INFORMATIEBEVEILIGING
MAGAZINE

Dossier:
Supply chain management in informatiebeveiliging

- Tussen regel en realiteit
  de groeiende uitdagingen van het cascade-cyberrisico
- Managing Supply Chain Cybersecurity Risk through Components Analysis
- Column: Encryptie is de oplossing, niet het probleem

JAARGANG 25 - 2025 - EDITIE 2

ISOPlanner

Eenvoudig Compliance Management in **Microsoft 365**

Waarom Microsoft 365?

Simpel: benut de kracht van Microsoft.

- Iedereen heeft Outlook en Teams. Naleving van compliance wordt als onderdeel van het werk ervaren.
- Vertrouwelijke gegevens zoals beleidsdocumenten en bewijsmateriaal blijven in jouw omgeving.
- Je lift vanzelf mee met innovaties. Bijvoorbeeld detectie van kwetsbaarheden en het automatisch ophalen van bewijs.

ISOPlanner is de enige integrale compliance oplossing in Microsoft 365. ISOPlanner brengt ISO naar jouw medewerkers toe en zorgt voor betere acceptatie en borging van informatiebeveiliging in jouw organisatie. Uiteraard ook voor de overheid (BIO), zorg (NEN7510) en de 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 2023 COMPLIANT

GDPR 2023 COMPLIANT

PENTEST 2023 SECURE

'To supply or not to supply, that's the question'

Chris de Vries

In deze uitgave bespreken we onder meer de leveranciersketen. Het artikel van hoogleraar Peter Roelofsma, Risk Management en Cybersecurity van de Haagse Hogeschool, gaat over cascade-cyberriskmanagement: *Tussen regel en realiteit*. Daarin komen toegepaste wetenschap en de operationele leveranciersketens samen.

Boeiend is de link tussen Dr. Jonathan Kwiks column over *Civiele sector in het vizier van de agressor* en het artikel *Cybercriminelen gaan publiek: jouw data, hun verhaal* van Marijke Stokkel en Eddie Versluis (BDO). Kwik, verbonden aan het Asser Institute, geeft een voorproefje van een aankomend stuk over oorlogsvoering met drones, AI en desinformatie. Stokkel en Versluis schetsen het dreigende scenario waarin cybercriminelen onze data gebruiken voor chantage – een ware thriller.

Fox Crypto's Ellen Wesselingh belicht het elimineren van de zwakste schakel binnen het leveranciersketenmanagement. Nick Nieuwenhuis bespreekt de integratie van cybersecurity en ondernemingsarchitectuur tot een effectief cyberriskmanagement. De redactie vertrouwt erop dat zij met al deze artikelen een complete tafel heeft opgedekt met voor ieders smaak wat. Gelardeerd met de gebruikelijke columns van onze onvolprezen columnisten.

Als laatste verwijs ik naar *Achter Het Nieuws* met betrekking tot de **S**pecial **I**nterest **G**roup (SIG) – **I**dentity and **A**ccess **M**anagement (IAM) die eind vorig jaar tot stand kwam. En een blik vooruit naar iB-Magazine 3, aan het einde van dit blad.

Tot slot: deze uitgave bevat Engelstalige content, maar als specialist in deze sector zal dat geen uitdaging zijn. Dus: *Enjoy the digestion processes presented in this magazine – until next time!*

Chris

IN DIT NUMMER

Auteur: Peter H.M.P. Roelofsma Full Professor Risk Management en Cybersecurity The Hague University of Applied Sciences

Tussen regel en realiteit

Cybersecurity is cruciaal voor het beschermen van infrastructuur, data en maatschappelijke systemen. Cyberrisico's, zoals datalekken en ransomware, kunnen grote schade veroorzaken. Een groeiende uitdaging is het cascade-cyberrisico, waarbij één incident een kettingreactie veroorzaakt binnen onderling verbonden systemen en organisaties.

Opmerkelijke voorbeelden van cascadecyberrisico's zijn waar te nemen in real world scenario's met wijdverbreide verstoringen veroorzaakt door ransomware-aanvallen zoals WannaCry en NotPetya, waarbij het falen van één systeem zich verspreidde over netwerken en industrieën. Dit leidde tot aanzienlijke economische en operationele schade. De SolarWinds-aanval, de Ledger-inbreuk en de Kaseya-ransomware-aanval zijn andere goede voorbeelden van dergelijke cascade-incidenten (Kruti et al., 2023; ENISA, 2023b; Oxford Analytica, 2021).

De toenemende digitalisering van activiteiten in sectoren zoals financiën, gezondheidszorg, defensie, energietransitie, stedelijke ontwikkeling en transport verergert het risicolandschap verder. Organisaties moeten de dynamische aard van deze risico's begrijpen om proactieve en effectieve cyberbeveiligingsstrategieën te ontwikkelen.

Sectie 1. Overzicht van dit document

In sectie 2 worden de tien gemeenschappelijke componenten van supplychain of cascadecyberrisico's geschetst. Sectie 3 legt de noodzaak uit van verhoogde maatschappelijke waakzaamheid met betrekking tot dit fenomeen. Sectie 4 bespreekt het 'Toren van Babel'-effect in Cascade Cyber Risk Management die een belangrijk achterliggend probleem vormt voor cascade cyber risicomanagement. Sectie 5 identificeert de vijf belangrijkste hiaten tussen regel en realiteit in cascadecyberrisicobeheer die verband houden met dit effect. Sectie 6 bespreekt de theoretische en computationele achtergrond voor het aanpakken van deze hiaten. Hierbij wordt de innovatieve AI-gebaseerde cascade-cyberrisicobeoordelingsmethode met behulp van computationele shared mental models beschreven. Sectie 7 beschrijft de methodologische benadering voor gegevensverzameling via het Cybersecurity Living Lab als de optimale uitwerking van deze aanpak. Sectie 8 schetst een narrative of change voor de toekomst van Cascade Cyber Risk Management die nodig is om de aanpak te laten slagen. Sectie 9 geeft de conclusie van dit document.

Sectie 2. Cascadecyberrisico's: componenten en implicaties

Cascadecyberrisico's verwijzen naar het domino-effect waarbij een cyberaanval op één systeem leidt tot daaropvolgende storingen in onderling verbonden systemen, met name in kritieke infrastructuur. Het Agentschap van de Europese Unie voor cyberbeveiliging ENISA (ENISA, 2023a) voorspelt dat cascade-aanvallen op de toeleveringsketen

Een groeiende uitdaging is het cascade-cyberrisico, waarbij één incident een kettingreactie veroorzaakt

in 2030 de belangrijkste cyberdreiging voor organisaties zullen worden. Recente literatuur identificeert tien belangrijke componenten van toeleveringsketen- of cascade-cyberrisico's, die elk bijdragen aan de potentiële ernst van dergelijke incidenten (Ghadge et al., 2019; Daniel et al., 2022; Paletti et al., 2021).

2.1 Onderling verbondenheid van systemen

Onderling verbonden systemen beïnvloeden elkaar, waarbij het falen van één component kan leiden tot het falen van andere. Deze onderlinge afhankelijkheid en interoperabiliteit creëert een netwerk van risico's dat snel kan escaleren. Naarmate systemen meer geïntegreerd raken, neemt de kans op systemische storingen toe.

2.2 Gedeelde kwetsbaarheden

Onderling verbonden systemen kunnen gemeenschappelijke kwetsbaarheden delen, wat betekent dat één enkele exploit meerdere systemen tegelijkertijd kan compromitteren. Het identificeren van gedeelde kwetsbaarheden is cruciaal voor organisaties om uitgebreide beveiligingsmaatregelen te implementeren.

2.3 Verschillende verspreidingsmechanismen

Risico's kunnen zich verspreiden via meerdere paden, waaronder gegevensstromen, gedeelde bronnen en services van derden. Hierdoor is het lastig om de volledige omvang van een risicogebeurtenis te voorspellen. Het begrijpen van deze mechanismen is cruciaal voor het ontwikkelen van effectieve mitigatiestrategieën. Organisaties moeten hun onderlinge afhankelijkheden in kaart brengen om potentiële verspreidingspaden beter te kunnen anticiperen.

2.4 Feedbacklussen

Feedbacklussen kunnen risico's verergeren. Deze lussen kunnen herstelpogingen belemmeren en de duur van een incident verlengen. Het herkennen van feedbackmechanismen is essentieel bij cascadecyberrisicomanagement om de veerkracht in onderling verbonden systemen te verbeteren.

2.5 Niet-lineaire effecten

De relatie tussen systeemcomponenten is vaak niet-lineair, wat betekent dat storingen kunnen leiden tot onevenredig grote gevolgen, wat risicobeoordeling en -beheer compliceert. Effectieve modelleringstechnieken zijn essentieel om deze dynamiek te begrijpen en te beperken.

2.6 Vertraagde effecten

De gevolgen van een cyberbeveiligingsincident zijn mogelijk niet direct merkbaar en leidt vaak tot vertraagde reacties die de situatie kunnen verergeren. Organisaties moeten mogelijk gevoeligere bewakingssystemen implementeren om problemen vroegtijdig te detecteren en effectiever te reageren. Het begrijpen van mogelijke vertragingen is essentieel voor het plannen van strategieën voor respons op incidenten en voor het vermijden van overreactie in het risicomanagement.

2.7 Afhankelijkheid van vertrouwen

Suboptimaal vertrouwen in andere componenten of systemen kan ertoe leiden dat organisaties potentiële kwetsbaarheden over het hoofd zien of juist overschatten. Hierdoor neemt de kans op opeenvolgende fouten toe. Het creëren van een just culture, d.i. een cultuur waarin potentiële risico's regelmatig kunnen worden beoordeeld, kan organisaties helpen deze afhankelijkheid te verminderen. Vertrouwen moet continu worden geëvalueerd in onderling verbonden omgevingen.

2.8 Complexiteit

De complexiteit van onderling verbonden systemen kan potentiële kwetsbaarheden verhullen en het moeilijk maken

om risico's effectief te identificeren en aan te pakken. Naarmate systemen evolueren, neemt de complexiteit toe, waarbij toenemende complexiteit deze uitdagingen versterkt.

2.9 Dynamische aard

De onderlinge verbondenheid van systemen verandert in de loop van de tijd, met nieuwe integraties en afhankelijkheden die zich vormen, die het risicolandschap kunnen veranderen. Continue monitoring en adaptieve governance-frameworks zijn nodig om te reageren op deze evoluerende risico's. Organisaties moeten wendbaar blijven om nieuwe uitdagingen aan te pakken zodra ze zich voordoen. De dynamische aard van onderling verbonden systemen, met evoluerende integraties en afhankelijkheden, kan het risicolandschap plotseling veranderen. Hierdoor zijn continue monitoring en adaptief bestuur noodzakelijk om opkomende risico's effectief te beheren.

2.10 Onzichtbaarheid van risico's

Cascadecyberrisico's kunnen verborgen blijven totdat ze zich manifesteren, waardoor proactief risicomanagement een uitdaging wordt. Organisaties moeten proactieve risicobeoordelingstechnieken toepassen om potentiële kwetsbaarheden te identificeren voordat ze tot incidenten leiden. Meer transparantie kan helpen bij het herkennen en aanpakken van deze onzichtbare risico's. De onzichtbaarheid van cascadecyberrisico's compliceert proactief risicomanagement, waardoor de invoering van proactieve risicobeoordelingstechnieken en meer transparantie noodzakelijk is om potentiële kwetsbaarheden te identificeren en aan te pakken.

Sectie 3. Op weg naar een geïntegreerde aanpak

De toenemende complexiteit en onderlinge verbondenheid van systemen vereisen verhoogde waakzaamheid en innovatieve technieken voor risicobeoordeling. Edward Tenner (1996) betoogt dat technologische vooruitgang risico's vaak transformeert in plaats van uitroeit, wat leidt tot onvoorziene negatieve gevolgen. Hij noemt dit het 'revenge-effect van technologische innovatie'. Dit concept van technologische wraakeffecten benadrukt de noodzaak van aanhoudende waakzaamheid bij het beschermen van de samenleving tegen de chronische en subtiele problemen die worden veroorzaakt door technologische innovatie (Tenner, 1996). Een geïntegreerde aanpak van cascade-cyberrisicomanagement is essentieel. Het revenge-effect wordt steeds belangrijker voor cyber risk management. Jazairy (2024) benadrukt het actuele belang hiervan door het integreren van cybersecurityrisicomanagement in strategisch management, waarbij cybersecurity-inspanningen worden afgestemd op bredere organisatiestrategieën om digitale activa en infrastructuur te beschermen tegen evoluerende cyberdreigingen. Melaku (2023) stelt voor om een dynamisch en adaptief cybersecurity-governancekader op te nemen om ervoor te zorgen dat beveiligingsrisico's op de juiste manier worden beheerd en organisatorische middelen worden geoptimaliseerd.

