 3: Life cycle with attack type categories. This figure assumes an ideal world in which hardware is developed and produced first. The full model with the details of attack types and countermeasures can be found in the appendix.

The model was further elaborated in multiple steps:

1. Reshuffled the original list of attacks into the newly defined categories Architecture, Standard, Hardware, Firmware, Software, Development environment. Discussed the attack list with expert colleagues. Analysed each attack for essentials such as the entity that is in control when the attack is staged, or whether the attack is staged at control handover in the life cycle or supply chain (which is a vulnerable point and frequently used for the staging of attacks).
2. Re-categorised, combined and rewrote the original list of attacks into abstract overarching attacks in the newly defined categories, reducing the number of attack descriptions from 42 to 20. Described more specific examples of subcategories of attacks within the most abstract categories and attributed them to three different problem domains that were defined:

1. Benign (design) decisions which lead to future problems due to insufficient focus on, or insight or knowledge of possible cybersecurity problems arising from those decisions;
2. Genuine mistakes in design or implementation due to insufficient security awareness, lack of security expertise or training;
3. Malicious mistakes or alterations to change the intended functionality of components, systems, or solutions.

The attacks were then mapped to the life cycle model, giving the figure on the next page.

The supply chain risk analysis may show that there are residual risks that remain even after application of all realistic countermeasures. In that case, the stakeholders or the customers must decide what to do with the residual risk: risk reduction in business processes or in the environment, or with other measures. This research was commissioned by the NLNCSA, part of the General Intelligence and Security Service of The Netherlands. The article is endorsed by Dutch crypto industry. The full article can be found at https://foxdatadiode.com/news/

This starts with a risk analysis, for which a supply chain risk analysis model was devised

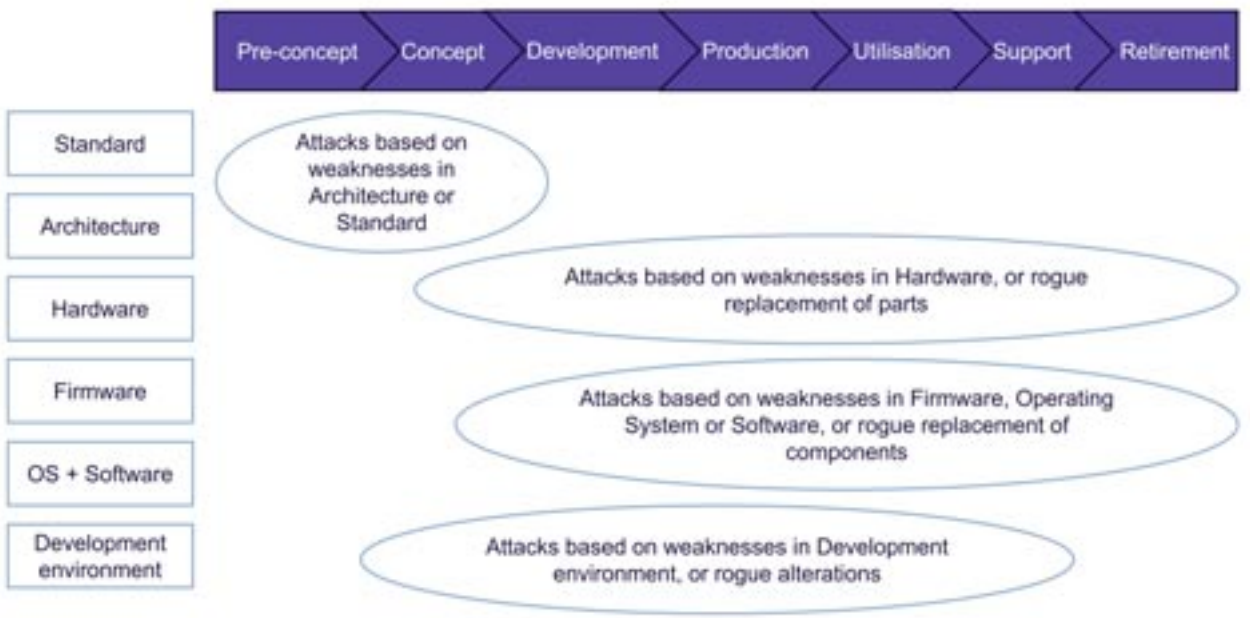


Figure 3: Life cycle with attack type categories.

Discussion and Conclusions

Supply chain attacks are a real risk, especially for high assurance products. There are multiple types of attacks that can be staged in the supply chain. To counter this problem, risk reduction is necessary. This starts with a risk analysis, for which a supply chain risk analysis model was devised. The developed model is based on a number of well-established standards and on sources of expertise, which together have led to a new model as presented in this article. In the process of updating the original model, the new model was validated in various stages and with varying groups with expertise in the field.

The model provides a basis for supply chain risk analysis that is suitable to identify possible attacks and can show how to mitigate these attacks with countermeasures. The exact implementation of the countermeasures is not part of the model.

This research was commissioned by the NLNCSA, part of the General Intelligence and Security Service of The Netherlands. The article is endorsed by Dutch crypto industry. The full article can be found at https://foxdatadiode.com/news/4

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Schuld en boete

Als kind droomde ik ervan eens in het pakhuis van Dagobert Duck te mogen rondzwemmen. Het klaterende goud rondsproeiend terwijl ik een bommetje maak vanaf de duikplank. Spannend was het ook nog eens! Er waren namelijk altijd boeven die het voorzien hadden op de glinsterende goudstukken. En zo is het natuurlijk eender in de mensenwereld waar door middel van bijzondere babbeltrucs en louche linkjes mensen hun geld afhandig wordt gemaakt. Recent waren vele klanten van bunq de pineut. Zij zagen binnen een half uur hun bij elkaar gespaarde centjes in rook opgaan.

Eigen schuld, dikke bult zei de bank. Had je maar niet op dat linkje moeten klikken, en daarnaast, je weet toch best dat wij nooit met je zouden bellen over je bankzaken? Nicole van der Meulen (columnist van dit magazine – red.) schreef er een raak opiniestuk over in NRC (1), waarin ze de vraag opwierp of het in deze tijden van deepfakes en andere AI-toepassingen nog wel terecht zou zijn om alle schuld op het bord van de klant te leggen. En ik denk dat ze daar een heel sterk punt heeft. Als de technieken rond misleiding zo sterk zijn dat je er bijna wel in moet trappen, is de schuld ver te zoeken.

Het gaat sowieso niet zo lekker met dat schuld toebedelen in de financiële sector. Recentelijk kwam wederom naar buiten dat personen met legitieme zaken (coffeeshops, bordelen) het maar niet lukt om aan een bankrekening te komen doordat ze als te risicovol worden aangewezen in screenings die terrorismefinanciering en witwassen zouden moeten tegengaan. Gegevens die ook uitgewisseld worden, dus eenmaal afgewezen en een label krijgen, betekent overal de kous op de kop. Een coffeeshophouder had noodgedwongen de eigen rekening dan maar gebruikt, die pardoes geblokkeerd werd door de bank – de relatie werd de wacht aangezegd. Het Gerechtshof in Arnhem oordeelde in deze zaak dat de bank het bij het verkeerde eind had – een bedrijf mag niet geweigerd worden omdat het in een bepaalde sector actief is.

Nu we toch over schulden bezig zijn. Die kredietregistratiebureau's laten ook nog weleens een pijnlijk steekje vallen. Informatie over schulden blijft extreem lang bewaard, bij het BKR is dat nu nog vijf jaar en in een nieuw Nederlands wetsvoorstel zal dat drie jaar worden. In de praktijk betekent dit, dat als jouw schuld afgelost is je nog jaren daarna geregistreerd blijft staan. En je daardoor bijvoorbeeld een hypotheek zou kunnen mislopen of geen abonnement bij een telecomprovider kunt afsluiten, terwijl daar dus allang geen geldige reden meer voor is. De Autoriteit Persoonsgegevens hekelt deze gang van zaken en dringt aan op een wijziging: als je schulden zijn afgelost, hoor je een schone lei te krijgen.

Het rommelt aan alle kanten in de financiële wereld en het wordt hoog tijd dat we serieus werk maken om klanten echt te beschermen door op een ethisch verantwoorde manier met hun gegevens om te gaan.

Rachel

(1) Met nog een rapport gaan wij cybercrime niet bestrijden Nicole van der Meulen NRC 16 juni 2024

Martijn Hoogesteger is Head of Cyber bij S-RM en is bereikbaar via m.hoogesteger@s-rminform.com.

COLUMN MARTIJN

Wat zou je doen met één miljard?

Meer dan één miljard dollar betaalden we aan cybercriminelen in 2023. We weten dit bedrag te herleiden omdat de betalingen allemaal via cryptocurrency verliepen en die transacties zijn publiek te volgen. Een recordbedrag, het is zelfs een verdubbeling van het jaar ervoor. Deze trend zien we in 2024 helaas alleen maar doorstijgen.

Waarom is dit bedrag zo groot? Deels omdat er nog nooit eerder zoveel ransomwareslachtoffers waren. Als je het losgeld niet betaalt, wordt je naam (en data) op de website van de ransomwaregroep gezet. Bijna 5000 slachtoffers werden in 2023 op het darkweb gepubliceerd. Wetende dat ongeveer 40-60% van de slachtoffers betaalt, betekent dit tussen de 8000 en 12000 slachtoffers.

Een belangrijke reden waarom er zoveel slachtoffers waren, was een focus op het vinden van nieuwe kwetsbaarheden (zero-days) en het aanvallen van de supply chain. Plaats jezelf in de schoenen van de criminelen: waarom zou je de moeite doen een bedrijf aan te vallen waarmee je maar één slachtoffer maakt, terwijl je een bedrijf met een hoop klanten kunt aanvallen en je 100 slachtoffers hebt? Vooral voor de ransomwaregroep Cl0p, in Nederland goed bekend, is dit hun verdienmodel.

De bijna drie miljard dollar die in totaal naar ze is gestuurd in de afgelopen vier jaar komt hen nu goed van pas. We weten uit bronnen binnen deze groepen dat er hele teams van criminele experts worden ingehuurd om kwetsbaarheden te vinden, bedrijven te onderzoeken, en tools te ontwikkelen om aanvallen nog slimmer uit te voeren. Het is ook gewoon een standaard bedrijfsstrategie: je geld investeer je daar waar je weet dat er nog meer winst te behalen is. Wat zou je er anders mee doen? Je land kun je niet meer uitreizen, je bent crimineel.

Ook statelijke actoren richten zich op deze aanvalsvector. Nu is dat niets nieuws, maar het komt steeds meer aan het licht. Zo werd in maart 2024 een kwetsbaarheid ontdekt in een stukje software (liblzma, NX Utils) dat ervoor zorgde dat een aanvaller een code kan laten uitvoeren door SSH. Deze kwetsbaarheid was geïntroduceerd door een ontwikkelaar binnen het project die meerdere jaren reputatie had opgebouwd om deze rechten te krijgen. Er zijn zelfs analyses die erop wijzen dat er meerdere accounts samenwerkten om mensen binnen het project te beïnvloeden zodat deze aanval mogelijk werd. Nu werd deze aanval gelukkig gedetecteerd door een slimme beheerder die zag dat het proces langzamer was geworden, maar ik vraag me af hoeveel van dit soort projecten geïnfiltreerd zijn zonder dat we het doorhebben.

Auteurs: Suyi Guo is Information Security Officier en TPSRM capability owner. Suyi is te bereiken via suyi@protect9.nl.
Sven Enthoven is Information Security Officer. Sven is te bereiken via sven.enthoven@mountaininfosec.com.

Tips en tricks voor het MKB om te starten met Third Party Risc Management (TRPM)

In sectoren die een sterk compliance gedreven aanpak vereisen, hebben bedrijven de laatste jaren hun TPRM-raamwerk opgezet en deze steeds verder uitgebreid. Door middel van onze ervaringen met deze raamwerken willen wij het MKB helpen door een aantal praktische voorbeelden en handvatten aan te reiken. Middels deze tips en tricks kan het MKB, denken wij, een goede start maken met de eigen TPRM-activiteiten.

Organisaties kiezen er steeds vaker voor om bepaalde diensten uit te besteden. Een begrijpelijke keuze, want organisaties doen graag die zaken waar ze goed in zijn en voor het MKB ligt deze stap wellicht nog meer voor de hand. Maar daarbij wordt ook een stukje controle uit handen gegeven. Het uitbesteden van (kern)activiteiten brengt namelijk ook risico's met zich mee. Aanvullende wet- en regelgeving, zoals Digital Operational Resilience Act (DORA) en Network and Information Security (NIS2) eisen dat de focus steeds meer gelegd moet worden op de controle van de (keten van) derde partijen.

Buiten de strengere wet- en regelgeving zijn er tegenwoordig ook legio voorbeelden te vinden waarbij een aanval op een leverancier zorgt voor beveiligingsincidenten bij afnemers. Denk daarbij bijvoorbeeld aan Solarwinds (1), waardoor Microsoft gehackt werd of aan de recentelijke hack bij AddComm waardoor een kwaadwillende potentieel toegang zou hebben gehad tot gevoelige gegevens van ABN AMRO en Waterbedrijf Groningen (2). Dit geeft aan dat het onmogelijk is om alle risico's op voorhand inzichtelijk te hebben en te voorkomen dat een leverancier gehackt wordt. Een TPRM-raamwerk en de daarbij behorende processen bieden inzicht in de potentiële risico's die een organisatie loopt met een leverancier. Een dergelijk inzicht helpt de organisatie om gedegen keuzes te maken in het aantrekken en behouden van de juiste leveranciers.
Het MKB heeft vanwege de beperkte omvang minder kennisgebieden binnen de organisatie. Bij grote organisaties zijn verschillende teams betrokken bij het opzetten en beheren van verschillende raamwerken, zoals bij een TPRM-raamwerk. Bij het MKB ligt dat ongetwijfeld anders, een medewerker van een MKB-bedrijf kan verschillende expertisegebieden hebben, waarbij de medewerkers bij een grote organisatie duidelijkere kaders hebben.

Figuur 1: TPRM Framework.

TPRM-raamwerk

Verschillende organisaties hebben een TPRM-raamwerk gepubliceerd waarin een continue cyclus van stappen wordt doorlopen. Deze raamwerken houden rekening met het vooronderzoek, de levenscyclus van het contract en de afronding. Price Waterhouse Cooper (PWC) heeft een raamwerk opgesteld dat in de afbeedling is weergegeven (3).

Stappen voor een kleinschalige aanpak

In het raamwerk zijn diverse ondersteunende processen en bedrijfsactiviteiten beschreven. Sommige processen en bedrijfsactiviteiten zijn niet exclusief opgetuigd om TPRM te realiseren. TPRM maakt hier enkel handig gebruik van. Binnen het MKB kan

TPRM is een continu proces, waarbij het assessment periodiek herhaald moet worden

het zijn dat deze onderwerpen niet volledig zijn uitgewerkt maar wel onderdeel zijn van het bedrijf.

Om de vertaalslag van het raamwerk naar een kleinschalige, risicogebaseerde aanpak van TPRM te beschrijven, staan hieronder globaal de processtappen voor het aangaan van een nieuw contract. Na een initieel assessment moeten bestaande contracten via continue monitoring worden bijgehouden. Een voorbeeld hiervan zal in het Tiering-onderdeel worden beschreven. Afhankelijk van de eisen van uw organisatie kunnen onderstaande stappen afwijken.

1. De organisatie heeft de noodzaak om een dienst af te nemen en stelt een shortlist van leveranciers op.
2. De leverancier wordt beoordeeld op afhankelijkheid, een veelvoorkomende methode is het gebruiken van een Tiering-model. Dit model wordt later in dit artikel behandeld.
3. Op basis van het Tiering-model wordt de diepgang van het assessment/due diligence opgesteld. Denk hierbij aan de informatiebehoefte om een assessment uit te voeren, de benodigde controls, etc.
4. Het initiële assessment wordt uitgevoerd. In het kader van een voortraject/aanbesteding kan er op basis van het assessment een advies gegeven worden welke leverancier een (on-)acceptabel risiconiveau heeft.
5. De risico's worden met de contracteigenaar en het managementteam besproken.
6. Afhankelijk van de risicoclassificatie van de bevindingen is opvolging en tijdsplanning van toepassing.
7. Afhankelijk van de Tiering zijn er periodiek overleggen nodig om de laatste status van eventuele risico's en afstemming te bespreken.
8. Afhankelijk van de Tiering zijn herbeoordelingen noodzakelijk.

In de voorgaande beschreven stappen is uitgegaan van een nieuwe leverancier. Bij het opzetten van het TPRM-raamwerk dienen deze stappen ook voor bestaande leveranciers uitgevoerd te worden. TPRM is dus een continu proces, waarbij het assessment periodiek herhaald moet worden. Door deze herhaling worden de nieuwste controls en laatste standaarden van het TPRM-raamwerk meegenomen in de beoordeling. Afhankelijk van de bevindingen en of dit voor het tekenen van het contract opgelost dient te worden, kan dit allemaal impact hebben op de planning. En dit kan uiteraard weer per organisatie verschillen.

Voorbeeld van Tiering-model

Het aantal leveranciers die onderdeel zijn van de (kern)activiteiten van een organisatie groeit. Hiermee groeien de risico's en afhankelijkheden die externe leveranciers meebrengen ook. Niet alleen in het kader van wet- en regelgeving, maar ook voor wat betreft bedrijfscontinuïteit is het belangrijk om de risico's inzichtelijk te maken en hier grip op te krijgen. Verschillende organisaties en bedrijven die diensten aanbieden om leveranciers te monitoren maken gebruik van een Tiering-model. Voor meer informatie zie Bluevoyant (4) en UpGuard (5). Gelaagdheid in het Tiering-model kan zo ver gaan als een organisatie zelf wil, dit heeft echter wel impact op de complexiteit van het model. Complexiteit is, zeker in het begin, niet wenselijk en daarom is het aan te raden om klein te beginnen. De verschillende risiconiveaus hebben verschillende vervolgacties en requirements aan zich gekoppeld. Deze vervolgacties zijn verschillend per organisatie. Een eenvoudige opzet van verschillende Tiering-classificaties met drie verschillende risiconiveaus kan er als volgt uitzien:

Tier	Criteria	Activiteiten
1	• Impact op de (kern)activiteiten • Toegang tot gevoelige (bedrijfs)informatie • Complexe wisseling van leveranciers • Omvang van contract • Financiële (en imago)schade is significant • Impact op de bedrijfscontinuïteit is groot	• Jaarlijkse uitvoering van de Due Diligence • Uitgebreide scope van controls van toepassing, afhankelijk van de overeenkomst en opzet van de dienstverlenging • Elke drie of zes maanden overleg met leverancier over (security)incidenten
2	• Belang voor de bedrijfsvoering, maar minder directe impact op de kernactiviteiten • Wisselen van leverancier is mogelijk met enige inspanning • Gelimiteerde toegang tot (bedrijfs)informatie	• Elk ander jaar uitvoering van Due Diligence • Middelmatige scope van controls van toepassing, afhankelijk van de overeenkomst en opzet van de dienstverlenging • Elke drie of zes maanden overleg met leverancier over (security)incidenten
3	• Beperkte toegang tot (bedrijfs)informatie • Eenvoudige vervanging van leverancier	• Eenmalige uitvoering van Due Diligence voor het tekenen van het contract • Beperkte scope van controls van toepassing, afhankelijk van de overeenkomst en opzet van de dienstverlenging

Tabel 1: Voorbeeld Tiering Tabel (afgeleid van (6)).

Door leveranciers in te schalen op een specifiek niveau wordt de organisatie in staat gesteld om op een risicogebaseerde aanpak de leveranciers te beoordelen. Vanzelfsprekend is het zo dat leveranciers met een tier-1 status aan meer controls zullen moeten gaan voldoen, strenger en vaker worden beoordeeld op de controls in vergelijking met een tier-2 of tier-3 leverancier. Een Tiering-model heeft daarnaast als aanvullend voordeel dat wanneer de eisen veranderen voor de leveranciers (denk aan veranderde wetgeving DORA, NIS2), dit eenvoudig te koppelen en toe te passen is op de betreffende leverancier. De samenwerking met een leverancier is ook aan wijzigingen onderhevig. Het advies is ook om periodiek een herbeoordeling van de toegewezen Tiering uit te voeren. Triggers hiervoor kunnen onder andere zijn: wijziging in het contract of periodiek op basis van het TPRM-raamwerk. De periode hangt af van de reeds toegewezen tier. Door de periodieke herbeoordeling van de toegewezen tier, voorkomt een bedrijf dat het leveranciers op een te laag of hoog niveau beoordeeld.

Het toepassen van het Tiering-model dient zowel voor bestaande, als potentiële leveranciers in het aanbestedingstraject worden toegepast, zodat er ook vooraf requirements gedeeld kunnen worden. De bepaling van de geschikte risicoclassificatie (tier) zal een samenspraak van de verschillende betrokkenen zijn, zoals beschreven in de volgende alinea.

Rollen en verantwoordelijkheden

Om de rollen en de bijbehorende verantwoordelijkheden effectief te kunnen beleggen binnen een organisatie,

dienen ze vastgelegd te worden in een beleidsstuk dat ondersteund wordt door het managementteam. Hieronder proberen we inzicht te verschaffen in de activiteiten die een expertrol zou kunnen bieden in een uitbestedingstraject. We benadrukken dat TPRM leunt op bestaande change-processen. De korte beschrijving van de rollen is een versimpelde versie en kan per organisatie verschillen. Eén persoon kan meerdere rollen vervullen. Er moet wel maar één eigenaar toegekend worden zodat het duidelijk is wie de accountability draagt.

Contracteigenaar (servicemanager)

De persoon die bevoegd is om namens het bedrijf te tekenen en uiteindelijk ook verantwoordelijk is voor het verlengen dan wel het beëindigen van het contract met de leverancier. De eigenaar monitort de dienstverlening op de daadwerkelijk geleverde kwaliteiten, vergelijkt deze met de afspraken in het contract en wint adviezen in van experts om een goed beeld te vormen van de dienstverlening. De contracteigenaar zou dit kunnen delegeren naar een servicemanager.

Subject Matter Experts (SME)

De vereiste expertise kan per organisatie en contract verschillen. Bij veel MKB-organisaties zijn bepaalde expertises belegd bij één persoon. TPRM zou in principe geïntegreerd moeten worden in bestaande (risk en change) processen. Hierbij doen we een suggestie naar de mogelijke experts die een organisatie kan hebben om een contracteigenaar te adviseren:

- Security: beoordeelt en adviseert over informatiebeveiligingsonderwerpen
- Legal/compliance: beoordeelt en adviseert of het contract voldoet aan interne eisen en de wet- en regelgeving
- Inkoop: begeleidt het proces van selectie tot aan het beëindigen van het contract. TPRM valt vaak binnen de afdeling Inkoop omdat de levenscyclus van het contract leidend is
- Architectuur: beoordeelt of de (IT-)uitbesteding past binnen de architecturale principes en ontwerp

Het is belangrijk om te benadrukken dat de verantwoordelijkheid van diverse aspecten gedeeld wordt tussen leverancier en afnemer (shared responsibility model), echter is de afnemer altijd verantwoordelijk. De accountability kan niet uitbesteed worden. Voor het beoordelen van de dienstverlening is het belangrijk om dit in gedachte te houden. Voorgaande lijst is niet uitputtend, en is puur bedoeld als voorbeeld. De lijst zou verder aangevuld kunnen worden met Privacy en Financiële expertise. Het management bepaalt vervolgens of de uitbesteding een (verhoogd/(on)-acceptabel) risico met zich meebrengt en bepaalt vervolgens of het contract getekend mag worden.

Due diligence

De volgende fase uit het TPRM-framework is due diligence en onder het kopje Rollen en verantwoordelijkheden blijkt dat de beoordeling van een uitbesteding een multidisciplinaire aangelegenheid is en dat de beoordeling per organisatie kan verschillen. Het wordt aangeraden om hiervoor bestaande 'vragenlijsten' te gebruiken. Het verbond van verzekeraars heeft een gestandaardiseerde vragenlijst (7) (gebaseerd op de ISO 27002 en) beschikbaar gesteld. Organisaties zouden deze vragenlijst op basis van hun tier-lijst kunnen inrichten, door bijvoorbeeld te kijken naar welke maatregelen altijd beschikbaar moeten zijn en welke beschikbaar moeten zijn bij een hogere tier-uitbesteding. Hierbij een simpel voorbeeld wat voor een SaaS-uitbesteding van toepassing zou kunnen zijn (zie tabel 2).

Leveranciers kunnen zelf ook assurance rapporten beschikbaar stellen die door erkende onafhankelijke partijen opgesteld zijn. De gebruikelijke rapporten zijn SOC 2 type 2 en de ISAE 3000 type 2. Deze rapporten zouden de vragenlijst kunnen vervangen. Zo'n assurance rapport biedt inzicht in de geïmplementeerde controls en of deze controls effectief zijn. Het is zeker raadzaam om vóór het tekenen van het contract deze rapportage op te vragen en zeker ook na het tekenen van het contract te blijven opvragen en te reviewen.