Sectie 4. Het 'Toren van Babel'-effect

De onderlinge verbondenheid van systemen vereist een gemeenschappelijke taal en verhaal om transparantie en samenwerking in de hele toeleveringsketen te bevorderen. Het ontbreken van een uniforme taal in cyberbeveiliging creëert echter aanzienlijke barrières voor effectieve communicatie, wat leidt tot het 'Toren van Babel'-effect (Dijkstra et al., 2024; ENISA, 2023b). Dit effect beschrijft de uitdagingen die worden veroorzaakt door uiteenlopende en onverenigbare terminologieën, richtlijnen, kaders en methodologieën tussen verschillende belanghebbenden, wat resulteert in miscommunicatie, inconsistente risicobeoordelingen en onsamenhangende mitigatie-inspanningen.

4.1 Behoefte aan een gemeenschappelijke taal

Het vaststellen van een gemeenschappelijke taal is essentieel om het 'Toren van Babel'-effect te overwinnen. Organisatieleiders en bestuurders dragen de verantwoordelijkheid om complexe concepten te vereenvoudigen en terminologie te gebruiken die bij alle werknemers aanslaat, ongeacht hun technische expertise. Deze aanpak verbetert het situationele bewustzijn en stelt werknemers in staat om op zinvolle wijze bij te dragen aan de cascadecyberresilience-inspanningen van de organisatie (World Economic Forum, 2017).

4.2 De rol van leiders en besturen

Leiders en bestuurders moeten ervoor zorgen dat cybersecurity is ingebed in de gehele organisatiecultuur en dat er een gemeenschappelijke taal en verhaallijn wordt vastgesteld. Zij moeten dit verhaal ook actief uitdragen. Door cybersecurity-inspanningen af te stemmen op bredere organisatiestrategieën, kunnen leiders een gedeeld begrip van de betrokken risico's en de collectieve verantwoordelijkheid voor het beperken ervan bevorderen.

Sectie 5. Misalignment tussen regels en realiteiten

Er zijn verschillende misalignments tussen regels en de realiteit in cascadecyberrisicomanagement, die effectieve cascade risicobeperking in de weg staat. Hieronder worden de vijf belangrijkste genoemd.

5.1 Rule based versus Risk based management

Cyberrisicomanagement in Nederland en de EU is sterk afhankelijk van verschillende risicokaders, wat leidt tot verwarring vanwege verschillende terminologieën en definities. Zo kan de term 'risico' meerdere interpretaties hebben, wat de afstemming van cyberbeveiligingsmaatregelen bemoeilijkt. Daarnaast kan er verwarring ontstaan over wat 'risicobereidheid' inhoudt en het benodigde niveau van veerkracht. Volgens Dijkstra et al. (2024) worstelen veel organisaties nog steeds met hun cyberrisico-identiteit en -bereidheid. De overvloed aan richtlijnen en kaders, zoals NIST, ISO en ITSRM2, verergert deze verwarring nog verder, wat vaak resulteert in een checkboxmentaliteit waarbij risicomanagers zich richten op vormen van naleving van regels in plaats van analyse van daadwerkelijke risico's in de actuele realiteit. Dijkstra en Veen stellen voor om een op risico's gebaseerde aanpak te hanteren en een routekaart voor cyberrisicobeheer te delen om deze kaders beter af te stemmen op risico's van de realiteit. Afstemming is noodzakelijk voor effectief cyberrisicobeheer en vereist gecoördineerde communicatie tussen verschillende organisatieniveaus, van CERT/CSIRT-teams tot senior management, risico-eigenaren, toezichthoudende instanties en nationale cyberbeveiligingsautoriteiten. Er is echter vaak sprake van onvoldoende afstemming in het verzamelen van informatie tussen managementteams, wat leidt tot geïsoleerde inspanningen en ineffectief risicobeheer. Het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA, 2024) benadrukt het belang van gecoördineerde communicatie voor gedeeld situationeel bewustzijn, dat momenteel onderontwikkeld is.

5.2 Usability versus Cybersecurity

Er bestaat een aanzienlijk probleem in afstemming tussen cyberbeveiligingsmaatregelen en bruikbaarheid, waardoor er spanning ontstaat tussen beveiliging en gebruiksgemak. Gebruikers vinden bijvoorbeeld complexe authenticatieprocessen vaak belastend, belemmerend of stressvol, wat leidt tot frustratie en mogelijke beveiligingslekken. Onderzoek door Furnell (2024) benadrukt de uitdagingen van het bruikbaar maken van cyberbeveiliging zonder de beveiliging in gevaar te brengen. Reuter et al. (2022) benadrukken de noodzaak van transparantie en aanpasbaarheid in beveiligingsmaatregelen om de acceptatie en effectiviteit van gebruikers te verbeteren. Grobler et al. (2021) pleiten voor een mensgerichte benadering van cyberbeveiliging, met de nadruk op gebruikersgedrag en cognitieve percepties om de kloof tussen beveiliging en bruikbaarheid te dichten. Afstemming is hier ook noodzakelijk. Discrepanties tussen bruikbaarheid en beveiliging kunnen een bron van kwetsbaarheden voor systemische risico's zijn in de supplychain.

5.3 Academische opleiding versus Behoeften van de industrie

Er is een opvallende discrepantie tussen cyberbeveiligingsonderwijs en de vereisten van de industrie. Huidige onderwijsprogramma's voorzien studenten vaak niet in de praktische vaardigheden die nodig zijn op de arbeidsmarkt. Yusuf (2024) betoogt dat cyberbeveiligingscurricula moeten worden bijgewerkt om aan de eisen van de industrie te voldoen, zodat afgestudeerden vanaf dag één klaar zijn voor een baan. AlDaajeh et al. (2022) stellen voor om onderwijsprogramma's af te stemmen op nationale cyberbeveiligingsstrategieën om de vaardigheidskloof te dichten. Towhidi en Pridmore (2023) presenteren een model voor het ontwerpen van cursussen die aansluiten bij de behoeften van de industrie en benadrukken daarbij het belang van praktische, hands-on ervaring. Het is cruciaal om deze discrepantie in het veld op te lossen. Hier is afstemming nodig. Er is bovendien een groot tekort aan personeel voor cascade-cyberrisico's en zij moeten adequaat zijn uitgerust om hun missie uit te voeren.

5.4 Misalignments in de cascade supplychain

ENISA (2023b) identificeerde vier categorieën van veelvoorkomende organisatorische misalignments tussen regels en realiteit met betrekking tot supply chain risk management. Ze benadrukten verschillende kennishiaten en relateerden deze aan een supply chain risk management. Deze hiaten werden gecategoriseerd in vier opeenvolgende gebieden met 'to do'-stappen, waarbij de nadruk werd gelegd op de misalignments tussen theoretische regels en praktische realiteiten:

a) Supply Chain Risk Management:

- Begrijp de supplychain; identificeer leveranciers en aanbieders
- Begrijp de potentiële risico's voor de organisatie en voor eindklanten.

  Misalignment: Organisaties slagen er vaak niet in hun

toeleveringsketen volledig in kaart te brengen, wat leidt tot hiaten in de identificatie en het beheer van risico's

b) Beheer van relaties in de toeleveringsketen:

- Beheer de toeleveringsketen; zorg voor beleid en overeenkomsten; definieer cyberbeveiligingsvereisten
- Monitor de prestaties van leveranciers en dienstverleners; beheer wijzigingen

  Misalignment: Beleid en overeenkomsten kunnen op papier bestaan, maar de implementatie en handhaving ervan zijn vaak inconsistent, waardoor kwetsbaarheden niet worden aangepakt

c) Omgaan met kwetsbaarheden:

- Beheer kwetsbaarheden; ken uw activa; begrijp de risico's van kwetsbaarheden
- Monitor kwetsbaarheden; patch kwetsbaarheden; zorg voor een gedefinieerd onderhoudsbeleid

  Misalignment: Ondanks dat ze kwetsbaarheidsbeheerprocessen hebben, worstelen veel organisaties met tijdige patching en asset management, wat leidt tot exploiteerbare hiaten

d) Kwaliteit van producten en diensten:

- Bied veilige producten en diensten; bescherm de infrastructuur; zorg voor veilige processen
- Implementeer technische maatregelen; creëer transparantie in de toeleveringsketen; meet de kwaliteit van producten en diensten

  Misalignment: De kwaliteit en veiligheid van producten en diensten schieten vaak tekort aan de normen vanwege ontoereikende technische maatregelen en gebrek aan transparantie in de toeleveringsketen

5.5 Misalignment van theoretische kaders

Hubbard (2020) en Cremer et al. (2022) betogen dat traditionele methoden en kaders voor risicobeheer voornamelijk falen vanwege hun afhankelijkheid van kwalitatieve beoordelingen en gebrek aan kwantitatief empirisch bewijs. Kwantitatieve benaderingen zijn nodig om zich aan te passen aan de dynamische aard van cascade cyberdreigingen, waar deze tekortkomingen bijzonder uitgesproken zijn. Cascadecyberrisico-onderzoek is bovendien vaak gebaseerd op ex post facto-gegevens, verzameld nadat een incident heeft plaatsgevonden. Wat nodig is, is uitgebreide gegevensverzameling in de hele toeleveringsketen – vóór, tijdens en na cyberincidenten. Er is ook een mismatch in het begrip van wat data is. Voor wetenschappelijke doeleinden moeten kwantitatieve gegevens meetbaar, herhaalbaar en toegankelijk zijn. Om deze mismatches tussen theoretische kaders en empirische gegevensverzameling aan te pakken, is een gezamenlijke inspanning vereist om cybersecuritypraktijken voortdurend te evalueren en te verbeteren op basis van empirische systemische gegevens. Het is bijvoorbeeld cruciaal om op basis van gegevens te voorspellen welke bedrijven binnen een toeleveringsketen waarschijnlijk worden aangevallen wanneer een leverancier binnen de keten wordt gecompromitteerd. Deze voorspellende capaciteit zou betere voorbereidings- en responsstrategieën mogelijk maken, waardoor de algehele veerkracht van de toeleveringsketen tegen cascade cyberbedreigingen wordt verbeterd. Samenvattend benadrukt de huidige stand van zaken van cascade cyber risk management verschillende belangrijke kwesties:

1) De noodzaak van verhoogde waakzaamheid tegen cascade threats
2) Verwarring en inadequate afstemming tussen regels en realiteit in meerdere domeinen in dit veld
3) een gebrek aan adequate empirische gegevens

Secties 6 en 7 zullen deze uitdagingen aanpakken door oplossingen te bieden voor de vijf geïdentificeerde verkeerde afstemmingen. In sectie 6 introduceren we de theorie van het computationele gedeelde mentale modellen dat AI-gebaseerde risicobeoordelingen van cascade-risico's faciliteert. Sectie 7 schetst de onderzoeksmethodologie van de Cybersecurity Living Lab-benadering, als oplossing voor bovengenoemde problematiek, en die uitgebreide gegevensverzameling voor cascadecyberrisico's mogelijk maakt.

Sectie 6. Computationele gedeelde mentale modellen voor cascadecyberrisicobeheer

De theorie van gedeelde mentale modellen biedt een aanpak voor het aanpakken van misalignments in cascadecyberrisicobeheer. Kenneth Craik (1943) introduceerde het concept van mentale modellen als interne representaties van de externe wereld die individuen helpen om door hun omgeving te navigeren. Deze modellen zijn dynamisch en kunnen in de loop van de tijd evolueren, wat zorgt voor een betere aanpassing aan nieuwe uitdagingen (Craik, 1943).

6.1 Organisatorisch leren

Organisatorisch leren begint met individuen die hun mentale modellen aanpassen als reactie op nieuwe ervaringen. Deze kennis kan worden gedeeld via discussies, evaluaties van fouten en best practices, games of andere sociale interacties, wat leidt tot collectief leren.