Contractonderhandeling

De bevindingen uit de due diligence fase dienen behandeld te worden in het bestaande riskproces. In de praktijk betekent dat accepteren of mitigeren. Elke organisatie heeft een ander risicoprofiel met een bijbehorende risk appetite. Wat voor de ene organisatie acceptabel is om de bevindingen voor het tekenen van het contract op te lossen, is het acceptabel voor een ander om dit op te nemen als een punt te monitoren tijdens de relatie. De security-SME zal tijdens de analyse een inschatting maken van het securityrisico en dit bespreken met de contracteigenaar. Risico's die vallen onder de risk appetite van de organisatie kunnen, in geval van risicoacceptatie, geaccepteerd worden binnen de kaders van de contract-

Referentie	Control	Vereiste minimale tier
11	Heeft uw organisatie een Secure Development Life Cycle geïmplementeerd en is deze ingericht in lijn met een markt standaard (b.v. Microsoft Security Development Lifecycle (SDL), OpenSAMM, BSIMM, SSE CMM, SafeCode of de NIST SSDF? (ISO: 8.25 Secure development life cycle) Penetration Testing is onderdeel van deze cyclus. In (assurance, audit) rapporten moet worden aangetoond dat minstens één keer per jaar een pentest is uitgevoerd en dat de bevindingen uit de test zijn opgelost op basis van de ernst van de bevindingen. (ISO: 8.29 Security testing in development and acceptance)	Tier 1
17	Maakt u gebruik van gescheiden omgevingen voor ontwikkeling, test, acceptatie en productie? Zijn deze voor iedere klant gescheiden (fysiek of logisch)? (ISO: 8.31 Separation of development, test and production environments)	Tier 3 Tier 2 Tier 1

Tabel 2: Voorbeeld van controls in Tiering-model.

eigenaar. Risico's met een onacceptabele rating dienen gemitigeerd te worden: dit kan zowel door compenserende maatregelen te treffen of er moet daarover door de leverancier worden onderhandeld. Hierbij een aantal suggesties om mee te nemen in het contract:

- De periodiek te ontvangen (assurance)rapportages
  - o SOC 2 type 2 / ISAE 3000 type 2
  - o Pentest rapporten
  - o (Her-)certificering van ISO 27001
- De leverancier werkt mee aan de periodieke (her-)beoordeling van hun securitylandschap
- Periodieke overleggen en/of rapportages waarbij de organisatie inzicht krijgt in bepaalde zaken zoals security, performance en incidenten.
- Geïnformeerd worden bij een hack of wanneer er data gelekt is.

Ook kan een organisatie nadenken over het beëindigen van het contract en punten hiervoor opnemen in het contract, een zogenaamde exit plan (8). Punten die in het contract meegenomen kunnen worden zijn:

- Het formaat van hoe de data beschikbaar gesteld wordt en vernietigd wordt na het beëindiging van het contract.
- Ondersteuning vanuit de leverancier om de data te migreren.
- Kennis en expertise die tijdens de migratie beschikbaar dient te komen van de leverancier. Ook hier kan natuurlijk per Tier de eisen verschillen, en niet elke leverancier kan voldoen aan de gestelde eisen en wensen.

Ongoing monitoring

In de voorgaande fases zijn de requirements in kaart gebracht, is de uitbesteding aan diverse SME's beoordeeld en is het contract getekend.. In deze fase willen we met name de tier-1 dienstverleningen en de daarbij behorende leveranciers gaan monitoren. Eerder is al aangegeven dat leveranciers periodiek beoordeeld moeten worden. Hier kunnen we kijken naar het verleden door het lezen van (assurance)rapporten, maar ook door gesprekken te voeren met de leveranciers over toekomstige wijzigingen. De volgende securityonderwerpen kunnen terugkomen:

- Bevindingen uit (assurance)rapporten
- Securityverbeteringen in het SaaSproduct en de organisatie
- Openstaande security-bevindingen

- (Aankomende) significante wijzigingen binnen de organisatie. Daarnaast zijn er diverse diensten beschikbaar die organisaties monitoren op kwetsbaarheden maar ook op het nieuws (9). Sommige bieden aanvullende diensten aan waardoor je als organisatie meer inzicht krijgt in je leveranciers en het risicoprofiel.

Afronding

Met de toenemende mate van afhankelijkheden ten opzichte van leveranciers is het belangrijk om tijdig te beginnen met de stappen binnen het TPRM-proces. TPRM begint al voor het tekenen van het contract en is een doorlopend proces (Plan Do Check Act). Door TPRM toe te passen voordat het contract is getekend, kunnen leveranciers die onacceptabele risico's vormen worden uitgesloten. Ook afscheid nemen van een leverancier is een belangrijk onderdeel binnen het proces. Hiermee wordt het hele lifecyclemanagement op leveranciers uitgevoerd. Als een leverancier vertrekt, is het goed om te weten welke informatie is opgeslagen en hoe het bedrijf ervoor zorgt dat de informatie op juiste en volledige manier wordt verwijderd.

Het in kaart brengen van leveranciers en het toekennen van een tier, kan een grootschalig en complex proces worden. Het advies is om klein te beginnen en gaandeweg uit te breiden. Afhankelijk van het aantal leveranciers kan de benodigde werkomvang berekend worden. Zeker in het begin, bij het opzetten van het raamwerk en het opdoen van de eerste ervaringen zal tijd gemoeid zijn.

Door middel van het toepassen van een risicogebaseerde aanpak wordt de organisatie in staat gesteld om zich te focussen op de leveranciers met de grootste impact. Door middel van het toepassen van het Tiering-model en het gebruiken van bestaande vragenlijsten is een organisatie in staat om snel inzicht te krijgen in de huidige risico's. Bovenstaande handvatten is een begin en de lijst is zeker niet volledig, maar naar ons inziens een goed begin om snel inzicht te kunnen krijgen en vervolgens uit te voeren.

De output van het TPRM-proces dient opgenomen te worden binnen reeds bestaande risicovastlegging en opvolgingsprocessen. MKB-bedrijven moeten de risico's in een managementteamoverleg bespreken en de benodigde vervolgstappen bepalen.

TPRM moet gedragen worden door verschillende expertisegebieden in de organisatie. Door met zijn allen een steentje bij te dragen zal de MKB-organisatie de risico's voor de belangrijkste leveranciers inzichtelijk kunnen maken en hierop kunnen acteren. Dit artikel richt zich voornamelijk op de punten vóór het tekenen van het contract, echter is het continue monitoren van de leveranciers net zo belangrijk, de Nederlandse Bank (DNB) heeft de Good Practice voor informatiebeveiliging 2023 beschikbaar gesteld (10). Onder het kopje Outsourcing staan hier aanvullende handvatten (waar dit artikel verder niet op ingaat) voor het inrichten van third party risk management. Ook hier geldt het advies om een risk-based aanpak te hanteren, waarbij men kijkt naar effectiviteit en haalbaarheid van de maatregelen.

In dit artikel is een beeld geschetst van een TPRM-opzet binnen een MKB-bedrijf, afgeleid van de grotere organisaties. Het is het fundament voor een uitgebreider en volwassener TPRM-proces. Gezien de toenemende mate van afhankelijkheid ten opzichte van leveranciers en de risicogedreven aanpak hiervoor is het van belang om de risico's binnen de gehele keten in kaart te hebben. Zonder het inzichtelijk hebben van de risico's op de bedrijfsactiviteiten is het haast onmogelijk om tijdig bij te sturen en de blootstelling aan risico's tot een acceptabel niveau te beperken.

Referenties

(1) https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
(2) https://www.dutchitchannel.nl/news/458170/eneco-abn-amro-en-anderen-getroffen-door-cyberaanval-op-addcomm
(3) https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/tprm-protecting-operations-brand-reputation.html
(4) https://www.bluevoyant.com/knowledge-center/third-party-risk-management-tprm-a-complete-guide
(5) https://www.upguard.com/blog/vendor-Tiering-best-practices
(6) https://adoptech.co.uk/wp-content/uploads/2020/05/Third-Party-Tiering-Template-1.pdf
(7) https://www.verzekeraars.nl/publicaties/actueel/verbond-stelt-vragenlijst-leverancierselectie-informatiebeveiliging-op
(8) https://www.legalz.nl/blog/exit-plan
(9) https://www.gartner.com/reviews/market/it-vendor-risk-management-solutions
(10) good-practice-ib-2023.pdf (dnb.nl)

COLUMN LEX

De keten platslaan

In de *Code voor Informatiebeveiliging: 2000*, deel 1 (het equivalent van de ISO 27002 norm nu) staan wat opvallende zinnen:

- 'Er zijn diverse redenen om derden toegang te verlenen' en:
- 'Derden dienen pas toegang… te verkrijgen wanneer er passende maatregelen zijn geïmplementeerd en er een contract is ondertekend…'.

Hierachter zit een gedachte: het is niet gewoon dat derden toegang krijgen. Derden krijgen toegang vanaf de fysieke locatie van de organisatie of via een specifiek communicatiekanaal. Derden krijgen pas toegang nadat er een risicoanalyse is uitgevoerd, maatregelen zijn genomen en er een geldig contract is.
Vierentwintig jaar later is het wel anders: toegang door derden over het internet is de norm. De risicoanalyse is gebleven. Contracten zijn steeds meer standaard geworden. Particuliere derden krijgen bescherming: privacybeleid, bancaire zorgplicht.

Deze column gaat over derden met toegang tot de eigen infrastructuur. De principes kunnen ook afgebeeld worden op een SaaS-oplossing, maar dan draaien af en toe de rollen beheerder/gebruiker om, wat het complexer maakt.

Wanneer je gecertificeerd bent tegen de ISO 27001 of NEN 7510 norm, dan mag je stellen dat je zicht hebt op je eigen beveiliging. Heb je dan ook genoeg zicht op de risico's van derden in de infrastructuur van de organisatie? Hier wordt het moeilijk. Het is lastig tot onmogelijk om leveranciers jouw beveiligingsregime op te leggen.

Wat je minstens kunt bereiken is dat je weet wie er allemaal toegang hebben tot welk deel van je infrastructuur, hoe je met deze gebruikers in contact kunt komen en – zonodig – de onmisbare beveiligingsmaatregelen kunt coördineren. Digitale toegang wordt verkregen via een gebruikersinterface (UI) of via een programma-interface (API). Hoe minder de invloed en medewerking van de ander, hoe meer je deze gebruikers wilt isoleren in je infrastructuur. Gebruikers van internetbankieren gebruiken de app en de gateway (API) of de webapplicatie (UI). Op het banknetwerk zul je niet kunnen komen.

Die toegang wordt gecontroleerd door software in de infrastructuur van de organisatie, al moet ik hierbij aantekenen dat daar ook vaak een beroep wordt gedaan op andere dienstverleners, zoals de verificatie van een organisatie-account door de Entra ID service van Microsoft. Het kan snel een wirwar van communicatie via API's over en weer worden, en wat er overblijft is een zogenaamd 'access token' dat vervolgens het bewijs van de gebruiker is dat hij geauthenticeerd en geautoriseerd is: Zero Trust heet dat.

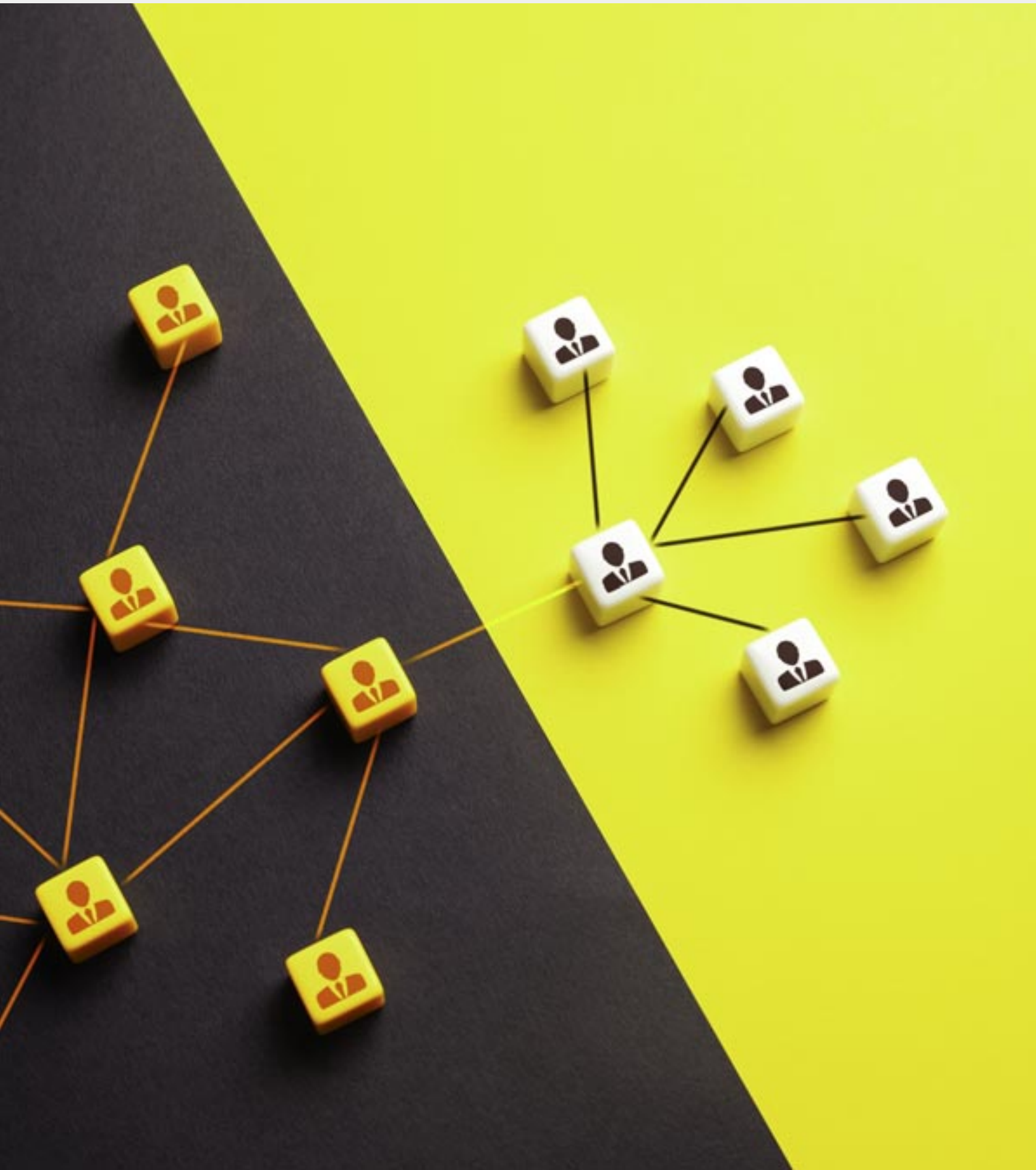
Als het werkt vormt het een prima beveiliging. Als het niet werkt, ligt potentieel je infrastructuur open. De werking van dit mechanisme wil je dus heel goed monitoren. Functioneel én op signalen van misbruik.

De andere maatregel is toch om het bereik van accesstokens van derden in je infrastructuur te beperken. De meest eenvoudige beperking is de locatie in de infrastructuur en data die toegankelijk is. Maar ook functionaliteit en tijd kunnen factoren zijn. Bij een hoog risico: geef alleen rechten af die beperkt zijn tot de situatie en voor een beperkte tijd.

Het aparte is dat dit geen zaken zijn die je (exclusief) in relatiemanagement regelt. Veel komt neer op het hebben van een veilige infrastructuur, een goede toegangsbeveiliging erop en monitoring van de hoog risico activiteiten in jouw infrastructuur. Dit mag je in principe ook verwachten van je SaaS-provider, al is het verstandig dat dan wel contractueel te regelen en je te beseffen dat de regie bij de provider ligt en je mogelijkheden om te monitoren veel beperkter zijn.

Lex Borger is security consultant bij Tesorion en oud-hoofdredacteur van IB Magazine. Lex is bereikbaar via lex.borger@tesorion.nl

Auteurs: Vincent van Dijk, eigenaar van Security Scientist, bereikbaar via vincent@securityscientist.net. Dr. Rick Hofstede, cybersecurity expert en oprichter van Cybermeester. Hij is bereikbaar via rick.hofstede@cybermeister.eu



De externe resources van de cybersecurityketen

'We hebben meer resources nodig', 'We hebben niet de nodige expertise', of: 'Zo kunnen we het project niet op tijd afmaken'. Dit hoor ik vaak van te veel managers van grotere organisaties. Hun reflex is om externen in te huren, zonder te begrijpen welke specifieke vaardigheden en capaciteiten nodig zijn voor het project. Tips voor het inhuren van een securityprofessional.

"De huidige medewerkers zijn al tot de nok toe volgeboekt met hun dagelijkse werkzaamheden", vervolgt de manager, "maar we moeten het project binnen de deadline afronden. Laten we externen inhuren." Dit is het moment waar de manager naar zijn telefoon grijpt en mensen begint te bellen die hij kent. Consultancybedrijven met potentiële expertise, security- en IT-serviceproviders die graag hun diensten of freelancers binnen hun netwerk aanbieden. "Wat heb je nodig?" vraagt de persoon aan de andere kant van de telefoon. "Uhh ..." zegt de manager terwijl hij nadenkt, "een security-architect". Dit alles met de illusie dat in deze schaarse markt specialisten voor een klus per direct klaar zitten en dat inhuur realiseerbaar is op basis van expertise in plaats van capaciteit. Een jaar later heeft het project vertraging opgelopen, is het budget overschreden en zijn er nog zes specialisten ingehuurd om het project af te ronden. Wat is hier gebeurd?

Niet alle specialisten zijn hetzelfde

Bij het inhuren van externe resources voor cyberbeveiligingsrollen en -projecten moet je begrijpen dat niet alle externe krachten gelijk zijn. De effectiviteit van deze resources hangt sterk af van expertise, ervaring en hoe goed ze integreren met het bestaande team. Simpelweg iedereen inhuren met een hartslag en het trefwoord dat je nodig hebt (bijvoorbeeld 'security-architect'), is niet de juiste aanpak.

En het gaat er niet alleen om de juiste mensen te vinden, maar ook om te begrijpen welke specifieke vaardigheden en capaciteiten nodig zijn voor het project en hoe deze externe bronnen beheerd en geïntegreerd zullen worden. Maar voordat je dat kunt doen, laten we eerst eens kijken naar het soort extra handen dat je kunt inhuren.

Er zijn diverse mogelijkheden om specialisten in te huren:

1. Consultancybedrijven
2. Cybersecurityproviders
3. IT-providers
4. Freelancers

Consultancybedrijven

Wij, de gemiddelde managers, kijken sceptisch naar de grote consultancybedrijven. Dit komt vooral doordat ze worden gekarakteriseerd door hun hoge uurtarief in relatie tot hun veronderstelde gebrek aan praktijkervaring, dat laatste zelfs als we kijken naar de grote vier adviesbureaus. Toch blijven we ze op grote schaal inhuren omdat zij de mensen zijn die op 'hoger niveau' denken. Ze bieden strategische begeleiding en helpen onze beveiligingsinspanningen vorm te geven, hoewel vaak te abstract. Hun betrokkenheid vertaalt zich echter regelmatig niet in praktisch, hands-on werk dat we zo hard nodig hebben om de resource gap van onze interne medewerkers en projecten te dichten; te vaak blijven ze steken in de modellen die ze aanhangen. Dit zorgt voor een frustrerende cyclus: we betalen voor waardevol advies op hoog niveau, maar hebben nog steeds niet de mankracht voor de implementatie.

Cybersecurityproviders

Beveiligingsproviders bieden een meer geïntegreerde oplossing. Ze komen met modulaire diensten die strategisch toezicht en operationele uitvoering omvatten. Ze functioneren vaak als

partner, die niet alleen de mensen heeft; maar ook de diensten, producten en leveranciers om je te helpen met verschillende problemen. Je moet vrezen voor vooringenomenheid als ze automatisch verwijzen naar hun eigen portfolio van diensten en producten. "Als cybersecurityproviders al een technisch specialist sturen, voldoen ze aan hun verantwoordelijkheid
tegenover de klant, die dat zocht, echter deze specialisten worden vaak thuisgehouden voor de eigen interne operaties (SOC's, pentesten, IR) en niet voor externe productimplentaties. Dit bijt elkaar, omdat hun prachtig samengestelde modules misschien te rigide zijn en niet werken in het dynamische, unieke karakter van jouw organisatie.

IT-providers

IT-providers zijn vaak een gemakkelijke optie, vooral als je het grootste deel van je IT uitbesteedt. Deze IT-providers kennen jouw infrastructuur (althans, dat hoop je); je verwacht dat hun service toegankelijk en kostenefficiënt is. Een groot beroep doen op IT-providers heeft echter ook zijn valkuilen. Hoewel ze jouw infrastructuur kunnen begrijpen, kan hun brede dienstenpakket soms leiden tot een gebrek aan diepgang in gespecialiseerde beveiligingsexpertise, die ze moeilijk kunnen verwerven dan wel behouden gezien de concurrentie met MSSP's. Hun beveiligingswerk kan ook hun collega's, die aan de IT-kant van de vergelijking werken, direct beïnvloeden en soms zelfs boos maken, wat resulteert in een later gevonden – verborgen kloof. `De slager keurt niet zijn eigen vlees', is een toepasselijke uitspraak in samenhang met het mogelijk gebrek aan onafhankelijkheid van deze IT-providers, die jouw cybersecurity gaan inregelen.

Freelancers

Freelancers vormen een interessante middenweg. Ze zijn vaak betaalbaarder dan adviesbureaus en kunnen een schat aan praktische, praktijkgerichte ervaring inbrengen, terwijl ze het vermogen hebben om zich aan te passen aan jouw organisatie. Het vinden van de juiste freelancers – met de exacte expertise die we nodig hebben – is echter een uitdaging en kost veel tijd. Je weet vaak niet wat je krijgt als je een freelancer inhuurt. Is het een goede of slechte, hands-on of een meer theoretisch georiënteerde freelancer? En, in tegenstelling tot IT-beveiligingsproviders en consultancybedrijven, heb je geen continuïteitsgarantie met betrekking tot hun inzet, juist wanneer je het nodig hebt. Het belangrijkste risico is dat je de freelancer moet vervangen, bijvoorbeeld nadat zij of hij de loterij heeft gewonnen, door iemand die het proces van zijn voorganger kan opvolgen!

Inhuren van een security-architect

Een recente projectie voor een klant toonde aan dat er bij hem een discrepantie zou ontstaan tussen zijn staande organisatie (menskracht, hard- & software) en de groeicapaciteit daarvan versus de vijfvoudige groei van de azure cloud-omgeving in 2026. Met als gevolg dat door de groeiende cloud-omgeving – gekoppeld aan de steeds hogere eisen die het bedrijf moet stellen aan de systemen – het gemakkelijk (b)lijkt te zijn om mislukkingen te wijten aan tekorten in beschikbare personele capaciteiten om de enorme hoeveelheid werk aan te kunnen. Dat is een te makkelijk excuus.

Maar elk IT-landschap van elke organisatie groeit elke dag en we kunnen niet blijven inhuren in hetzelfde tempo waarin deze landschappen groeien; dat is gewoonweg onmogelijk. Dus toen de manager om een `architectuurman' vroeg, probeerde hij alleen maar brandjes te blussen. Hij was niet bezig met het oplossen van de hoofdoorzaak van het probleem.

Het kernprobleem ligt niet in het gebrek aan resources, maar in de fundamentele benadering van projectmanagement en de toewijzing van middelen. Door voortdurend resources in te huren zonder de onderliggende problemen aan te pakken, passen organisaties slechts tijdelijke oplossingen toe voor diepere, systematische problemen. Hier zijn enkele specifieke problemen met deze aanpak:

- Verkeerde afstemming van vaardigheden en eisen: wanneer een manager haastig om een security-architect vraagt, doet zij/hij dit vaak zonder een grondig begrip van de specifieke vaardigheden en expertise die nodig zijn. Dit leidt tot een mismatch tussen de capaciteiten van de ingehuurde persoon en de werkelijke vereisten van het project. Het resultaat is suboptimale prestaties en verdere vertragingen omdat de nieuwe medewerker moeite heeft om zich aan te passen aan vage of ongedefinieerde projectscopes.
- Gebrek aan langetermijnstrategie: voortdurend moeten vertrouwen op externe aanwervingen voor onmiddellijke projectbehoeften wijst op een gebrek aan strategische

planning. Organisaties moeten langetermijnstrategieën ontwikkelen voor de werving en ontwikkeling van talent en ervoor zorgen dat ze de juiste mix van vaardigheden in huis hebben om lopende en toekomstige uitdagingen aan te gaan. Dit omvat het identificeren van belangrijke vaardigheidstekorten, het investeren in de opleiding van werknemers en het creëren van een pijplijn van talent dat klaar staat om in te springen als dat nodig is.