Feedbackloops stellen organisaties in staat om van individuen te leren en vice versa, wat de algehele aanpassingsvermogen verbetert (Canbaloglu et al., 2022; Roelofsma et al, 2024).

6.2 Netwerkmodellering van complexe systemen

Adaptieve netwerkmodellen kunnen de complexiteit van gezamenlijk mentale modellen en organisatorisch leren weergeven. Deze modellen leggen relaties vast tussen staten en hun dynamiek, wat zorgt voor realistischere representaties van leer- en vergeetprocessen. Deze aanpak ondersteunt een beter begrip en modellering van hoe organisaties leren en zich aanpassen in de loop van de tijd (Treur, 2020; Roelofsma et al., 2024).

6.3 What-if-analyse voor cascaderisicobeoordeling

De what-if-analyse evalueert verschillende cascadecyberaanvalscenario's en hun potentiële impact op de beveiligingshouding van een organisatie en de samenleving. Met behulp van AI-technieken helpt deze analyse mogelijke toekomstige gevolgen te beoordelen onder verschillende contextuele kenmerken, waardoor het vermogen van een organisatie om zich systematisch aan te passen aan cyberrisico's en deze te beperken, wordt verbeterd (Mestour et al., 2024; Roelofsma et al 2024).

Sectie 7. De Cybersecurity Living Lab (CSyLL)-methode

Het Cybersecurity Living Lab (CSyLL)-initiatief speelt in op de behoefte aan meer afstemming in cyberbeveiliging en bovenstaande problematiek aan te pakken door gebruik te maken van het Quadruple Helix- raamwerk (Carayannis et al., 2009, 2012). Dit raamwerk integreert de academische wereld, de industrie, de overheid en het maatschappelijk middenveld om veerkrachtige beveiligingspaden samen te creëren en te ontwerpen. De Living Lab-methode omvat een adaptief kennisdelingsproces om samenwerking en innovatie te bevorderen, zodat de unieke perspectieven en expertise van elke sector bijdragen aan uitgebreide cybersecurityoplossingen.

De Living Lab-benadering integreert gedeelde mentale modellen en theorieën over organisatorisch leren om samenwerking en innovatie te verbeteren. Door gedeeld begrip en continu leren te bevorderen, streeft het Lab ernaar de effectiviteit van zijn gezamenlijke inspanningen te verbeteren (Lupp, 2021; Roelofsma et al., 2024).
Het Cybersecurity Living Lab is een experimentele werkomgeving waar studenten, onderzoekers, bedrijven, publieke instellingen en eindgebruikers samenwerken om nieuwe ideeën, producten en diensten op het gebied van cybersecurity te ontwikkelen, testen en evalueren in de praktijk. Door middel van innovatieve experimenten en onderzoek leren deelnemers effectief te reageren op cyberdreigingen en risico's te beheren.

7.1. Doelstellingen van het Cybersecurity Living Lab

Het CSyLL-initiatief heeft tot doel:

- Gegevens verzamelen: empirische gegevens verzamelen voor op bewijs gebaseerd cascade-risicobeheer
- Oplossingen samen creëren: veerkrachtige beveiligingspaden ontwikkelen met meerdere belanghebbenden
- Onderwijs verbeteren: studenten praktische ervaring bieden in cybersecurityrisicobeheer
- Onderzoek faciliteren: onderzoekssamenwerkingen mogelijk maken om innovatieve benaderingen van cybersecurity te verkennen

Het proces in het Living Lab is iteratief, met voortdurend feedback verzamelen en verbeteringen aanbrengen. Hierdoor kan het Lab innovaties ontwikkelen die aansluiten bij de behoeften en het gedrag van gebruikers in hun dagelijks leven. Living Labs richten zich op complexe maatschappelijke uitdagingen, waarbij onderzoek en duurzaamheid centraal staan. Ze bevorderen realtime leren en dichten de kloof tussen theoretisch onderzoek en praktische toepassing. Innovaties zijn hierdoor gericht op daadwerkelijke bruikbaarheid en acceptatie door de gebruiker. In het Cybersecurity Living Lab creëren de deelnemers met deze visie een leergemeenschap voor cybersecurity.

7.2 Wat gebeurt er in het Cybersecurity Living Lab?

De belangrijkste onderdelen van het Lab zijn:
Cybersecuritywerkplaats. In de cybersecuritywerkplaats werken de deelnemers met het Living Lab-concept aan de toekomst van cyberveiligheid. Zij ontwikkelen nieuwe technologieën, leermodules, AI-hulpmiddelen en meer. Realtime dreigingsmonitoring en incidentrespons. Studenten en professionals leren hoe ze effectief kunnen
reageren op cyberaanvallen met realtime dreigingsdetectie, incidentrespons en cyberrisicomanagement.
Security Operations Center (SOC). In het lab zetten de deelnemers een SOC op waar studenten en onderzoekers leren hoe ze cyberdreigingen kunnen identificeren, analyseren en aanpakken, vergelijkbaar met hoe professionele cybersecurityteams dat doen. Dit biedt hen niet alleen

praktijkervaring, maar ook de mogelijkheid om onderzoek te doen naar risicomanagementmethoden.
Onderwijs en training. Studenten en andere deelnemers doen praktijkervaring op met cybersecuritytools, zoals risicomanagementraamwerken, beveiligingssoftware, procedures voor incidentrespons en cyberwargaming. Ze leren hoe ze risico's kunnen beoordelen, monitoren en beheren, en hoe ze kunnen reageren op cyberdreigingen. Het lab biedt ook mogelijkheden voor stages, afstudeerprojecten en postdoctoraal onderzoek. In samenwerking met docenten en het bedrijfsleven streeft het Living Lab ernaar onderwijsvernieuwingen te realiseren die beter aansluiten bij de praktijk.

Toegepast onderzoek. Samen met bedrijven, onderzoekers en studenten doen we onderzoek naar innovatieve oplossingen voor cybersecurity. De onderzoeksthema's variëren van het optimaliseren van cyberrisicomanagement en het bestuderen van biases en kennisoverdracht tot het ontwikkelen van gezamenlijke mentale modellen. Daarnaast onderzoeken we het co-creatieproces met eindgebruikers, bijvoorbeeld bij systeemontwerp en authenticatie. Tot slot richten we ons op onderzoek naar beslisondersteuning, de rol van cyber management games en de inzet van kunstmatige intelligentie als hulpmiddel bij cyberrisicomanagement.

Cyber Security simulatielab. Dit is een belangrijk onderdeel van het Living Lab. In het Cyber Security simulatielab ontwikkelen de deelnemers specifieke simulaties voor cyberrisicomanagement met behulp van AI- modellen. Deze simulaties worden gebruikt voor onderwijs, productontwikkeling en onderzoek. Verbinding tussen onderwijs en bedrijfsleven. Het Living lab werkt nauw samen met bedrijven om ervoor te zorgen dat de activiteiten aansluiten bij de nieuwste security- en veiligheidsnormen, regelgeving en technologische trends. Hierdoor blijft het onderwijs relevant en up-to-date, en kunnen studenten werken met tools en gegevens die in de praktijk worden gebruikt.

Sectie 8. Een 'Narrative of Change'

In een tijdperk van toenemende cyberdreigingen realiseren organisaties zich dat ware cyberveerkracht niet in isolatie kan worden bereikt. De onderlinge verbondenheid van de digitale wereld betekent dat één kwetsbaarheid kan leiden tot cascadecyberrisico's, waarbij één inbreuk meerdere storingen veroorzaakt. Het cyberbeveiligingslandschap vereist samenwerking, gedeeld begrip en collectieve actie. Net zoals de mensen van Babel een monumentaal project begonnen, moeten wij een maatschappelijke transitie naar verbeterde cyberbeveiliging ondernemen, ondersteund door een positieve en omarmde mindset.

Het verhaal van de Toren van Babel herinnert ons aan de gevolgen van verdeeldheid en ambitie zonder gedeelde verantwoordelijkheid. De mensen van Babel wilden een grote stad en toren bouwen om roem te vergaren, maar hun gebrek aan samenwerking leidde tot verwarring en mislukking. Dit principe geldt ook voor cyberbeveiliging: echte prestaties liggen in samenwerking, niet in concurrentie. Wanneer organisaties individuele onderscheidingen boven collectieve verantwoordelijkheid stellen, volgen verwarring en fragmentatie. Cascadecyberrisicomanagement is zowel een technische als maatschappelijke uitdaging. We moeten een gedeeld mentaal model bevorderen dat organisatorische grenzen overstijgt. Door een cultuur van samenwerking en effectieve communicatie te creëren, kunnen we veerkrachtige systemen bouwen die bestand zijn tegen cyberdreigingen. Dit vereist een positieve benadering van verandermanagement en een gedeeld gevoel van doel en verantwoordelijkheid.

Sectie 9. Conclusie

Cascadecyberrisico's vormen aanzienlijke uitdagingen voor moderne organisaties, met name in kritieke infrastructuur. De onderlinge verbondenheid van systemen, gedeelde kwetsbaarheden en niet-lineaire effecten compliceren risicobeoordeling en -beheer. Een geïntegreerde aanpak, ondersteund door gedeelde mentale modellen en organisatorisch leren, is essentieel voor het verbeteren van de veerkracht tegen cascadecyberdreigingen. Het Cybersecurity Living Lab-initiatief biedt een veelbelovend raamwerk voor het aanpakken van deze uitdagingen door samenwerking tussen de academische wereld, de industrie, de overheid en het maatschappelijk middenveld te bevorderen. Door adaptieve netwerkmodellering en empirische gegevensverzameling te benutten, kunnen organisaties beter anticiperen op cascade cyberrisico's en deze beperken, wat zorgt voor een veiliger en veerkrachtiger digitaal ecosysteem.

Voor een complete lijst van referenties, kun je het artikel raadplegen dat vanaf eind april op de site van PvIB staat.

Auteur: Ellen Wesselingh is senior architect at Fox Crypto, 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. The full article can be found on https://foxdatadiode.com/news/

Eliminating the weakest link

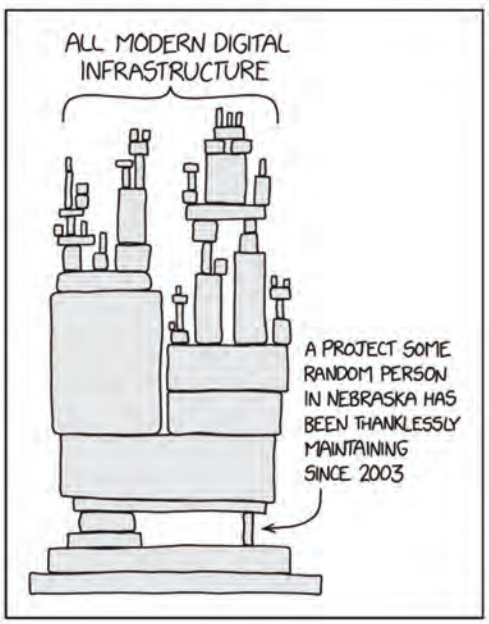
Managing Supply Chain Cybersecurity Risk through Components Analysis

This article describes a follow-up activity for analysis described in Eliminating the weakest link – Managing Supply Chain Cybersecurity Risk through Life Cycle Modelling (IB-Magazine 4 2024): the analysis of security critical components, and follow-up action. Not all components in a system are security critical, so measures in the supply chain may vary in rigour. An example are the screws with which a casing is closed, provided the casing is not essential for security measures, such as anti-tamper. Hence, the security critical functions, being those functions that are security enforcing and those being security supporting, must be identified. After the supply chains for a product have been identified, measures may be discussed with partners. Open source projects may have to be treated differently.

In the previous article (IB-Magazine 4 2024), a supply chain risk analysis model was introduced, based on a MITRE model dating from 2013. Where the primary focus was to develop a supply chain attack framework that addresses the primary process in which a product with IT components is produced, this article builds on that model to further refine the risk analysis.

When developing a system, whether it is an embedded system with hardware, firmware, and software components, or a software only system, many supply chains exist. Randall Munroe (XKCD) showed this very profoundly for Open Source Software (OSS), in a 2020 cartoon (1). The picture illustrates the problem with many supply chains. In commercial as well as open source supply chains, the entity that finally brings the product on the market has little overview on, and control over, the many suppliers.