- Integratie: Externe medewerkers ondervinden vaak problemen bij de integratie met bestaande teams. Het kan zijn dat ze de contextuele kennis van de infrastructuur en processen van de organisatie missen, wat leidt tot inefficiënties en miscommunicatie. Effectieve integratie vereist een gestructureerd onboarding proces en voortdurende ondersteuning om ervoor te zorgen dat externe resources naadloos kunnen samenwerken met interne teams.
- Afhankelijkheid van resources: Een te grote afhankelijkheid van resources kan een afhankelijkheid creëren die zowel kostbaar als onhoudbaar is. Interne teams zullen minder verantwoordelijkheid nemen in de aanwezigheid van externen ervan uitgaande dat die de verantwoordelijkheid nemen. Dit belemmert de ontwikkeling van interne capaciteiten, waardoor de organisatie kwetsbaar blijft wanneer externe hulp niet beschikbaar is. Het opbouwen van een robuust intern team met de nodige vaardigheden en expertise is cruciaal voor succes en veerkracht op de lange termijn.

Mogelijke oplossingen

Om de problemen aan te pakken is een proactieve houding nodig. Dit betekent een fundamentele verandering in de manier waarop we met ons resources omgaan en projecten aanpakken, hoe talent wordt gezocht en ontwikkeld en hoe teams samenwerken.

Een van de belangrijkste stappen is om af te stappen van ad-hoc inhuur. In plaats van naarstig op zoek te gaan naar inhuur als een project al loopt of vertraging heeft opgelopen, moet je kiezen voor een meer systematische, holistische aanpak. Door ruim van tevoren te anticiperen op projectbehoeften, kun je de juiste resources planmatig inzetten en ervoor zorgen dat alle benodigde vaardigheden op het juiste moment beschikbaar zijn. Dit zorgt voor een soepele projectuitvoering, vermindert de afhankelijkheid van externe inhuur op het laatste moment en is veel kostenefficiënter.

Tot slot kun je strategische partnerschappen aangaan. Zoals het gezegde luidt: een schaap met vijf poten bestaat niet; je kunt niet verwachten dat één persoon alles weet en kan. Dit is vooral relevant wanneer je met freelancers werkt, die als dé cyberexperts worden gezien, maar geen duizendpoten zijn. Freelancers moeten samenwerken met interne medewerkers, leveranciers of andere freelancers om een team te vormen voor de klant.

Ik (Vincent) werk nu bijvoorbeeld aan een project samen met een freelancer. Hij is een sterke communicator die graag naar kantoor gaat. Ik woon in Denemarken, dus voor mij is het lastig om dagelijks naar kantoor te gaan. Mijn kwaliteiten liggen in het behouden van structuur en het op schema houden van projecten. Daarnaast ben ik ervaren in het schrijven en vastleggen van strategie tot operatie. De combinatie van cybersecuritykennis en de communicatiekwaliteiten van mijn freelancer collega resulteert in een goed team en uitstekende end-to-end resultaten voor de klant. Het kan dus een goed idee zijn om strategische partnerschappen aan te gaan met freelancer-communities die gebaseerd zijn op samenwerking van professionals. Dit resulteert in een flexibele, schaalbare schil voor de benodigde extra resources; resulterende in kostenefficiëntie. Het bevorderen van een actieve gemeenschapsgeest, waarbij het duidelijk is dat collectieve inspanningen meer resultaat opleveren dan solo-inspanningen, zal output verhogend werken en zo de behoefte aan extra handen verminderen.

Conclusie

De vraag naar cybersecurityspecialisten groeit sneller dan dat er specialisten bijkomen. In de schaarse markt waarbinnen wij opereren zal de wijze waarop wij werken moeten veranderen. De vraag voor ons allen is dus: hoe zetten wij op schaalbare wijze de schaarse specialisten in? Hoe zetten wij hen in hun kracht, hoe bevorderen wij samenwerking? Samengevat: hoe voorkomen wij 'snijverlies'?

Onze conclusie luidt: transitie is vereist, de verandering ligt daarin dat in plaats van inhuur meer gewerkt wordt door aanbieding van hoogwaardige diensten en het realiseren van projecten op basis van gemeenschap. Op macrobasis constateren wij dat er een trend is naar individualisering; daartegenover staat het vertrek van talenten bij de grote vier en bij de MSSP's, welke talenten freelance gaan werken. Dus wij staan wellicht aan de vooravond van een freelancer-community, mits zij uitgaan van samenwerking!

Auteur: Michiel Herrebrugh is Security & privacy consultant bij MichielH Services. Michiel is te bereiken via: info@michielh.nl

Hoe invulling te geven aan de eisen vanuit DORA

Grip krijgen op leveranciersrisico's

Vanaf 17 januari 2025 moeten financiële instellingen aan DORA (Digital Operational Resilience Act) voldoen. Eén van de kernpunten van DORA is het grip krijgen en houden op de volledige uitbestedingsketen. Maar wat schrijft de wet voor en hoe geeft een kleine of middelgrote financiële instelling op een praktische manier invulling aan het managen van leveranciersrisico's?

DORA bestaat uit vijf pijlers, waarvan het beheer van ICT-risico van derde aanbieders er één is. Dit laat het belang van het managen van uitbestedingsrisico's zien. De specifieke eisen zijn vastgelegd in artikelen 28 t/m 30. Artikelen 31 t/m 44 bevatten de regels rondom het overzichtskader, maar die zijn op dit moment voor financiële instellingen minder relevant.

Om aan DORA te voldoen moet een instelling de wettekst naleven (de zogenaamde level 1-eisen). Er zijn echter voor verschillende onderwerpen verdiepende technische reguleringsnormen (level 2-eisen) waar ook aan voldaan moet worden. Deze level 2-eisen zijn op het moment van schrijven nog niet goedgekeurd door de Europese Commissie, maar de (Engelstalige) conceptversies zijn wel al gepubliceerd. Op het gebied van leveranciersrisico's zijn dit:

- RTS (regulatory technical standard): Policy on ICT services performed by third parties
- ITS (implementing technical standard): Templates for the register of information
- RTS: Elements when sub-contracting critical or important functions en
- RTS: Information on oversight conduct.

Hoe invulling wordt gegeven aan de eisen vanuit DORA verschilt per toezichthouder. De Autoriteit Financiële Markten heeft in 2019 'Principes voor Informatiebeveiliging' gepubliceerd, maar deze principes zijn dusdanig generiek dat ze weinig handvatten bieden voor de implementatie van DORA. Nuttiger is de 'Good Practice Informatiebeveiliging' van De Nederlandsche Bank (DNB). In deze Good Practice staan redelijk gedetailleerde eisen waarmee aangetoond kan worden dat informatiebeveiliging op een goede manier is ingericht. Door te voldoen aan de versie uit 2023 wordt tegemoetgekomen aan een groot gedeelte van de level 1-eisen vanuit DORA.

Implementatie van de DORA-eisen

Om invulling te geven aan de eisen vanuit DORA/de Good Practice van DNB, moeten in elk geval de punten uit de onderstaande afbeelding geïmplementeerd zijn. Dit is echter geen uitputtende lijst: vanuit andere wetgeving, normenkaders of bedrijfseisen kunnen additionele activiteiten nodig zijn, zoals het uitvoeren van een Data Protection Impact Assessment (DPIA) of het aanmelden van een (ICT-)uitbesteding bij de toezichthouder.

1. Uitbestedingsbeleid

Elke financiële instelling moet een uitbestedingsbeleid – oftewel een strategie inzake ICT-risico van derde aanbieders hebben. Hierin staan de beleidsregels voor het uitbesteden van ICT-diensten. Ook moet het algemene risicoprofiel van deze ICT-diensten beoordeeld worden. Om aantoonbaar te voldoen aan de gestelde eisen, is het belangrijk om het gehele proces rondom uitbesteding te beschrijven: wat zijn de stappen die genomen moeten worden bij welk type leverancier. Dit kan onderdeel zijn van het uitbestedingsbeleid, maar kan ook in een aparte procesbeschrijving staan.

2. BIA/BIV-classificatie

Binnen de organisatie is het van belang dat er duidelijkheid is

over hoe kritisch welke bedrijfsprocessen zijn. Met een business impact analyse (BIA) of materialiteitsassessment wordt dit in kaart gebracht. Voor leveranciersmanagement is dit van belang, omdat er onderscheid gemaakt wordt tussen ICT-diensten ter ondersteuning van kritieke of belangrijke functies (hierna: kritieke ICT-diensten) en alle andere ICT-diensten (zie kader).

De BIA is ook nodig om te bepalen wat de BIV-classificatie van het systeem is of gaat worden: hoe belangrijk zijn de beschikbaarheid, integriteit en vertrouwelijkheid van het systeem en de data? Deze BIV-classificatie is nodig om in de volgende stap de securityvereisten op te stellen.

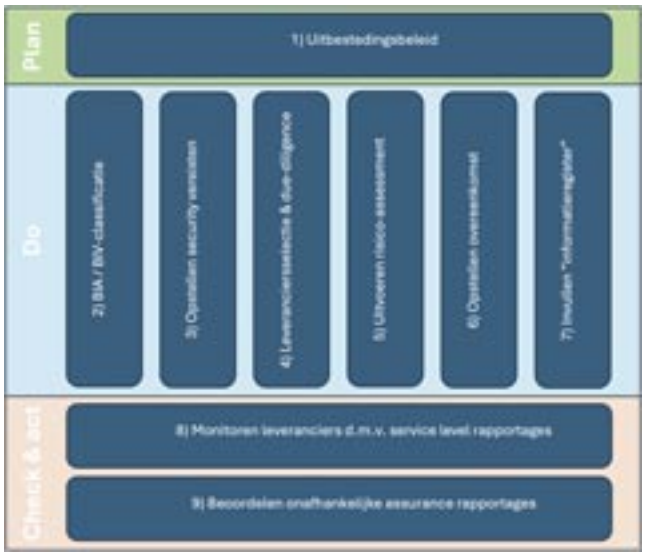
Wat zijn kritieke of belangrijke functies?
De definitie binnen DORA (artikel 2) omschrijft dit als 'een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten.'

3. Opstellen securityvereisten

Het is belangrijk om passende securitymaatregelen te implementeren: niet te veel, maar ook niet te weinig. Om te voorkomen dat bij elke uitbesteding ad hoc bepaald wordt welke securityrequirements van toepassing zijn, helpt het hebben van een vooraf gedefinieerde maatregelenset. Hierbij kunnen de maatregelen gedifferentieerd worden naar BIV-classificatie, zoals in tabel 2 is weergegeven. De BIV-classificatie bepaalt uiteindelijk welke beheersmaatregelen contractueel afgesproken worden met de leverancier, zodat de maatregelen passen bij het risicoprofiel van de uitbestede dienst.

4. Leverancierselectie & due diligence

Wanneer de (security)requirements duidelijk zijn, kan gezocht worden naar een geschikte leverancier. DORA schrijft niet voor hoe de meest geschikte leverancier geselecteerd moet worden, maar er wordt wel van de financiële instelling verwacht dat er passend (due diligence)onderzoek gedaan wordt. Ook moet



Figuur 1: DORA verplichtingen leveranciersmanagement.

beoordeeld worden of aan de toezichtvoorwaarden voor het sluiten van het contract is voldaan en of er eventueel belangenconflict kan voortkomen uit de overeenkomst.

5. Uitvoeren risico-assessment

De wetgever stelt specifieke eisen aan het uitvoeren van een risico-assessment voorafgaand aan het uitbesteden van ICT-diensten. Alle relevante risico's met betrekking tot de overeenkomst moeten in kaart gebracht worden, waarbij in het geval van kritieke ICT-diensten tenminste een aantal specifieke risico's moeten terugkomen:

- Concentratierisico: in hoeverre is de leverancier vervangbaar; en ontstaat er geen kritische afhankelijkheid door te veel diensten bij dezelfde leverancier af te nemen?
- Onderuitbesteding: wat betekent het voor de instelling als de dienstverlener bepaalde ICT-diensten verder uitbesteedt, met name naar onderaannemers in het buitenland? Wat is de impact van potentieel lange of complexe uitbestedingsketens op het vermogen van de financiële instelling om de contractuele afspraken te monitoren?
- Insolventie & faillissement: wat is het risico als een ICT-dienstverlener niet meer aan zijn financiële verplichtingen kan voldoen en kan de instelling dan nog zijn gegevens herstellen?
- Privacy: worden de Europese privacyregels nageleefd bij uitbesteding naar het buitenland?

Om de risico's te kunnen mitigeren, moeten potentiële leveranciers hun volledige onderuitbestedingsketen inzichtelijk maken,

Hoe geeft een kleine of middelgrote financiële instelling invulling aan het managen van leveranciersrisico's?

Beschikbaarheid	**Laag**	**Midden**	**Hoog**
- Beschikbaarheidspercentage	80%	90%	99,9%
- Uitwijkbaarheid	N.v.t.	Cold standby	Hot standby
- Uitwijktesten	Geen	Tweejaarlijks	Jaarlijks
Vertrouwelijkheid	**Laag**	**Midden**	**Hoog**
- Encryptie	Encryption in transit	Encryption in transit + rest	Encryption in transit + rest
- Authenticatie	Username + password	Username + password	MFA
- Authenticatie beheerders	Username + password	MFA	MFA

Tabel 1: Voorbeeld beveiligingsmaatregelen per classificatieniveau voor beschikbaarheid en vertrouwelijkheid.

inclusief de wijze waarop zij de relevante risico's beheersen die aanwezig zijn bij die onderleveranciers.

Na het bepalen van de risico's kunnen mitigerende maatregelen bepaald en afgesproken worden. Ook kan blijken dat de uitbesteding toch niet door mag gaan, omdat het een onacceptabel risico oplevert voor de instelling.

6. Opstellen overeenkomst

Wanneer duidelijk is of een ICT-dienst een kritieke of belangrijke functie ondersteunt, de BIV-classificatie en bijbehorende beheersmaatregelen duidelijk zijn, de leverancier is geselecteerd en de gedefinieerde risico's beheersbaar zijn, kan overgegaan worden tot het opstellen van de overeenkomst. DORA stelt expliciete eisen aan deze overeenkomst: er wordt een negental punten beschreven die in elke uitbestedingsovereenkomst van ICT-diensten moeten terugkomen. Daarnaast zijn er zes verplichtingen voor contracten met leveranciers van kritieke ICT-diensten.

Twee punten die het benadrukken waard zijn: (1) het hebben van een exitstrategie en (2) het uitvoeren van threat led penetration testing.

1) Een financiële instelling moet een redelijke mate van zekerheid hebben dat het beëindigen van een overeenkomst kan gebeuren zonder dat dit leidt tot een verstoring van de bedrijfsactiviteiten of de dienstverlening naar klanten. Hiervoor moet een exitstrategie zijn beschreven in de afspraken met de leverancier en moet deze periodiek geëvalueerd worden.
2) Threat led penetration testing, of dreigingsgestuurde penetratietest, gaat verder dan normale penetratietesten. Hierbij worden realistische aanvalsscenario's van bestaande actoren nagebootst, waarbij de test zich niet beperkt tot één specifiek systeem. Artikelen 26 en 27 beschrijven de eisen rondom deze testen.

7. Invullen informatieregister

Elke financiële instelling is verplicht om een informatieregister te hebben met daarin informatie over alle contractuele overeenkomsten rondom uitbestede ICT-diensten en de ICT-leveran-

Eisen voor elke overeenkomst rondom uitbestede ICT-diensten	Aanvullende eisen aan contracten met leveranciers van kritieke ICT-diensten
1. Beschrijving van alle te leveren functies en diensten, inclusief eisen en voorwaarden aan onderuitbesteding van een kritieke ICT-dienst 2. De locatie waar de diensten moeten worden geleverd en waar de gegevens moeten worden verwerkt. De financiële instelling moet geïnformeerd worden voorafgaand aan het veranderen van de locatie 3. Beveiligingsbepalingen rondom de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid 4. Afspraken over de toegang tot, het herstel van en de teruggave van data in het geval de overeenkomst -om wat voor reden dan ook- wordt beëindigd (inclusief bij insolventie/faillissement) 5. Beschrijvingen van het dienstenniveau 6. De verplichting dat de ICT-dienstverlener bij een incident kosteloos, of tegen een vooraf bepaalde prijs, bijstand verleent 7. De verplichting dat de ICT-dienstverlener volledige medewerking verleent aan de toezichthouder(s) van de financiële entiteit 8. Het recht om een dienst te beëindigen en de bijbehorende minimumopzegtermijn 9. Afspraken over deelname aan bewustwordingsactiviteiten van de financiële instelling door medewerkers van de ICT-dienstverlener (waar relevant)	a. Nauwkeurige kwantitatieve en kwalitatieve prestatiecriteria, zodat de financiële instelling monitoringsactiviteiten kan uitvoeren (ter aanvulling op punt 5) b. De verplichting van de ICT-leverancier om de financiële instelling te informeren over ontwikkelingen die impact kunnen hebben op de naleving van de Service Level Agreements c. De verplichting van de ICT-leverancier om bedrijfscontinuïteitsplannen te hebben en te testen; en om beveiligingsmaatregelen te hebben geïmplementeerd die passend zijn d. De verplichting van de ICT-leverancier om deel te nemen aan threat led penetration testing (TLPT) e. Het recht om de prestaties van de ICT-leverancier te monitoren, inclusief: i. Het recht op onbeperkte toegang, inspectie en audit door zowel de financiële instelling als de toezichthouder, inclusief het recht om ter plaatse kopieën te maken van relevante documentatie en de plicht van de ICT-dienstverlener om daaraan mee te werken ii. Het recht om andere garantieniveaus af te spreken indien de rechten van andere klanten worden aangetast iii. De verplichting voor de ICT-dienstverlener om gedetailleerde informatie te verstrekken over waar, hoe en hoe vaak de audits plaatsvinden f. Er moet een exitstrategie afgesproken zijn

Tabel 2: DORA eisen aan contracten.

ciers. Dit register moet voldoen aan de eisen zoals beschreven in de ITS Templates for the register of information. Er is een Excel-template beschikbaar gesteld die gebruikt kan worden voor het informatieregister (1).

In het template valt op dat er relatief veel informatie gevraagd wordt, zeker voor een kleine of middelgrote financiële instelling. Het document correct invullen is echter van belang, omdat het register opgevraagd mag worden (en naar verwachting zál worden) door de toezichthouder. Het template helpt daarnaast om invulling te geven aan alle level-2 eisen die gesteld worden vanuit de bovengenoemde ITS.

8. Monitoren d.m.v. service level rapportages

Zoals onder punt 6 beschreven staat, moeten er in contracten afspraken gemaakt worden over service levels (eis 5) en moeten er – in geval van kritieke ICT-diensten – kwalitatieve en kwantitatieve prestatiecriteria worden opgesteld (eis a). Het is van belang om deze prestatiecriteria breder te formuleren dan enkel de beschikbaarheidseisen en operationele reactietijden bij incidenten en problemen: specifiek op het vlak van informatiebeveiliging en cyberweerbaarheid kunnen prestatiecriteria over analyse en reactietijden op Indicators of Attack of Indicators of Compromise bijdragen aan het vaststellen of een leverancier de benodigde volwassenheid heeft.
De financiële instelling moet – mede door middel van service

level rapportages – grip houden op de dienstverlening door de leverancier van kritieke ICT-diensten. Daarnaast helpt het periodiek overleggen met leveranciers om het vermogen om effectief samen te werken regelmatig te evalueren en een goede relatie op te bouwen: deze relatie is misschien wel het belangrijkste middel om risico's te mitigeren.
De rapportages moeten worden geanalyseerd en over de uitkomsten hiervan moet worden gerapporteerd aan het verantwoordelijke lijnmanagement. Op deze manier houdt de financiële instelling toezicht op (de betrouwbaarheid van) de volledige uitbestedingsketen van kritieke ICT-diensten.

9. Beoordelen onafhankelijke assurancerapportages

Elke financiële instelling is verantwoordelijk voor het voldoen aan de eisen vanuit DORA, ook wanneer ICT-diensten uitbesteed worden. Daarbij is het niet voldoende om te vertrouwen op beloftes van een leverancier: naleving van de eisen moet aantoonbaar zijn. De meest gebruikelijke en efficiënte manier om dit te doen is door onafhankelijke assurancerapportages op te vragen bij de leverancier en deze te beoordelen. Hierbij is een ISO 27001 certificering niet voldoende: er moet aangetoond worden dat beveiligingsmaatregelen effectief werken over een langere periode, bijvoorbeeld door middel van een ISAE 3402 type 2 of een SOC-2 type 2 verklaring. Deze vereiste geldt ook voor onderleveranciers.
Bij het beoordelen van een assuranceverklaring zijn twee aandachtspunten van belang:

1. Zijn alle subcontractors in scope van de verklaring?
Vaak worden onderleveranciers niet meegenomen bij de uitspraken over effectieve beheersmaatregelen (carve-out). Aangezien elke financiële instelling de gehele uitbestedingsketen moet monitoren, is het – als onderleveranciers niet in scope zijn – nodig om assuranceverklaringen bij de onderleveranciers op te vragen en te beoordelen. Het is dus effectiever om met een ICT-leverancier af te spreken dat ook de onderleveranciers meegenomen worden in de rapportage.

2. Zijn alle relevante beveiligingsmaatregelen in scope van de verklaring?
Niet elke assuranceverklaring heeft dezelfde scope. Een financiële instelling moet de zekerheid hebben dat alle relevante beveiligingsmaatregelen getest en effectief bevonden zijn. Welke beveiligingsmaatregelen relevant zijn, kan verschillen per type leverancier (zie onderstaande tabel). Door hier van tevoren over na te denken, kunnen vergelijkbare ICT-leveranciers op een vergelijkbare manier beoordeeld worden. Het is aan te bevelen om ruimte te houden om, wanneer nodig, af te wijken van de standaardmapping, waarbij afwijkingen naar een lager niveau wel eerst voorgelegd moeten worden aan een (C)ISO of tweedelijns riskfunctionaris.

	SaaS leverancier	Data-center	Software-ontwikkelaar
Screening (DNB 08.4)	X	X	X
Secure coding (DNB 10.1)	X	-	X
Uitwijktesten (DNB 11.2)	X	X	-
Fysieke beveiliging (DNB 21.1 & 21.2)	-	X	-

Tabel 3: Voorbeeld mapping DNB normen - type leverancier.

Vervolgens kan voor elk van de relevante maatregelen vastgesteld worden of de assuranceverklaring een uitspraak doet over de effectiviteit van de maatregel. Leg deze beoordeling, inclusief eventuele afwijkingen/uitzonderingen en verbeteracties, vast om aan te tonen dat de financiële instelling invulling geeft aan deze wettelijke verplichting.

Naderende deadline

Vanaf 17 januari 2025 moet elke financiële instelling voldoen aan DORA. Wacht dus niet te lang met de implementatie van de vereisten. Dit artikel draagt er hopelijk aan bij om duidelijk te krijgen wat gedaan moet worden om aan artikelen 28 t/m 30 van DORA te voldoen. De wetgeving is echter breder dan alleen die artikelen en dusdanig uitgebreid en specifiek dat het onmogelijk is om alle verplichtingen in één artikel te beschrijven. Neem dus ook de tijd om zelf de wetgeving en de onderliggende technische reguleringsnormen erop na te slaan om goed in kaart te brengen wat er moet gebeuren om aan deze nieuwe wetgeving te voldoen.

Referentie

(1) https://www.eiopa.europa.eu/publications/set-rules-under-dora-ict-and-third-party-risk-management-and-incident-classification_en

COLUMN NICOLE

Op de cybercrime-catwalk zien wij vooral vintage

Ik begin deze column graag met een bekentenis: ik ben een beetje hypocriet. In mijn vorige column betoogde ik dat we meer vooruit moesten kijken, maar in deze column ga ik je vertellen dat we juist meer achteruit moeten kijken.

Sinds 2011 ben ik betrokken bij het schrijven van cybersecuritydreigingsbeelden. Deze zijn bedoeld om een strategisch overzicht te geven van dreigingen binnen het cybersecuritylandschap. Destijds was het pionieren, maar inmiddels worden organisaties overspoeld door dreigingsbeelden. Hierdoor is een strijd ontstaan om de aandacht van de lezer. De focus ligt doorgaans op veranderingen in de modus operandi van criminelen en andere kwaadwillenden. In het begin waren ze daarom erg waardevol om een indruk te geven van de soorten dreigingen waar organisaties en burgers mee geconfronteerd werden. De laatste jaren, waarin ik leiding gaf aan het Internet Organised Crime Threat Assessment (IOCTA) bij Europol, had ik het gevoel dat de meerwaarde van de dreigingsbeelden langzaam aan het verdwijnen was. Ik voelde een constante druk om nieuwe dreigingen te ontdekken, maar het beste wat ik kon vinden waren marginale veranderingen. Grote veranderingen, zoals het gebruik van double en triple extortion bij ransomware, waren eerder uitzondering dan regel. Terwijl ik dagelijks vanuit meerdere hoeken hoorde dat het dreigingenlandschap zo snel veranderde dat we het nauwelijks konden bijhouden, zag ik in de praktijk vooral meer van hetzelfde, in ieder geval op strategisch niveau.