Some suppliers are large corporations with the means to implement cybersecurity measures in all their development processes. Other suppliers are on the opposite side of the spectrum: small communities without the means or the



Dependency (Munroe), source (1)

Supply chain attacks are a real risk, and come in new formats frequently

knowledge to implement and maintain cybersecurity measures. Many more are probably in between those ends of the scale. The challenge is, that the entity bringing the product on the market, probably does not know exactly the status of each supplier.

Analysing all components of a product, and their respective supply chains, is probably impossible. Therefore, the scope of the components under analysis must be reduced. This is done by eliminating non-security critical components from the analysis. How this can be done is the topic of this article. Secondary services such as the supply chain of other office 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 original research was inspired by a presentation from Andrew Huang for a Blue Hat conference. In his presentation, Huang mentioned a number of attacks. 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.

Some seminal software attacks were studied for illustration of supply chain software attacks. In 2024, a next level type of open source attack emerged (XZ Utils): a combination of social engineering and poisoning of open source libraries with backdoors. The attack did not materialise in full, but was very close to success. Other examples of supply chain problems that emerged in 2024 are the worldwide failure of Windows servers due a CrowdStrike update in July, the temporary shutdown of the Dutch high-security network NAFIN in August, and the pager/walkie-talkie attacks on Hezbollah in September. The Windows and NAFIN problems were probably not the result of an act with malicious intent, the resulting system failure caused widespread problems for society nonetheless. Finally, the attack on Hezbollah was an elaborate supply chain attack, in which an Advanced Persistent Threat (APT) was capable of manipulating a complete supply chain.

The XZ Utils backdoor showed that a malicious entity was capable to create a persona (or multiple), and build trust with that random person thanklessly maintaining the library since 2003. The malicious entity was eventually able to take over the project, and implant a backdoor to target security critical software like OpenSSH. In this case, an application built on top of the core was able to infect another component through that core. One of the largest cyber incidents in history was avoided because one developer running Debian Sid Linux noticed the SSH Daemon using a bit more CPU time than normal, while benchmarking something completely unrelated. The type of attack shows the importance of knowing your supply chains. It also shows how difficult it is to manage all supply chains.

The model as described in the previous article is the starting point for the next step in the process: the determination of security critical components, and detailed analysis of the supply chains of these components. For this part of the research, the Common Criteria is used. This international standard for IT product security evaluation defines the notion of security enforcing, security supporting, and security non-interfering functions.

Previous model

The model as described in the previous article uses the following step-by-step supply chain risk analysis:

1. Sketch a life cycle and if possible, a supply chain model.
2. Determine the applicable categories from the attack surface categories: architecture, standard, hardware, firmware, operating system or software, development environment.
3. For the above determined applicable categories, determine the attacks that are applicable.
4. Plot the attacks on the life cycle model.
5. For each attack, discuss with expert colleagues what countermeasures are possible to counter the attack.
6. For all countermeasures, discuss with the relevant supply chain partners what is possible.
7. When all countermeasures that will be applied are known, identify any remaining risk.
8. Within a specific evaluation / certification framework, the risk may be quantified. For example, in the Common Evaluation Methodology there is a vulnerability analysis, of which the outcome is the calculation of attack potential needed to attack the IT product under evaluation successfully.

The steps described above, are the generic steps for any supply chain analysis. However, there are many types of products with their own supply chain specific issues. Therefore, for a specific product, a more detailed analysis is necessary. This analysis requires to narrow the scope to keep the workload manageable. The first step is to define for each component whether it is:

1. Security enforcing: these components directly implement a security functional requirement, for example user identification and authentication.
2. Security supporting: these components do not directly implement a security functional requirement, but have to function correctly for the security enforcing components to be able to do their job. A typical example is the Human Machine Interface (HMI), which is used for user identification and authentication.
3. Security non-interfering: the security enforcing and supporting components do not rely on these components for their correct functioning. Ideally, these components cannot influence the correct functioning of security enforcing and supporting components at all. The XZ Utils case showed just how difficult this is. Examples are usually the casing and power connection.

Next steps in the analysis

The definition of a component as security enforcing, supporting, or non-interfering, is dependent on multiple factors. The first, and main, input is the definition of assets in the security claim. This claim should describe what the type of assets are, such as (personal) data, or operational processes. For the defined assets, it must be clear what protection is to be provided: confidentiality, integrity, or availability. Typically, for (personal) data, confidentiality is the most important aspect. For operational processes, availability is usually the most important aspect. Both confidentiality and availability require system integrity as a fundament.

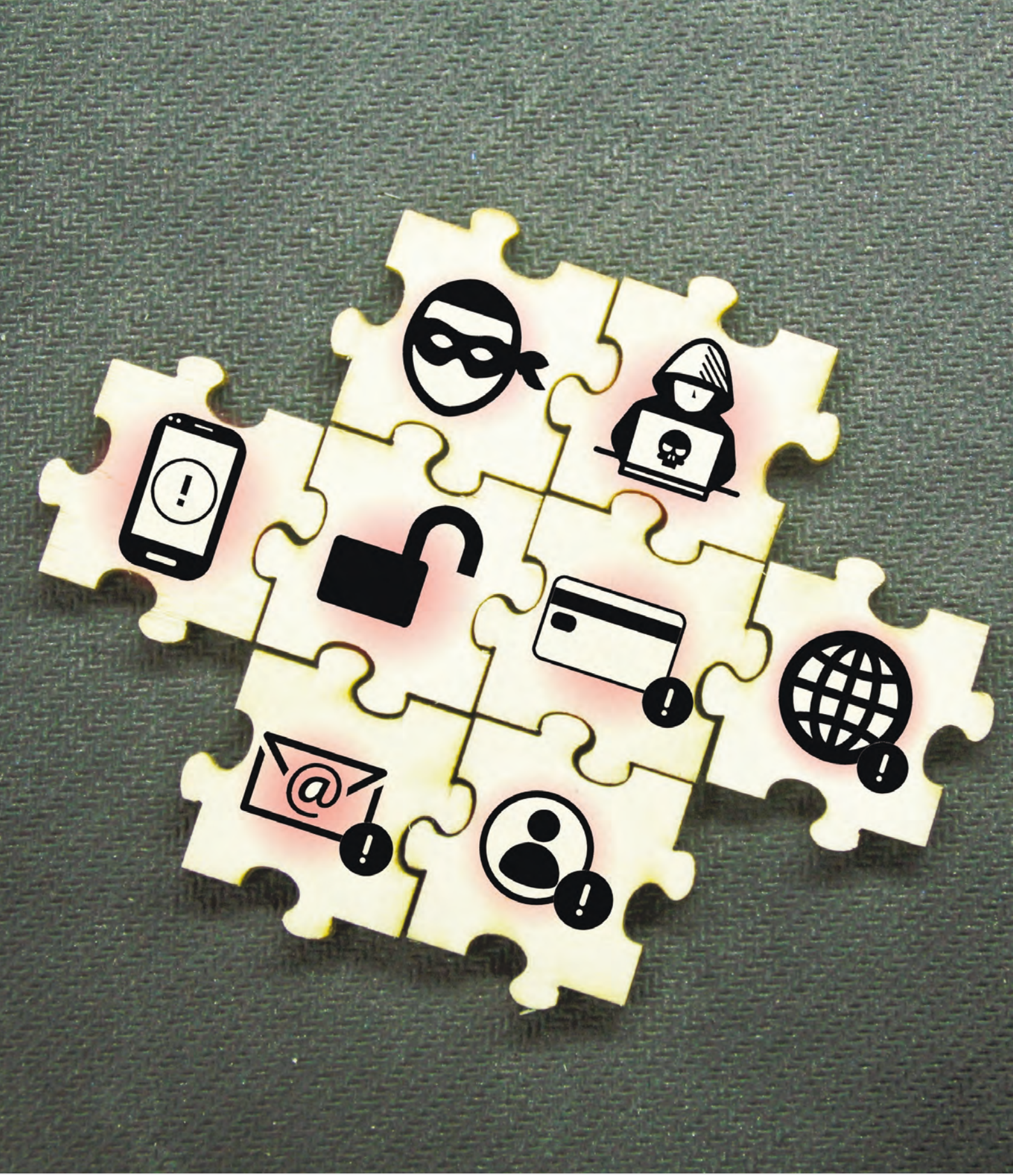
The second, and very important, input is the security functionality that the product has to provide. The fact that the security claim is used for analysis, means that certain quality criteria apply to that claim. If a security claim description is not factual or measurable, then it is not possible to base the analysis on that claim. Common Criteria provides a library with standardised security functional requirements to support the development of a well-defined security claim.

The experts decide for all components their contribution to the security functions. This is usually done in the format of a meeting with experts from different disciplines. For each component, its function with regard to the assets as defined in the security claim, is discussed. This leads to a list of components classified as either security critical (enforcing or supporting), or non-interfering. Security non-interfering components do not have to be subject to precautionary measures in the supply chain, security critical components do.

For these security critical components, the manufacturers are determined. A manufacturer can be a commercial entity, established in the EU itself or through a partner. This type of supplier can be addressed in a formal contractual relationship. A manufacturer can also be an open source project. With this type of supplier, no formal relationship exists. The community maintaining the open source project may even be unaware of the fact that specific companies use their products. Therefore, this type of supply chain needs to be treated differently.

Managing Supply chain partners

When dealing with formally established entities, supply chain security measures can be negotiated and defined in the contract. Agreed security measures, comparable to a Non-Disclosure Agreement (NDA), would help to formalise the supply



chain relationship between supplier and acquirer. As an input to this contractual agreement, the measures as described in the appendix of the previous article can be used.

When dealing with an open source community, establishing a formal relationship may prove to be hard. Fox-IT has experience with this process, when building OpenVPN-NL on top of OpenVPN. OpenVPN exists since 2001, and is maintained by an international community. OpenVPN-NL exists since 2011, and is maintained by Fox-IT. It took several years to establish a relationship of trust between both parties. There are other examples of commercial companies supporting open source projects, for example by giving employees with specific expertise time to maintain an open source project. Other communities are strong communities themselves, built in the course of years.

Sponsors could play a role in building stronger OSS communities. Commercial entities may be willing to participate in the development of open source projects under the umbrella of Corporate Social Responsibility (CSR), but maintaining a large open source project is probably more expensive than the CSR budget. However, when multiple companies donate, the burden is shared. In 2011, Fox-IT published OpenVPN-NL open source, Fox Crypto is maintaining it. In 2022, Fox-IT made its own toolset for incident response analysis, Dissect, open source. In 2023, Fox Crypto built, and published open source, its' own implementation of a Post Quantum Resilient XMSS algorithm. Parts of these project have been sponsored by the Dutch government. This sponsorship enables the Fox companies, which are medium businesses, to help in building a more (cyber)secure society.

How, as a company, to build trust in an open source community? In our experience, communication and participation are crucial. Trust must be mutual. Companies often support with technology (code), but can also help a project to make their development processes more mature. For example, by contributing to secure development processes or providing infrastructure or tooling to perform code quality checks. Building trust typically requires showing capabilities and long-term commitment. Over time, a community will be able to judge company contributions on their merits, and the company can judge whether the stability and maturity of the community meets their supply chain requirements.

Basically, everything that the attacker in the XZ Utils case did… In hindsight, it is somewhat strange to see that a company that builds trusted systems for the high assurance industry is met with suspicion, while entities claiming to be an individual are not rigorously checked at all. Given the history of government meddling in cryptographic issues, it is understandable. But companies are usually not lead by malicious intent with regard to building backdoors on purpose, the problems probably arise due to incompetence rather than maliciousness.

Steps to assure if the components fit

What should manufacturers of composite systems do, when incorporating open source components in their product? They should at least assess whether these components are security critical. For those components, the following checks may provide some assurance that the components are fit for purpose:

1. Whether the community is a robust community, in the sense that it is well established, and maintained by a sufficiently large pool of maintainers. With regard to maintenance, active maintenance can be monitored using the following metrics: the time it takes to solve reported issues, how many pull requests are currently open, average time a pull request remains open.
2. If possible, verify where the community is established, and where the maintainers reside. Find out which organisation maintains the community, are one or more companies or other established organisation involved, or is the community maintained purely by volunteers. Do the organisations supporting the community have a solid reputation. Team size is also an indicator of the stability of the community. Refrain from using open source software from communities established in nations with an offensive cyber-strategy.
3. Review the quality of the product, the accompanying documentation, and the work processes. Check whether the product is feature complete, if not, what the status of the product is. Check whether the documentation is available, readable, and complete. Verify if issues are reported and fixed on for example GitHub, and if the time between reporting of an issue and solving the issue is commensurate with the functionality of the product and the severity status of the issue. Verify if the product is actively discussed on platforms like Discord, Reddit, Stack Overflow. If there is a product roadmap available, this provides assurance about long term availability.
4. If possible, use externally verified components. Some OSS have been evaluated, which provides some assurance about the quality. The OpenVPN-NL variant of OpenVPN is

such an example.

5. When the technical expertise is available, do a source code review. As source code reviews are laborious, focus on the security critical components, such as input validation or cryptographic operations. Another option is to verify that public (high quality) code reviews have been done. OpenVPN for example is audited externally every now and then.
6. Finally, check whether the OSS license is fit for purpose. There are license types that prohibit certain types of use of the product, or that require open source publication of any changes to the product.
7. Once an OSS component has been chosen, incorporate open source vulnerability scanning in the work process for importing it. This does not stop zero day attacks such as the XZ Utils attack, but it limits the potential attack surface.

These steps require resources. This may be viewed as a cost factor, where it should be viewed as an investment factor. It starts with the realisation that a security breach will certainly happen when security has not been properly reviewed during the development process. Security breaches tend to be very costly (see below).

Final steps

When the security critical components have been identified, and the applicable countermeasures are agreed upon with the supply chain partners, or otherwise addressed, remaining risks can be identified. For this step, a suitable risk identification method for the specific industry should be used. The Common Evaluation Methodology (CEM) provides a generic method for products, by modelling the attack potential that is needed to successfully attack a product. For Integrated Circuits (IC) and similar devices, there is a specific methodology available. However, these methods are laborious. For low risk Information Technology (IT) products, a method using Security Integrity Levels along the axes of exposure and impact may be sufficient. For Operational Technology (OT), a method using exposure, harm, in combination with controllability, should be used. For example, automotive safety standard ISO26262 uses Automotive Safety Integrity Level (ASIL). This model might be transposed to cybersecurity.

The remaining risk then has to be assessed for risk mitigation with the implementation of additional measures, or risk acceptance. The level of risk should be assessed against the cost of further risk reduction. Weighing risk against (further) mitigation is ultimately a business decision. This requires understanding of cybersecurity risks by the business. Seminal cases, such as Diginotar, University of Maastricht, and Maersk, which have been publicly discussed, may help the business in assessing the potential cost of a cybersecurity breach. In the case of Maersk, the entire global internal network had to be rebuilt. Not only does this lead to the cost of having to rebuild the network, it also leads to serious cost due to lost productivity. The latter may have been the largest factor in the total cost in this case.

Discussion and Conclusions

Supply chain attacks are a real risk, and come in new formats frequently. Analysis of the attack surface, to be reduced by countermeasures, is the starting point for mitigation. This article discussed further steps in the analysis of components provided by partners in the supply chain. While not all supply chain risks may be mitigated, thinking about your supply chains and options for risk mitigation are an important step towards a more robust supply chain from a security perspective.

The use of well-established standards and methods helps in establishing a base line with regard to cybersecurity in the supply chain. For small companies, or companies with little cybersecurity experience, this will be a challenge. These companies may start by using cybersecurity certified products, when available. These products are often more expensive than non-certified products, because certification requires effort and hence, a business case. However, a breach in the security of a product can prove to be very expensive. A famous example of just how expensive a breach can be, is the Dutch Diginotar case. The company eventually ceased to exist, after it was hacked. The Maersk breach with NotPetya lead to an estimated cost of $300 Million, and this company was not the only victim that suffered severe damage.

The model and the next steps as described in this article, provide a basis for supply chain risk analysis and mitigation. Important steps to make are to identify the supply chains, to identify the security critical components suppliers in the supply chain, and to make formal arrangements with those partners. The exact implementation of the countermeasures is not part of the model, as these are at the discretion of the supply chain partners.

Reference

(1) Randall Munroe (XKCD). Cartoon #2347 Dependency. August 17, 2020. https://xkcd.com/2347/ (CC-BY-NC 2.5) and https://www.explainxkcd.com/wiki/index.php/2347:_Dependency (visited 11 June 2024)

COLUMN PRIVACY

Mr. Rachel Marbus

Recht hebben versus recht krijgen

Bij de introductie van de AVG zette onze toezichthouder een flinke marketingcampagne in om duidelijk te maken welke rechten we hebben. En met succes, want steeds meer mensen weten de weg te vinden om hun gegevens in te zien, te laten wijzigen of te laten wissen. Een van de meest gebruikte gaat over inzage – wat hebben jullie van mij en wat doen jullie daarmee? En daar is al langere tijd wel wat om te doen. Zo blijkt ook uit recent onderzoek van de EDPB (European Data Protection Board). Het gaat namelijk niet bepaald lekker met de uitvoering in de praktijk.

Maar weinig organisaties hebben een eenduidige procedure ingericht. Het tijdig aanleveren van resultaten is een issue, de FG heeft ten onrechte een rol in het proces en er wordt nog steeds onnodig vaak naar een paspoort ter identificatie gevraagd. We hebben prachtige rechten op grond van de AVG, maar je recht ook ingewisseld krijgen, is nog geen uitgemaakte zaak.

Laat ik voorop stellen dat bij geen enkele organisatie waar ik gewerkt heb, een dergelijk proces vanaf het begin af aan vlekkeloos is verlopen. Maar er zijn wel een aantal zaken die je kunt oppakken die het beter kunnen maken. Mijn eerste advies is om het proces: 'Rechten van betrokkenen', eens helemaal uit te schrijven. Wie zijn betrokken in het proces en welke stappen moeten allemaal gevolgd worden? Juist door op te schrijven hoe de situatie nu is, zie je snel waar knelpunten zitten die je vervolgens weer kunt oppakken ter verbetering. Periodiek reviewen met alle betrokkenen is wel een absolute verplichting als je er het beste uit wilt halen.

Wat ook helpt voor een strakker verloop: Zorg dat je maar één ingang en één uitgang hebt. Dat kan al heel eenvoudig door maar één e-mailadres te hebben waarnaar gemaild kan worden en dat ook altijd te gebruiken voor communicatie met mensen die hun rechten uitoefenen. Het proces loopt verreweg het meest gesmeerd in organisaties waar een zogenaamde 'desk' achter deze ene in- en uitgang bestaat – een groep mensen die zorgdragen dat administratief gezien het hele proces doorlopen wordt. En, dump dat niet op het bureau van de (vaak kleine) Privacy Office, want hen heb je nodig voor advisering bij de complexe zaken en niet voor de administratieve afhandeling. Het is simpelweg zonde om de kostbare privacykennis daarvoor in te zetten.

De derde factor die onontbeerlijk is: de organisatie heeft de datahuishouding op orde. Dit is weliswaar niet iets waar je als privacy- of securityspecialist altijd zelf actief aan kan werken, maar je kunt hier wel een belangrijke rol spelen in de behoeftestelling. Die basisorde vereist bijvoorbeeld dat er beleid is voor bewaartermijnen (die kun je schrijven) en dat dit ook geïmplementeerd is (daar zit je behoeftestelling). Meer hulp nodig? Sla er vooral ook dat onderzoek van de EDPB op na (1) – die bevat namelijk een lijst met zaken die rondom de rechten van betrokkenen in de basis op orde moeten zijn en biedt daarmee een super praktisch houvast voor de praktijk.

Rachel

(1) 2024 Coordinated Enforcement Action Implementation of the right of access by controllers, Adopted on 16 January 2025

Auteur: Nick Nieuwenhuis MSc, Cyber Security Researcher and Consultant. Feel free to reach out to nick@nicknieuwenhuis.com for any questions or inquiries

Integrating Cyber Security and Enterprise Architecture to improve Risk Management

Cyber risks have evolved from mere annoyances to catastrophic events, posing challenges for enterprises worldwide. This article highlights the findings of recent research on the integration of Cyber Security and Enterprise Architecture to Improve Cyber Risk Management, executed within the Cyber Security research centre of the Utrecht University of Applied Sciences.

As organizations take on various digital transformation initiatives to deliver value to their stakeholders, cyber security (CS) has never been more important. IBM's Ponemon institute estimates the average cost of a data breach to be at an all-time high: 4.88 million USD. Additionally, organizations must comply with growing laws and regulations, such as the renewed NIS2 directive (cyberbeveiligingswet), Cyber Resilience Act (CRA), and the Digital Operational Resilience Act (DORA). These challenges underscore the need for a holistic and integrated approach to manage cyber risks.

Enterprise Architecture (EA) can be a promising vehicle to manage these cyber risks because of its holistic capacity overarching the business, data, application and technology domains. Prior research on EA benefits highlighted that EA could improve risk management, quality management and business-and-IT alignment. Unfortunately, CS and EA are isolated departments in most enterprises, resulting in ineffective cyber risk management that keep enterprises vulnerable.

Research Method

This research aimed to bridge the gap by studying how CS and EA could be integrated, by identifying blockers and enablers for this integration. Furthermore, the research aims to understand how this integration impacts Cyber Risk Management. The central question in this research is: How can Cyber Security and Enterprise Architecture be integrated in relation to Cyber Risk Management within enterprises? To collect data, a literature review on the state-of-the-art of CS and EA integration was combined with a focus group (6 participants) and interviews (4 participants). Participants where seasoned experts in the EA and/or CS domain, from various backgrounds and had at least 10 years of professional experience. The participants were chosen to ensure a rich diversity of perspectives.

Findings

This section summarizes the most important findings of this research. Before starting in-depth questions around CS-EA integration, participants were asked to what extent CS and EA are currently integrated within enterprises based on their experience. The answer was a 3.2 on a five-point scale, which translates to 'somewhat integrated'. Participants mentioned that CS is already part of some EA frameworks, such as TOGAF and SABSA. Another participant mentioned that architects work in close collaboration with the CISO.

To validate the existing literature on CS-EA integration, participants were asked to rate six strategies for integrating CS and EA in order of perceived importance. The results and their respective score (0-100) can be found below:

1. Integrating Cyber Security into EA Frameworks (29.2)
2. Adopting the Security-by-Design paradigm (25.8)
3. Integrating business requirements with security requirements (18.4)
4. Leveraging EA to provide input for Cyber Risk Assessment (15)

5. Mapping identified cyber risks to EA components (5.8)
6. Managing cyber risks by aligning business & IT activities (5.8)

Other strategies not mentioned in literature are:

- Giving security representation in the (enterprise) architecture board
- Making security an explicit part of the architecture
- Improving Security awareness of EA professionals

Blockers

A score of 3.2 meant that there is room for improvement. Participants were asked which blockers hinder the level of integration. Three main themes emerged:

1. **Different mindsets & focus:** Both CS and EA teams work mostly in isolation and have different goals and purposes. A participant remarked: 'Enterprise Architects thinks in possibilities, while CS professionals think in limitations'
2. **Organizational misalignment:** Both departments usually report to different managers, and only 'meet' each other late in the process. Security is therefore often seen as an afterthought.
3. **Skills & knowledge gaps:** CS professionals usually do not have the architecture skills to make (strategic) decisions. EA professionals on the other hand lack the in-depth security knowledge to fully incorporate security in architectural processes and documents.

Enablers

The research also highlighted enablers that facilitate the integration of CS and EA. The main themes that emerged were:

Security integration in EA Frameworks: Security is to some extent already integrated within EA frameworks, which makes decision-making, modeling concerns and viewpoints, and establishing a common language easier.

Adopting Secure Development Methodologies: Secure software development methodologies, especially DevSecOps and Security by Design, also facilitate integration, because security measures are added upfront instead of reactively.

Security Awareness in the Business: Another enabler of the integration is rising security awareness in the business. This means more non-technical employees are aware of cyber risks, such as phishing and fraud. This makes it easier to implement security controls from an architectural standpoint.

Impact on Cyber Risk Management

Ultimately, sound integration of CS and EA impacts Cyber Risk Management. To assess how this was impacted, participants were asked to map improvements to the ISO 27005 cyber- and information security risk management process. The (perceived) improvements and their respective process step can be found below.