Desondanks lijkt er een obsessie te zijn met het vinden van nieuwe dreigingen. We willen nieuwswaardig zijn. We willen niets liever dan vooruitkijken en op zoek gaan naar the next best thing, of beter gezegd: the next worst thing. Toen ik in 2019 ransomware opnieuw de grootste dreiging wilde noemen in het persbericht over de jaarlijkse IOCTA, droop de teleurstelling ervan af bij onze communicatieafdeling. Ransomware was out of fashion en niet geschikt voor de cybercrime catwalk. Voor criminelen is ransomware als een prachtige vintage Gucci jurk: oud, maar nog even stijlvol als altijd, en inmiddels veel meer waard dan tien jaar geleden. Dat is de reden dat we anno 2024 ransomware nog steeds niet onder controle hebben. Dus voordat we enthousiast op zoek gaan naar nieuwe dreigingen, zoals revolutionaire vormen van AI-geleide aanvallen, is het belangrijk dat we stilstaan en reflecteren. Wat hebben we geleerd van de afgelopen jaren?

In 2018 brachten we de vijfde editie van de IOCTA uit. Een uitstekend moment om achteruit te kijken. In plaats van nieuwe dreigingen zagen we in deze flashbacks vooral een doorontwikkeling van bestaande vormen van cybercrime, zoals crime as a service en ransomware. En dat is nog steeds het geval. Criminelen misbruiken GenAI vooral om hun bestaande methoden te verbeteren, te versnellen of op een andere manier te verbreden. Maar ik betwijfel of zij daadwerkelijk iets 'nieuws' gaan introduceren.

Laten we dus onze focus leggen op het begrijpen van de geschiedenis en het DNA van bestaande cyberdreigingen. Op die manier zijn we beter voorbereid op de toekomst. Het is tijd voor reflectie.

Dr. Nicole van der Meulen is expert op het gebied van cybersecurity en emerging technologies en werkzaam bij SURF als Cybersecurity Innovation Lead, ns.vandermeulen@gmail.com

Authors: Reinder Wolthuis, senior consultant/projectmanager at TNO. Marth Breure, innovation analyst at TNO Vector and Ruggero Montalto, projectmanager at TNO. Authors to be reached at reinder.wolthuis@tno.nl, marth.breure@tno.nl and ruggero.montalto@tno.nl

Security innovation and tech transfer

Security innovation is done by many organizations and is essential to protect society against advanced cyber-attacks. But these innovations are useless unless they are also applied in practice. The Dutch cybersecurity innovation community currently experiences a tech transfer gap, where innovation results don`t always find their way into actual products and services available on the market. This article assesses the prominent reasons why this gap exists and proposes potential solutions to reduce it.

The Partnership for Cybersecurity Innovation (PCSI, www.pcsi.nl) is a collaboration among TNO, ABN AMRO, ING, ASML, Achmea, and the Netherlands Tax Administration (Belastingdienst).

PCSI has the ambition to collaboratively innovate on cybersecurity by producing innovative technical, process, or methodological results. These innovation results are intended to improve the protection against cyber-attacks both for the PCSI partners and the Dutch community.

PCSI has been striving to produce results that will be used in practice by the PCSI Partners and the Dutch community after an innovation project has been finalised. This ambition could not be sufficiently fulfilled until now for several reasons. PCSI clearly experiences a 'tech-transfer gap' in between innovation and the actual adoption and use of the result.
The broader Dutch cybersecurity innovation community also experiences a tech transfer gap, where innovation results not always find their way into actual products and services on the market. One of the instruments that the Ministry of Economic Affairs and Climate Policy (EZK) has implemented to support this topic is dcypher, a collaboration platform for research and development on cybersecurity in the Netherlands (1).
Since EZK has a high interest in the success of tech-transfer of innovation results, they awarded a project to TNO to find potential solutions that could reduce the tech transfer gap for the PCSI as well as the Dutch cybersecurity innovation community.

A resulting report, specifically addressing the PCSI tech transfer, has been published earlier this year (2) and a more generic report on tech transfer for the Dutch cybersecurity innovation community will soon be published. Results have been gathered from literature, interviews with relevant stakeholders, and workshops.
The tech transfer gap is graphically represented in Figure 1, showing a combination of the Market Readiness Level and the Technology Readiness Level:

- TRL – the Technological Readiness Level scale measuring the maturity of a technology being developed by a project.
- MRL – the Market Readiness Level scale measuring the commercial readiness of a technology in respect to the market.

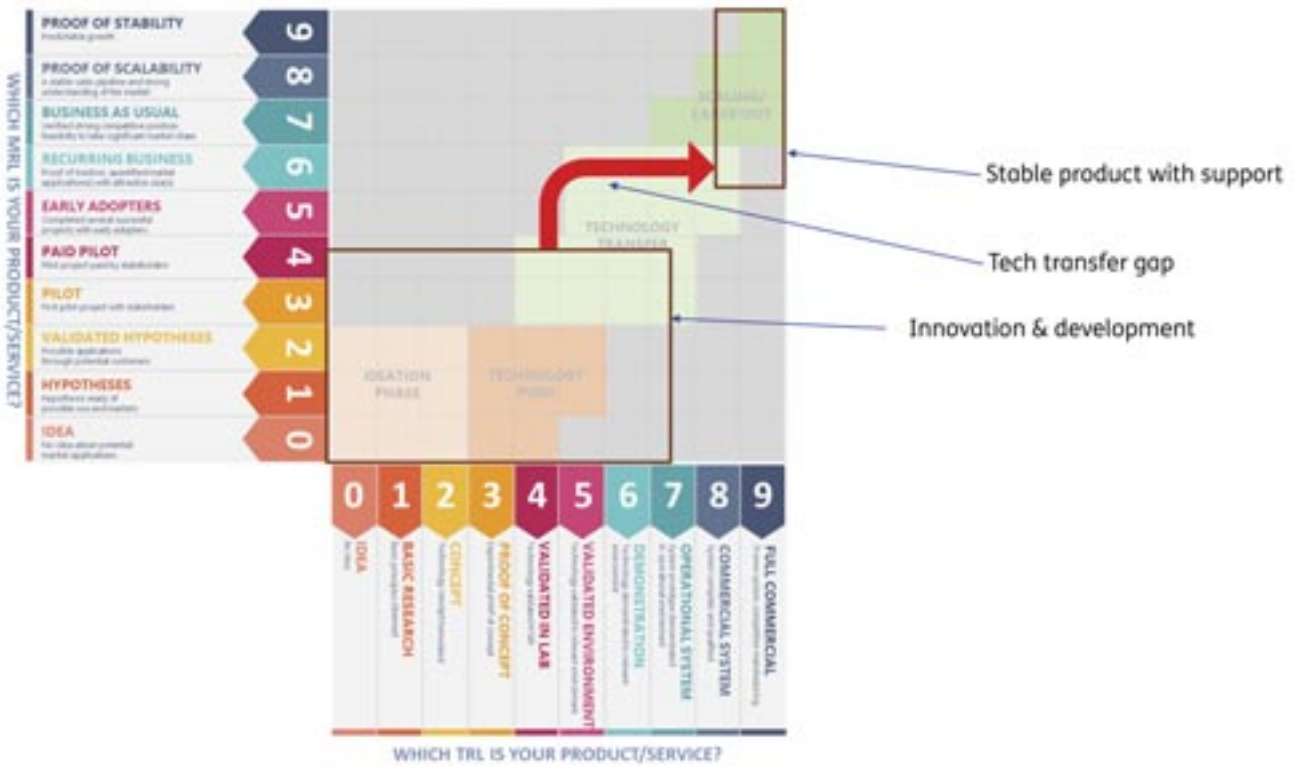


Figure 1: The tech transfer gap from the perspective of TRL and MRL level.

As Figure 1 shows, innovation projects usually produce results at TRL 6-7 and MRL 4. A product needs to be at TRL 9 and MRL 6-7 in order to be considered mature and suitable for the market. The tech transfer gap is the difference between these two stages for innovation projects. Ideally, this gap is not present, and a solution finds its way to market in an uninterrupted manner. But, more often than not, this is not the case.

Tech transfer barriers

One of the main findings from our research is that the maturity of the cybersecurity ecosystem in the Netherlands is relatively high. The Netherlands has a thriving educational cybersecurity environment and mature research and knowledge institutes (doing well on TRL levels lower than 5). The Netherlands also has an active government, mature investigation services, and a high number of companies that are active in the cybersecurity field. However, transforming good ideas and innovative results into products and services that can be used in practice remains to be a difficult journey. In particular, from the information gathered it seems that the number of Dutch start-ups with cybersecurity technologies or services is low compared to what one sees in other countries.This is due to the harshness of the entrepreneurial climate, Dutch culture, the inherent difficulty of the cybersecurity target market, regulatory and entry-level barriers, and a limited workforce with the right expertise.

Within the Dutch market, large end users of cybersecurity solutions tend to focus on large suppliers with proven track record and product suites that offer a multitude of functionalities. They prefer to buy off the shelf systems. Although understandable from a supplier management perspective, this hinders the introduction of small start-ups that often focus on a specific technology and are not stable companies yet. The lagging demand for Dutch alternatives for these global products also means that the knowledge, IP and technology is bought, instead of developed.

The lagging demand can also be accounted to the smaller size of the Dutch national market for cybersecurity products compared to the demand in market of other countries. This

When users know their needs and can articulate them to entrepreneurs, better cooperation and better fit products arise

smaller demand than neighbouring countries such as France, the Baltic countries, the U.K. and Israel, is in part to be explained by the lower impending sense of danger or of lack of threat experienced by an imminent cyber-attack of a foreign actor. This also explains why the US and Israel have such large demands for cybersecurity.

Culturally, the Dutch prefer avoiding investing in the development of long-term, disruptive and innovative cybersecurity solutions due to the high risk and delayed ROI associated with long term R&D. The lack of funding and market opportunities leads Dutch entrepreneurs to sell their innovative cybersecurity start-ups to foreign buyers (often American or Israeli) or even avoid investing in innovative cybersecurity to begin with. This means that the acquired IP and knowledge, also leaves the country. Entrepreneurs seem to work from a short-term ROI perspective instead of a long-term Cybersecurity self-sufficiency vision.

Competition in commercial bids is also a barrier for the tech transfer of innovative cybersecurity products: Requests for Proposal (RFPs) focus on competition and do not facilitate cooperation and demand articulation. When users know their needs and can articulate them to entrepreneurs, better cooperation and better fit products arise. Moreover, Venture capital investors on one hand are usually interested in products with their own intellectual property rights, and therefore prefer funding technology focused cybersecurity companies. The Dutch market on the other hand is mostly interested in service oriented cybersecurity companies.
Another aspect is that cybersecurity products are usually not mass-market products. But the lesser customization a cybersecurity product requires, the higher the potential ROI will be and consequently the chances to attract potential investors will be higher.

Also, EU laws and regulations (e.g., the requirement of GDPR compliance) complicates market introduction, especially when components are included that come from outside the EU.
Finally, start-up technology often needs to integrate or collaborate with tools and technology already prevalent in the market. This integration usually takes considerable effort that could slow down the actual implementation of innovative cybersecurity solutions.

The barriers experienced in the Netherlands are in line with what we find in literature: the lack of entrepreneurial competency and attitude within academia has been frequently highlighted (7,8), as has the need for better market research and increased connection with the market (3). Another factor described in literature is the lack of long term substantial financial support while the return on investment on innovative cybersecurity products is insecure (5). This is exacerbated by the extended development and resource requirements (11), and the high degree of uncertainty and risk associated with high-tech innovation (6, 10, 11).

Potential solutions

Although most solutions to solve the tech transfer gap in the literature are often difficult to turn into realistic business cases, there are some easy steps suggested in literature; optimizing the support and trainings from the technology transfer office and to add an experienced business coach to mentor the spin-off (5). Another suggestion is involving non-academic business colle-

By separating the activities, the disconnect between academia and entrepreneurs can be avoided

agues with previous experience in the industry (4) and strong work ethic/motivation in the core team as a surrogate entrepreneurial from an early phase onwards (9). Finally, extra emphasis is put upon the necessity of a ROI analysis (10, 11).

Aligning academic and industry goals in a common language while understanding the sector differences is not easy. Not all academics and entrepreneurs are able to switch ways of working so immediate. Recent literature on high-tech transfer suggests splitting the activities in two (3); a technology-focused development stage under the lead of academia and an application-oriented stage headed by entrepreneurs. By separating the activities, the disconnect between academia and entrepreneurs can be avoided. Academics are highly skilled in the development stage and technical proficiency, but they often lack the skills necessary for successful technology commercialization in the application stage, such as entrepreneurial capabilities, familiarity with industrial use-cases, and access to venture capital. With the separation, the tech-transfer can be improved by letting the researchers focus on the technology and transferring the final development steps and commercialization paths not only through spin-offs, but primarily through licensing to existing or newly founded companies.