Context establishment: The integration of CS and EA makes it easier to identify and assess risks on the organizational and process level, including identifying supply chain risks and stakeholder dependencies.

Risk Assessment: The integration of CS and EA improves risk identification, analysis and evaluation because EA can clarify dependencies in process and technology and the risks involved.

Risk Treatment: Most improvement could be mapped to risk treatment phase, especially risk mitigation (reducing the risk to an acceptable level). CS-EA integration realizes faster and more structural solution for risk mitigation that can be reused, aligning security controls with the architecture.

Monitoring and Review: CS-EA integration makes it easier to monitor security controls for their expected and desired effects.

Overall, multiple improvements were mentioned by all research participants. Although these are qualitative statements and thus no statistically significant conclusion can be drawn upon this, it shows the promising effects of CS-EA integration and the positive impact it can have on Cyber Risk Management.

Conclusion

This research highlights that integrating security into EA frameworks, adopting secure development methodologies, improving skills and knowledge, and aligning both departments in the organizational structure can yield benefits for enterprises seeking to improve their Cyber Risk Management capabilities. Although future research is necessary to validate and extend these findings, EA shows to be a promising vehicle for managing cyber risks.

For more information, references and further reading, please find the full and free to download thesis 'Towards the Integration of Cyber Security and Enterprise Architecture to Improve Cyber Risk Management' (pdf) here.

Lessen uit de Target-hack

Eind 2013, terwijl de wereld zich voorbereidde op de feestdagen, vond een van de meest impactvolle datalekken plaats in de geschiedenis van retail. De Target-hack (Target is een Amerikaans warenhuis-red.) resulteerde in de diefstal van de betaalkaartgegevens van 40 miljoen klanten en de persoonlijke informatie van nog eens 70 miljoen mensen. Ik was een van die klanten.

Tijdens een vakantie in New Bedford (VS) gebruikte ik mijn creditcard bij een Target-winkel. Nietsvermoedend rekende ik af voor een paar eenvoudige aankopen, niet wetende dat mijn gegevens werden onderschept door malware die zich stilletjes had genesteld in Targets point-of-sale (POS)-systemen. Weken later werd ik, net als miljoenen anderen, geconfronteerd met de harde realiteit: mijn creditcardgegevens waren gestolen. Dit was voor mij gelukkig snel opgelost – ik moest mijn creditcard vervangen en waakzaam zijn voor verdachte transacties, maar de impact van de hack op Target was enorm.

Dit incident kostte Target meer dan 200 miljoen dollar, aan schadevergoedingen, juridische kosten en beveiligingsupgrades. Daarnaast schatte het bedrijf de reputatieschade in de miljarden. Wat mij toen het meest verbaasde, was hoe eenvoudig de aanval was uitgevoerd. Hackers drongen door tot Targets POS-systemen via het ongesegmenteerde bedrijfsnetwerk, na binnengekomen te zijn in een winkel via een leverancier van HVAC-diensten, een bedrijf met minder geavanceerde beveiliging.

Deze zwakke schakel in de keten maakte het voor cybercriminelen mogelijk om het netwerk van een van de grootste retailers ter wereld te infiltreren. Het incident benadrukte het belang van leveranciersbeheer, netwerksegmentatie en snelle detectie van bedreigingen. Het was een wake-upcall voor bedrijven wereldwijd, maar de vraag bleef: Welke lessen zou het bedrijfsleven hieruit leren?

Nu, een decennium na de Target-hack, en met een SolarWinds incident erbij in 2020, lijkt de wereld eindelijk de lessen van het verleden ter harte te nemen. Leveranciersbeveiliging ontwikkelt zich naar een kernonderdeel van bedrijfsvoering en beveiligingsraamwerken. Ik constateer dat we flink aan het verbeteren zijn:

- **Leveranciersbeheer is prioriteit** – Veel organisaties hebben systemen ingevoerd om leveranciersrisico's beter te documenteren en te beheren. Leveranciers moeten nu voldoen aan strengere eisen en regelmatige audits ondergaan.
- **Verbeterde regelgeving** – Europese regelgeving zoals NIS2 en de AVG verplichten bedrijven om bedrijfsinformatie en persoonsgegevens beter te beschermen. Er is gericht toezicht op de naleving hiervan.
- **Zero Trust-beveiligingsmodellen** – Zero Trust heeft een prominente rol gekregen. Organisaties segmenteren hun netwerken en beperken toegang tot alleen wat strikt noodzakelijk is. Tooling om dit te doen werkt beter.
- **Proactieve detectie en respons** – Moderne beveiligingstechnologieën maken gebruik van AI en machine learning om bedreigingen vanuit leveranciers sneller te detecteren en aan te pakken. Managed dienstverlening op dit vlak is nu standaard.

Toen mijn creditcardgegevens in 2013 werden gestolen bij Target, leek dit een onfortuinlijk, maar geïsoleerd, incident te zijn. Nu, ruim tien jaar later, wordt er structureel gekeken naar de beveiliging van leveranciers. Er zijn structurele verbeteringen doorgevoerd om leveranciersrisico's te beheersen.

Soms gaat verandering niet zo snel als we dat zouden willen. Het leek toen ook alsof er weinig mee gedaan werd, maar terugkijkend constateer ik dat we toch wel tevreden mogen zijn met de ontwikkelingen in leveranciersbeheer, regelgeving en technische maatregelen.

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

Auteur: Dr. J. Kwik is onderzoeker internationaal recht bij het Asserinstituut in Den Haag.

Civiele sector in het vizier van de agressor

Google's recente besluit (1) om het verbod op AI-ontwikkeling voor militaire doeleinden te schrappen, stelt onderzoekers en ontwikkelaars in de technologiesector voor een uitdaging: hoe houden ze afstand van het militaire domein? Veel experts (2) geven de voorkeur aan die scheiding. Uit een recente peiling van ELSA Lab Defence (waar de auteur bij betrokken was) blijkt dat de meerderheid van AI-onderzoekers in Nederland persoonlijk bezwaar heeft tegen defensieve AI-toepassingen, zoals autonome (cyber)wapens en doelbestrijdingssoftware.

Het komt regelmatig voor dat AI-gerelateerd onderzoek een militair staartje krijgt. Waar in het verleden innovaties vaak ontstonden in een militaire context en vervolgens hun toepassingen vonden in de civiele sfeer (zoals de mobiele telefoon of de magnetron), is de situatie nu omgekeerd: defensie leert, leent en bouwt voort op producten uit de civiele sector. Denk hierbij aan openbaar beschikbare grote taalmodellen (LLM), die getraind worden tot militair-operationele planningsadviseurs (3).

Civiele sector doelwit

De civiele en militaire AI-ecosystemen raken steeds verder met elkaar verweven, en dat heeft consequenties voor dreigingen waar privébedrijven rekening mee zullen moeten houden. Momenteel zijn cyber- en informatieaanvallen in het kader van hybride conflicten zoals in Oekraïne (4) nog voornamelijk gericht tegen militaire of publieke installaties; digitale spionageoperaties tegen inlichtingendiensten of cyberaanvallen tegen energienetwerken. De toekomst zal leren dat ook de civiele sector een steeds aantrekkelijker doelwit wordt voor vijandelijke machten.

Om hier een voorbeeld van te noemen: stel dat partij X als doel heeft om de militaire planningsadviseur van tegenstander Y te saboteren. Eén optie is om Y's software te beschadigen met een virus. Dit heeft weinig kans van slagen, aangezien de software zich in een gesloten en beveiligd militair netwerk bevindt. Het alternatief viseert een gemakkelijker doelwit: de database van de LLM-ontwikkelaar waar de planningsadviseur op is gebaseerd. Door het injecteren van vergiftigde exemplaren in de dataset of het installeren van een backdoor in het LLM-model, kan X het eindproduct compromitteren (5) zonder ooit Y's beveiligde netwerk te hoeven hacken. Slachtoffer: de LLM-ontwikkelaar en de burgers die ook gebruikmaken van deze LLM.

Het tweede voorbeeld: AI is in staat hele verfijnde en doelgerichte desinformatie en cognitieve aanvallen (6) te genereren tegen personen, zolang er voldoende data beschikbaar is over de gedachtenpatronen en voorkeuren van deze persoon. Dit maakt het hacken van brain-computer interfaces (BCI) (7) zoals Neuralink, een aantrekkelijke strategie: dergelijke apparaten slaan immers continu de breinsignalen van de drager op. Slachtoffer: de drager van de BCI en het geassocieerde bedrijf.

Begrip voor nieuwe dreiging

Voor onderzoekers en ontwikkelaars wordt het steeds moeilijker om zich af te zonderen van de lange arm van het moderne slagveld. De verstrengeling tussen militair en civiel zal ervoor zorgen dat zelfs als een bedrijf het militaire domein niet opzoekt, laatstgenoemde hem toch zal vinden. Van belang is daarom dat deze nieuwe dreigingen begrepen worden en in acht worden gehouden, zelfs als de technologie op het eerste gezicht weinig te maken lijkt te hebben met defensie – zoals het voorbeeld van BCI's laat blijken.

De auteur is onderzoeker internationaal recht bij het Asser Instituut in Den Haag. In een latere uitgave verschijnt een uitgebreider artikel van zijn hand over de rol van drones, AI, desinformatie en andere digitale technieken op het slagveld, inclusief de bijbehorende ethische vraagstukken. Dit artikel dient alvast als smaakmaker.

Referenties

(1) https://www.nu.nl/tech/6344877/google-schrapt-verbod-op-het-gebruik-van-zijn-ai-voor-wapens.html
(2) https://nypost.com/2025/02/06/business/google-may-use-ai-for-weapons-surveillance-prompts-backlash/
(3) https://defensescoop.com/2024/11/04/scale-ai-unveils-defense-llama-large-language-model-llm-national-security-users/
(4) https://www.rodekruis.nl/nieuwsbericht/trollen-en-hackers-zo-werkt-vechten-in-een-cyberoorlog/
(5) https://lieber.westpoint.edu/anti-ai-countermeasures-warfare-terra-incognita-ihl/
(6) https://www.ie.edu/insights/articles/cognitive-war-turns-the-mind-into-battle-ground/
(7) https://www.aria.org.uk/opportunity-spaces/scalable-neural-interfaces

Auteur: Marijke Stokkel, senior manager cybersecurity, BDO cybersecurity, marijke.stokkel@bdo.nl en Eddie Versluis, dreigingsanalist, BDO cybersecurity, eddie.versluis@bdo.nl

Cybercriminelen gaan publiek: jouw data, hun verhaal

Wat begint als een normale werkdag bij Uber, neemt een onverwachte wending als een melding binnenkomt op de interne chatapp Slack. 'I announce I am a hacker and Uber has suffered a data breach'. Medewerkers nemen het bericht aanvankelijk niet serieus en reacties stromen binnen: emoji's van popcorn en sirenes, de beroemde 'It's happening'-gif. Ubermedewerkers communiceren met de aanvaller in de veronderstelling dat het een grap is.

'Sorry dat ik de pretbederver moet zijn,' schrijft een medewerker, 'maar ik denk dat IT liever minder memes ziet terwijl ze de hack proberen op te lossen.' Het is inderdaad geen grap. De aanvaller probeert, zoals later blijkt een jongen van 18 jaar met op de darkweb-marktplaats gekochte inloggegevens, in te loggen op Uber's netwerk. Als hij wordt geblokkeerd door een extra beveiligingslaag (MFA), doet de aanvaller zich via WhatsApp voor als een medewerker van Uber's beveiligingsteam. Hij vraagt de betreffende medewerker een van de MFA-verzoeken goed te keuren vanwege 'verdachte activiteiten'. Na een vloedgolf aan meldingen geeft de medewerker toe. De aanvaller krijgt toegang tot het interne VPN, vindt de inloggegevens van een beheeraccount en heeft daarmee vrijwel onbeperkte toegang tot meerdere essentiële systemen (1). Naast de chatuitwisseling met Ubermedewerkers, bespreekt de aanvaller zijn acties ook met journalisten en een security-onderzoeker.

Uber heeft geluk dat het de aanvaller alleen om de kick gaat en hij geen systemen vernietigt of versleutelt. Maar een PR-ramp is het wel. De aanval wordt al snel opgemerkt door de media en de besmuikte reacties zijn niet van de lucht. 'It's a big deal, and an embarrassment to the company', schrijft gerenommeerd security-expert Bruce Schneier (2). De aandelen Uber openen de volgende dag flink lager (3).