From the interviews we learned that headway in the desired direction (decreasing the tech transfer gap) can be made by stimulating the entrepreneurial climate in the Netherlands. This would require:

- A clear vision of the demand articulation of the market, supported by economic anchors (large companies that can strengthen an entire ecosystem, e.g., the semiconductor industry around ASML) that change and support the entire landscape with their demand.
- More availability of risk capital on the market, which requires a change of mind set on investors and tax support measures. Strategically engaging investors should be brought in when there is a functioning TRL 6 prototype.
- Support by the Dutch government with advice (e.g. availability of tech transfer coaches), (pre-) competitive finding, positive investment climate, guidelines to stimulate the market.
- Willingness of end users (both government and private companies) to buy and use products from start-ups.
- A preference to buy products from EU start-ups by (EU) governmental agencies.
- Sufficient availability of security expertise (by education and/or attracting expertise from abroad).
- Less regulatory pressure for start-ups and entrepreneurs.

Also, more innovation collaborations should be set-up, such as the PCSI. E.g. a PCSI like collaboration on Operational Technology or product security. Collaboratively, the scale of work, available knowledge and resources can be used more efficiently and barriers can be overcome more effectively.

For start-ups, the availability of unbiased and high quality information and knowledge is important but not always easy to obtain. Easy access to e.g. knowledge institutes, academia, and relevant databases should be arranged for start-ups.

Establishing a (virtual) demonstration platform for products could streamline the tech-transfer process, serving as a repository for innovation and a "shopping window" for interested commercial parties (whether those may be potential investors, security vendors or end-users).

To be maximally effective, practical solutions to the tech transfer gap problem should have a systemic approach; for instance, it is advisable to have tech transfer 'in mind' from the beginning when researching or working on cybersecurity innovation at a low/medium TRL. In practice, that means having a solid knowledge of the current cybersecurity market, as well as a properly outlined mapping of the relevant key-stakeholders. These include (but are not limited to) end-users (both people using the product and people responsible for purchasing a product), investors, open-source projects and communities, government representatives, but also marketers, legal- and innovation experts. Investors are more ready to invest in an idea for a new innovative product that really solves a problem of an end-user instead of a pure technology driven product.

With respect to commercial bids, it would help if end-users both in the private sector and the public sector start tenders with a Request for Information (RFI) instead of a RFP, lowering the focus on competition and facilitating cooperation and demand articulation instead.

Finally, since the take-over by non-EU organizations of successful Dutch companies (some of which are funded with subsidies) is a real challenge, leveraging the new Veiligheidstoets investeringen, fusies en overnames (VIFO) regulations could improve the rate of retention of Dutch start-ups. The VIFO can in fact prevent the foreign acquisition of a company when the product or services the company sells are important for the strategic autonomy and the economic security of the Netherlands.

The solutions described above all focus on commercially driven tech transfer. But security tech transfer could also profit from Open Source models, which are in essence not commercially driven. This will facilitate collaboration and exchange of knowledge.

References

(1) Dcypher website

(2) PCSI tech-transfer, Improving the applicability of PCSI innovation results, Reinder Wolthuis, Marth Breure, Ruggero Montalto, 2024

(3) From Building Block to Application: A Deep Tech Commercialization Framework, Halecker and Dotzel, 2023. www.proquest.com/docview/2840810979?pq-origsite=gscholar&fromopenview=true

(4) Accelerating a Technology Commercialization; with a Discussion on the Relation between Technology Transfer Eciency and Open Innovation, Wahyudi Sutopo, Rina Wiji Astuti and Retno Tanding Suryandari, 2019. Journal of Open Innovation. www.mdpi.com/2199-8531/5/4/95

(5) Spin-Off Strategy and Technology Transfer Office: Cases in Sweden, S. Adesola, S. Datta, 2020. doi.org/10.1007/978-3-030-48013-4

(6) Development of a Life Cycle Model for Deep Tech Startups, G. Schuh, B. Studerus, and C. Hämmerle, 2022. Journal of Production Systems and Logistics, Volume 2 article 5 d-nb.info/1253580243/34

(7) Firms' Genetic Characteristics and Competence-Enlarging Strategies: A Comparison between Academic and Non-Academic High-Tech Start-Ups. Colombo, Massimo G., and Evila Piva, 2012. Research Policy, Volume 41, Issue 1 Elsevier. www.sciencedirect.com/science/article/pii/S0048733311001673

(8) Academic Networks in a Trichotomous Categorization of University Spinouts, Nicolaou, N. and S. Birley, 2003. Journal of Business Venturing 18, 333–359 www.sciencedirect.com/science/article/pii/S0883902602001180

(9) Bridging the Bubbles: Connecting Academia and Industry in Cybersecurity Research Rasha Kashef et al, 2023. Presented during the Rogers Cybersecure Catalyst webinar series in November 2022. rshare.library.torontomu.ca/articles/preprint/Bridging_the_Bubbles_Connecting_Academia_and_Industry_in_Cybersecurity_Research/24132645

(10) The DeepTech Investment Paradox: a call to redesign the investor model. Portincaso, M. Gourevitch, A., de la Tour, A., Salzgeber, T. and Hammoud, T., 2021. Boston Consulting Group & Hello Tomorrow

(11) Context perspective on University-Industry Collaboration processes: A systematic review of literature. Nsanzumuhire, S.U. and Groot, W., 2020. Journal of Cleaner Production, 258, p. 120861. doi.org/10.1016/j.jclepro.2020.120861

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over 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 kun je sturen naar ibmagazine@pvib.nl.

De Digital Decade

Is iets nog nieuws als in 2021 de eerste berichten al verschenen? Wij denken van wel, omdat het erop lijkt dat we ons nu, in 2024, pas ten volle beseffen wat er op ons afkomt en zien wat de plannen van toen betekenen voor onze organisaties. De wetgeving uit Europa vliegt ons om de oren, allemaal volgens een uitgedacht plan van de Europese Commissie. Zij presenteerden al in 2020 (1) de Europese datastrategie voor het vormgeven van de digitale toekomst van Europa. Daaruit volgde een stappenplan en 'wetgevingstrein' (2) die invulling geeft en moet gaan geven aan de stevige ambities van de EU op het gebied van digitale soevereiniteit, digitale vaardigheden, infrastructuur, innovatie, data, kunstmatige intelligentie, en cyberveiligheid. De Rijksoverheid reageerde daar al in 2021 op richting de Kamer (3), waar het toenmalige kabinet liet zien de urgentie te erkennen. De wetgevingstrein is inmiddels volop gaan rijden en de ene wet na de andere wet vliegt ons om de oren. NIS2, DORA, AI Act, gigabitinfrastructuur en er volgt nog meer. Een blik van onze redacteuren op de Digital Decade.


Fook Hwa Tan


Leo van Koppen

Fook Hwa Tan - Intrinsieke motivatie: de ware kracht achter de Digital Decade

Het is waar, de Digital Decade brengt een stortvloed aan wetgeving met zich mee, gestuurd door de Europese Commissie en ondersteund door nationale regeringen zoals die van Nederland. Deze regels en richtlijnen zijn onmiskenbaar belangrijk om een kader te bieden voor de digitale toekomst en om de veiligheid en privacy van individuen te waarborgen.

Maar laten we niet vergeten dat ware transformatie niet alleen van bovenaf komt, maar ook van binnenuit groeit. Intrinsieke motivatie, de innerlijke drive om te innoveren, te leren en te groeien, is de ware motor achter de Digital Decade. Het is de passie van individuen en organisaties die écht het verschil zal maken in het digitale landschap van de toekomst.

De Digital Decade biedt ons een ongekende kans om onze creativiteit, veerkracht en verbeeldingskracht te benutten. Het gaat niet alleen om het naleven van regels, maar ook om het omarmen van mogelijkheden. Laten we deze kans grijpen om te bouwen aan een toekomst die gedreven wordt door onze eigen intrinsieke motivatie, waar innovatie en vooruitgang hand in hand gaan met ethiek en verantwoordelijkheid.

Dus laten we niet alleen naar wetten en regelgeving kijken, maar laten we ook kijken naar de kracht binnenin ons, de wil om te groeien, te leren en te evolueren. Dat is wat ons echt zal leiden door deze Digital Decade en ons zal helpen om de digitale toekomst te vormen waar we allemaal van dromen.

Leo van Koppen - Europa moet, wij moeten

Op het moment van schrijven is Europa weer volledig in focus vanwege de Europese verkiezingen. Samenwerken levert meerwaarde op, ook in Europa. Het Verenigd Koninkrijk voelt nu de pijn van de Brexit en alle populistische partijen zijn daarvan geschrokken en hebben hun programma's bijgesteld. Er is helemaal geen sprake meer van een Nexit, Bexit of you-name-it-exit. De Europese samenwerking heeft ons allemaal verder gebracht, het is duidelijk: Europa moet!

Wat moet dan wel en wat kan dus echt niet is vervolgens de politieke discussie. Politieke thema's als Klimaat, Economie, Justitie, Cyber, ze zijn allemaal grensoverschrijdend en dat moet je dus in gezamenlijkheid regelen. Dat is dus ambtelijk opgepakt en verder uitgewerkt in programma's. Vervolgens gaat dat stroperige politieke proces van de Europese politiek daarmee aan de slag. Ik las afgelopen week een mooi artikel in De Correspondent waarin dat proces wordt uitgelegd. Het is me nu heel goed duidelijk geworden waarom dat proces zo verschrikkelijk stroperig is. In een volzin: heel veel vergaderen, lobbyen en politieke (koe)handel door Europese Raadsleden om een voorstel in elkaar te timmeren dat vervolgens door resp. de Europese Commissie of door de Ministers uit de verschillende landen zo weer teruggestuurd kan worden. Dat is, zo begrijp ik, de reden dat die Europese Richtlijnen zo lang op zich laten wachten. Vervolgens krijgen alle landen nog een paar jaar de tijd om ze om te zetten naar wetgeving die dan vervolgens over 'het volk' wordt uitgestort. Zie daar de lange doorlooptijden en moeizame uitwerking.

Maar vanuit ons vakgebied zien we allemaal de noodzaak dat er dingen moeten gebeuren om de cyberveiligheid te kunnen borgen. Risico's in de keten (Network and Information Systems Directive 2), kwaliteit van software (Verordening cyberweerbaarheid), Risico's bij AI-toepassingen (AI-verordening) het komt allemaal voorbij en ongetwijfeld ook op ons bordje. Maar het moet vanwege cyberveiligheid. Het geeft ons veel werk (dus business!) maar we zijn al met zo weinig mensen, hoe krijgen we het voor elkaar? Gaat dat dan allemaal wel lukken? Het zal wel moeten! Mijn vurige wens daarbij is wel dat de overheid niet alleen voorschrijft in de vorm van wetgeving, maar dat de overheid ook faciliteert. Dat instanties zoals NCSC, dCypher, TNO, e.a. de ondernemers ver(der) op weg helpt om deze wetgeving op een effectieve en efficiënte wijze in de praktijk te laten uitwerken. Dat zou het harde moeten aanzienlijk kunnen verzachten.

Referenties

(1) Digital decade policy programme - https://digital-strategy.ec.europa.eu/en/library/digital-decade-policy-programme-2030

(2) overzicht van doelstellingen Digital Decade - https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_nl

(3) Beoordeling door NL - https://www.rijksoverheid.nl/documenten/publicaties/2021/09/15/fiche-6-digital-decade

PvIB
Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

REDACTIE
Bianca Brooijmans
Alex Dingemanse
Marcel Feenstra
Maarten Hartsuijker
Fook Hwa Tan
Lilian Knippenberg
Leo van Koppen
Rachel Marbus
Chris de Vries

BLADMANAGEMENT
MOS bv
Caroline Knobbe
Sam Dekkers
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
Eric Noordam
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

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

ABONNEMENTEN
De abonnementsprijs in 2024 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

TSTC

ICT en Security Trainingen

Ransomware? Log4j?

ADVANCE YOUR CAREER WITH SECURITY IN 2024

AIGP - Certified AI Governance Professional
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v12
OSCP - Offensive Security PEN-200
BIO - Certified Bio Professional
NIS2 - NIS2 Lead Implementer

GET SKILLED
WWW.TSTC.NL

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

CEH - Certified Ethical Hacker
CHFI - Computer Hacking Forensic Investigator
CPENT - Certified Penetration Testing Professional
SSCP - Systems Security Certified Professional
OSCP - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

CISSP - Certified Information Systems Security Professional
CISM - Certified Information Security Manager
CISA - Certified Information Systems Auditor
CRISC - Certified In Risk And Information Systems Control
C|CISO - Certified Chief Information Security Officer

PRIVACY TRAININGEN

CIPP/E - Certified Information Privacy Professional / Europe
CIPM - Certified Information Privacy Manager
CIPT - Certified Information Privacy Technologist
CDPO - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

ISO 27001 - Foundation
ISO 27001 - Lead Implementer
ISO 27001 - Lead Auditor
ISO 27005 - Risk Manager
ISO 27701 - Privacy Management

www.tstc.nl

Onze trainingen zijn klassikaal of Live Online te volgen