Negatief framen

Wat opvalt aan deze casus is niet alleen hoe MFA-pushberichten zo hinderlijk kunnen worden dat het doelwit uiteindelijk toegeeft, maar ook dat de aanvaller Ubermedewerkers via Slack benadert en journalisten inschakelt om het nieuws te verspreiden. Het feit dat aanvallers niet alleen hun primaire doelwit aanvallen, maar ook stakeholders en de media erbij betrekken, is een relatief nieuw fenomeen (4).
Voor veel organisaties is dit dan ook een onbekende situatie. Tijdens onze cybercrisisoefeningen zien we geregeld dat crisisteams reageren met: 'We communiceren voorlopig niets' of 'We melden alleen een storing.' Ten onrechte denken ze dat zij bij een aanval controle hebben over de inhoud en timing van communicatie. Dit terwijl in het scenario van de oefening de aanvallers dan al een bericht over de succesvolle inbreuk op het darkweb hebben gezet. In het algemeen geldt dat als aanvallers als eerste berichten en de aanval negatief framen, bijsturen heel moeilijk is. Organisaties moeten beseffen dat hackaanvallers niet alleen hen, maar ook hun stakeholders direct kunnen benaderen en tevens publiekelijk over de aanval kunnen communiceren. Laten we deze strategie verder verkennen.

Nationale schokgolf

Ransomwareaanvallers benaderen vaak klanten, patiënten of medewerkers om extra druk te zetten. Dat gebeurde bijvoorbeeld in oktober 2020 in Finland. Duizenden Finnen kregen de schrik van hun leven toen ze een afpersingsmail ontvingen. Vastaamo, hun psychotherapiekliniek, bleek slachtoffer van een grote cyberaanval waarbij de complete patiëntendatabase werd buitgemaakt. Alle gegevens waren gestolen, waaronder informatie over angstaanvallen, overspel, pedofiele gedachten en zelfmoordpogingen van patiënten. Nadat het bedrijf weigerde losgeld te betalen, richtte de aanvaller zich op de patiënten. Binnen 24 uur moesten ze 200 euro in bitcoin betalen. Wie weigerde, liep het risico dat gegevens gepubliceerd zouden worden. Binnen korte tijd verschenen de eerste dossiers online, waaronder die van politici en andere publieke figuren (5).
De aanval veroorzaakte een nationale schokgolf in Finland vanwege de grootschaligheid van het lek en de ernst van de gestolen informatie. Minstens één zelfdoding werd aan het datalek gekoppeld. Vastaamo ging failliet en de CEO werd strafrechtelijk vervolgd omdat hij een eerder datalek verzweeg en het bedrijf onvoldoende beveiligde tegen cyberaanvallen.

Data leak sites

Ransomwaregroepen gebruiken ook eigen kanalen om een breder publiek te bereiken. Sinds enkele jaren creëren zij data leak sites (DLS) op het darkweb. Op deze platforms publiceren ze gestolen gegevens of dreigen ze daarmee, als onderdeel van hun afpersingsstrategie. Bij uitblijvende betalingen volgen meer bestanden. Veel DLS hebben aftelklokken die aangeven wanneer data vrijkomt of geven korting bij de eerste kopers van gestolen data. Op sommige platforms is de data doorzoekbaar. Andere bevatten persberichten en FAQ's die de informatie zo laagdrempelig mogelijk beschikbaar maken voor derden. Journalisten spelen hier gretig op in. In januari 2025 berichten meerdere media, waaronder techwebsite Tweakers, dat ransomwarebende Cl0p data van IT-dienstverlener Centric op hun DLS heeft geplaatst (6). Dit dwingt Centric vervolgens om publiek te reageren.

Eerlijke pentesters

Ransomwaregroepen begrijpen goed dat hun activiteiten nieuwswaardig zijn en spelen daar handig op in. Door succesvolle aanvallen aan te kondigen, demonstreren ze hun capaciteiten en vergroten ze hun dreiging naar toekomstige slachtoffers.
Ransomwaregroepen gebruiken DLS ook als recruitmentmiddel. Hoge losgeldbedragen op DLS geven ransomwaregroepen een reputatie bij andere cybercriminelen. Door de wereld van ransomware als cool en lucratief voor te spiegelen, proberen ze

Besef dat hackaanvallers niet alleen jou, maar ook jouw stakeholders direct kunnen benaderen en publiekelijk over de aanval kunnen communiceren

meer leden en samenwerkingspartners aan te trekken (7).
Tot slot gebruiken ransomwaregroepen DLS om een bepaald narratief uit te dragen. Ze presenteren zichzelf als 'eerlijke pentesters' die 'cybersecurityonderzoek' uitvoeren. Sommige bieden getroffen organisatie aan om een rapportage op te leveren over hoe ze zijn binnengekomen en hoe dit voortaan voorkomen kan worden (vaak door een update uit te voeren op het kwetsbare systeem). Deze groepen proberen hun acties goed te praten door hun doelwitten af te schilderen als onverantwoordelijk of nalatig. Een FAQ op de leak site van ransomwaregroep 8Base geeft dit treffend weer.

Q: 'I am (was) a client of a company found in your list and became a victim of their irresponsible processing of my personal data and business secrets. What can I do?'
A: 'First of all, we find it necessary to say we are sorry that you were affected by companies 'negligent attitude to the privacy and security of their customers' personal data. But there is a bright side, because it gives you the opportunity to request compensation from such companies' (8).

Je hoeft overigens niet naar het darkweb voor informatie over hackaanvallen. Cybercriminelen promoten hun DLS ook via forums en sociale media op het 'gewone' internet. Daarnaast verzamelen platforms als Ransomware.live via het open source project Ransomwatch gegevens van meerdere DLS en maken die beschikbaar voor een breder publiek.
Hackaanvallers communiceren dus actief over hun aanvallen. Hoe moet je hier als getroffen organisatie mee omgaan? Een aantal tips.

• Wees er snel bij

Als het niet lukt de aanvallers vóór te zijn, zorg dan in elk geval dat je direct op de hoogte bent zodra jouw organisatie op het darkweb verschijnt. Monitor het darkweb in real-time - een logische taak voor het Security Operation Center (SOC). Houd niet alleen je eigen organisatie in de gaten, maar ook leveranciers en samenwerkingspartners met toegang tot jouw data. Zo bleek bij het eerdergenoemde datalek van Centric, data van opdrachtgever gemeente Amersfoort te zijn betrokken.

• Communiceer als eerste

Breng slecht nieuws zelf als eerste naar buiten. Zo houd je controle en bepaal je het narratief, een strategie die bekend staat als stealing thunder. Wacht niet tot er data op een DLS verschijnt. Zodra je weet dat vertrouwelijke gegevens zijn buitgemaakt, is openheid cruciaal. Dit geldt in het bijzonder voor gegevens van derden, zoals klant- of partnerdata. Stakeholders waarderen het wanneer een organisatie verantwoordelijkheid neemt, dat vergroot het vertrouwen. Bovendien vermindert proactieve communicatie de kans dat aanvallers of de pers een ongunstig frame neerzetten, wat moeilijk te corrigeren is.

• Zet de meest getroffenen op de eerste plaats

Sommige organisaties stellen tijdens een crisis hun eigen reputatie boven alles, maar dat werkt vaak averechts. Het oogt egoïstisch en komt onbetrouwbaar over. Richt je in plaats daarvan op de echte getroffenen - zoals mensen van wie gegevens zijn gelekt of medewerkers die niet kunnen werken. Ondersteun hen met concrete acties en transparante communicatie. Een crisis draait om hún belang, niet dat van de betrokken organisatie. Oprechte, empathische communicatie met de meest getroffenen versterkt het vertrouwen en toont verantwoordelijkheid.

Cybercriminelen zoeken steeds vaker de openbaarheid. Weet hoe ze te werk gaan en wees voorbereid.

Referenties

(1) https://www.theverge.com/2022/9/16/23356213/uber-hack-teen-slack-google-cloud-credentials-powershell
(2) https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html
(3) https://investorplace.com/2022/09/uber-stock-falls-5-on-major-cybersecurity-breach/
(4) https://news.sophos.com/en-us/2023/12/13/press-and-pressure-ransomware-gangs-and-the-media/
(5) They Told Their Therapists Everything. Hackers Leaked It All | WIRED
(6) Data van Centric verschijnt op de site van ransomwarebende - Computer - Nieuws - Tweakers
(7) Press and pressure: Ransomware gangs and the media – Sophos News
(8) https://news.sophos.com/en-us/2024/08/06/turning-the-screws-the-pressure-tactics-of-ransomware-gangs/

COLUMN NICOLE

Encryptie is de oplossing, niet het probleem

Toen ik jaren geleden bij Europol werkte, bevond ik me regelmatig in het moeras van de discussie over encryptie. Het was een taaie, eindeloze strijd. Opsporingsdiensten willen toegang tot versleutelde communicatie om criminelen op te sporen, terwijl gebruikers hun recht op privacy willen beschermen. Het woord balans kwam veelvuldig ter sprake, maar dit was slechts een sympathieke term die goed klonk op papier maar waardeloos was in de praktijk. Als het gaat om encryptie is het kiezen of delen. Soms zijn dingen nu eenmaal wél zwart-wit, hoe graag beleidsmakers het ook anders zouden willen zien.

Dit thema dook recent opnieuw op toen Catherine de Bolle, de executive director van Europol, een oproep deed aan big tech – een herhaling van een strijdtoneel dat ik al zo goed ken. Ze was onderweg naar Davos en zal ongetwijfeld door haar adviseurs ingefluisterd zijn dat het een goed moment was om dit onderwerp weer aan te kaarten. Big tech heeft immers een imagoprobleem en Europol lijkt daar graag op mee te willen liften.

De Bolle stelde dat bedrijven meer moeten doen om opsporingsdiensten te helpen, en dat het een 'sociale verantwoordelijkheid' was. Zouden de bedrijven dit niet doen, dan zouden zij het risico lopen de democratie te ondermijnen. Op basis van alles wat ik tot nu toe gezien heb, betwijfel ik ten zeerste of dit argument enig effect zal hebben. Sterker nog: aangezien al vanuit zoveel verschillende hoeken wordt geroepen dat big tech de democratie en democratische processen ondermijnt, lijkt het mij dat de bedrijven inmiddels immuun zijn voor dit soort aantijgingen – als ze dat al niet waren vanaf het begin.

Ik zie daarnaast een ander probleem met de uitspraak van de executive director: toegeven aan de wens van opsporingsdiensten om toegang te krijgen, is juist ondermijnend. Encryptie beschermt de communicatie en gegevens van alle gebruikers – inclusief criminelen. Maar dat is de prijs van vrijheid én de sleutel tot veiligheid, want zonder encryptie zijn álle gegevens kwetsbaar voor kwaadwillenden.

Ik begrijp hoe groot de uitdaging is voor opsporingsdiensten. Maar als zij dan toch een appèl doen op big tech, waarom niet vragen om meer actie op een andere manier? Meta ondernam vorig jaar eindelijk stappen om tieners te beschermen tegen sextortion, na groeiende druk om iets te doen. Zo lanceerde Instagram een campagne in samenwerking met organisaties zoals NCMEC en Thorn om jongeren en hun ouders bewust te maken van sextortion-scams en hoe ze deze kunnen vermijden. Daarnaast introduceerden ze nieuwe maatregelen, zoals het wereldwijd uitrollen van een nudity protection-functie, het blokkeren van screenshots van bepaalde afbeeldingen in privéberichten, en het verbergen van volglijsten voor mogelijke scammers. Zulke acties tonen aan dat big tech verantwoordelijkheid kan nemen zonder de rechten van gebruikers aan te tasten.

De discussie over encryptie zit al jaren muurvast. In plaats van te blijven hameren op dezelfde spijker, wordt het tijd om alternatieve manieren te zoeken om criminaliteit te bestrijden. Die zoektocht is overigens niet uitsluitend de taak van opsporingsdiensten – zij zijn primair gericht op opsporing, dit gaat om innovatie. Deze zoektocht is een maatschappelijke verantwoordelijkheid. Encryptie is niet het probleem. Het is de oplossing. Het beschermt ons in een digitale wereld waarin gegevens het goud zijn voor kwaadwillenden. Het lijkt alsof we steeds opnieuw moeten kiezen tussen vrijheid en veiligheid, maar dat is een vals dilemma. De echte vraag is of we bereid zijn te investeren in beide – om zowel onze rechten als onze samenleving te beschermen.

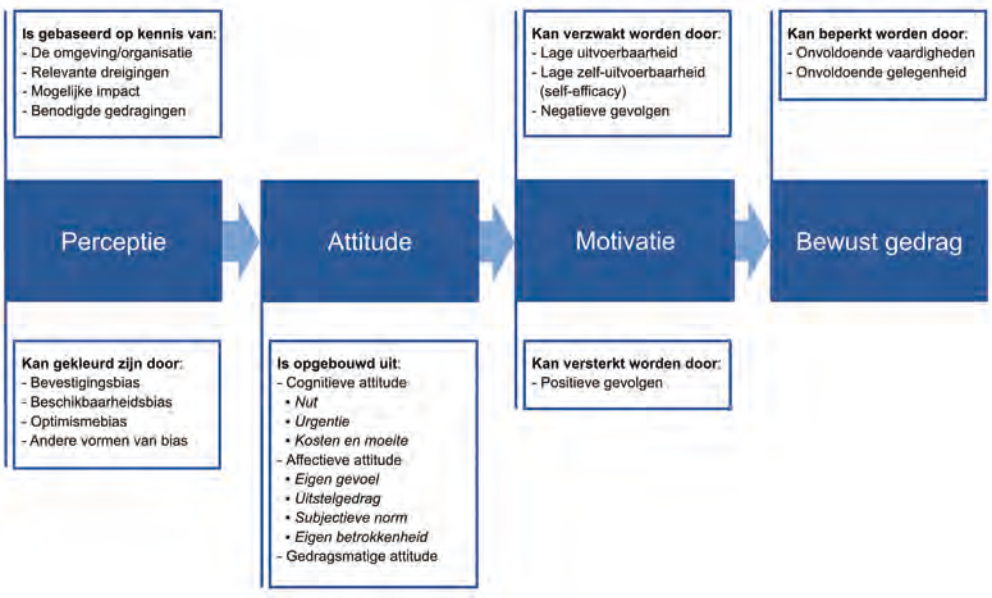
Dr. Nicole van der Meulen is expert op het gebied van cybersecurity en emerging technologies en werkzaam bij SURF als Cybersecurity Innovation Lead, ns.vandermeulen@gmail.com

Auteurs: Marcel Spruit is Lector Cybersecurity aan het Kenniscentrum Cybersecurity van de Haagse Hogeschool in Den Haag. Hij is te bereiken op m.e.m.spruit@hhs.nl. Céline Kreffer was ten tijde van het onderzoek, waarop deze publicatie is gebaseerd, Onderzoeker Cybersecurity aan het Kenniscentrum Cybersecurity van de Haagse Hogeschool. Inmiddels is zij Analist Bestuurlijke Informatie bij het Ministerie van Justitie en Veiligheid in Den Haag.

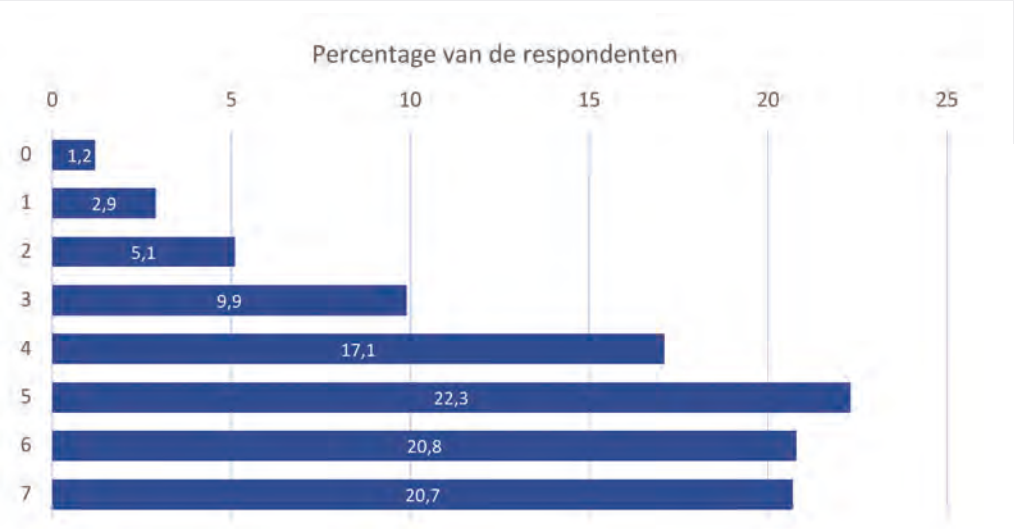
Veldonderzoek naar (on)veilig gedrag

Het is waardevol om een praktisch en wetenschappelijk onderbouwd model te hebben om menselijk gedrag – en de fouten daarin – te verklaren. Maar zo'n model bevat veel factoren. Welke daarvan zijn relevant voor veilig gebruik van mobiele digitale media, zoals smartphones en laptops? In dit artikel bespreken we de belangrijkste factoren en hoe we hier in de praktijk mee om kunnen gaan.

In de informatiebeveiliging wordt de mens beschouwd als zwakke factor. Dit is niet geheel onterecht, want mensen maken fouten, veel fouten. Sommige mensen maken meer fouten dan anderen. Fouten worden echter lang niet altijd veroorzaakt door degenen die in de fout gaan, want ook de omgeving, bijvoorbeeld de organisatie waar iemand werkzaam is, kan fouten in de hand werken of de impact ervan verergeren. In ons vorige artikel (1) hebben we een wetenschappelijk gefundeerd gedragsmodel gepresenteerd, zie figuur 1. En bovendien hebben we laten zien dat dit model gebruikt kan worden voor het stapsgewijs aanpakken van fouten in informatieveilig gedrag van medewerkers in een organisatie.



Figuur 1: Gedragsmodel met factoren (2).



Figuur 2: De uitvoering van O tot 7 veilige gedragingen.

Het model bevat nogal wat factoren en deelfactoren die het gedrag van iemand kunnen beïnvloeden. Dat doet de vraag rijzen of in de praktijk al die factoren wel van belang zijn of dat we slechts met één of een paar factoren rekening hoeven te houden.

Aanpak

Om bovenstaande vraag te kunnen beantwoorden, hebben we een veldonderzoek gedaan op basis van een breed uitgezette enquête over veilig gedrag met persoonlijke, mobiele, digitale media, zoals smartphones en laptops (2). Een aantal factoren uit figuur 1 zijn in dat geval dan niet van belang, zoals lage uitvoerbaarheid en onvoldoende gelegenheid.

Aangezien vragenlijsten in gangbare enquêtes niet de duidelijke antwoorden zouden opleveren die we wilden hebben, hebben we voor onze enquête een nieuw type vragenlijst opgesteld waarin we zowel naar het gedrag van de respondent in het afgelopen jaar vroegen, als naar de verklaring die de respondent daar zelf voor geeft. Voor het gedrag hebben we, op basis van relevantie en geschiktheid voor ons onderzoek, gekozen voor de volgende gedragingen:

1. verschillende wachtwoorden gebruiken;
2. beveiligingssoftware installeren;
3. VPN gebruiken;
4. privacy-instellingen voor software checken en zo nodig aanpassen;
5. toegang tot gevoelige gegevens op sociale media beperken;
6. onnodige cookies weigeren of aanpassen en
7. de locatiedienst uitzetten als deze niet nodig is.

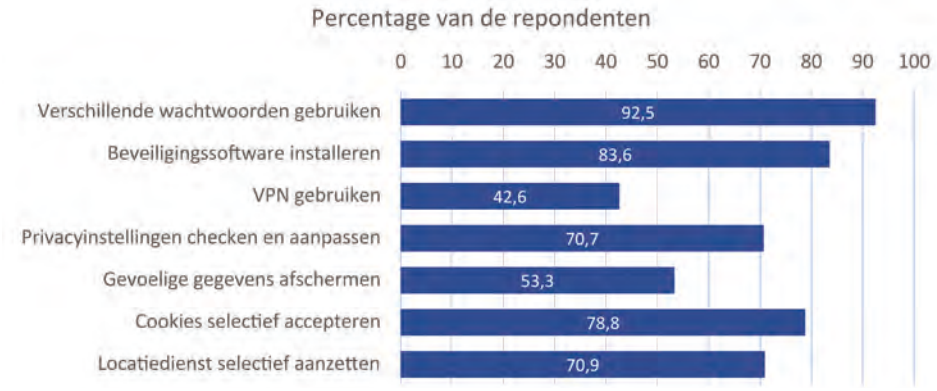
Uit vooronderzoek met respondenten waarvan het gedrag bij de onderzoekers bekend was, bleek dat respondenten hun eigen gedrag van het afgelopen jaar goed kunnen reproduceren, als dit gedrag gekoppeld is aan voor hun goed herkenbare beslissingen of activiteiten. Ook bleek dat de respondenten in een anoniem onderzoek in het algemeen eerlijk zijn over hun gedrag. We gaan er dan ook vanuit dat de antwoorden van de respondenten overeenkomen met hun feitelijke gedrag. Bovendien werd aan de respondenten gevraagd naar de verklaring die ze zelf geven voor hun gedrag. Uit het vooronderzoek bleek dat het voor respondenten moeilijk is om de psychologie achter hun eigen gedrag te verklaren. Daarom hebben we een lijst met herkenbare beweringen opgesteld waaruit de respondenten per gedraging de voor hun best passende beweringen konden kiezen. Dat bleek goed te werken. Op basis van de gemaakte keuzes konden de onderzoekers vervolgens bepalen welke gedragsbeïnvloedende factoren aan zet waren geweest. De enquête is anoniem uitgezet bij Nederlanders van twintig jaar en ouder. De respons kwam van 1.000 mensen, die samen een goede afspiegeling vormden van de Nederlandse samenleving van twintigplus (3).

Bevindingen

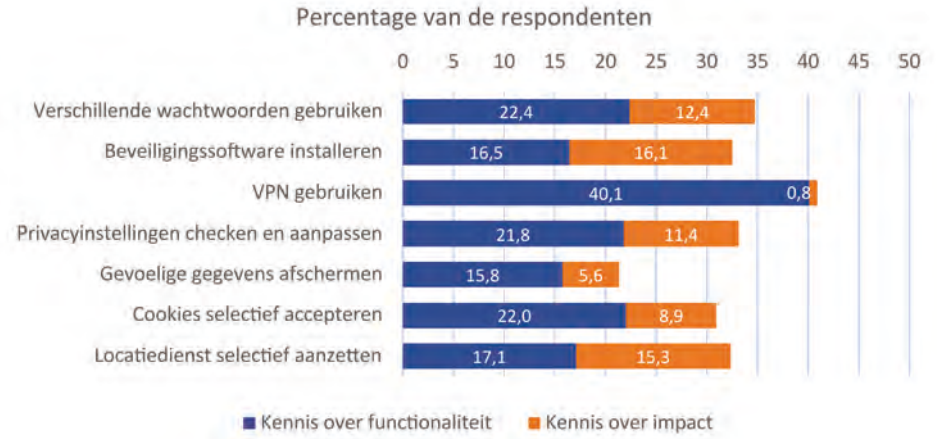
De resultaten van de enquête laten zien dat ongeveer 80% van de respondenten niet alle bevraagde veilige gedragingen uitvoeren, zie figuur 2. Ongeveer één procent van de respondenten gaf zelfs aan dat ze geen enkele hiervan uitvoerde.

De populariteit van de bevraagde veilige gedragingen verschilt aanzienlijk, zie figuur 3. Met name het gebruik van een VPN en het afschermen van gevoelige gegevens op sociale media komen er bekaaid vanaf. In figuur 4 zien we voor welk percentage van de respondenten het gemis aan de benodigde kennis de oorzaak was om een gegeven gedraging niet te doen. Hierbij maken we per gedraging onderscheid tussen twee deelfactoren, namelijk het niet weten wat de gedraging behelst (functionaliteit) en het missen van inzicht in de potentiële impact van het al dan niet doen van de gedraging. In de figuur zien we dat beide deelfactoren de oorzaak kunnen zijn van het niet uitvoeren van veilige gedragingen.

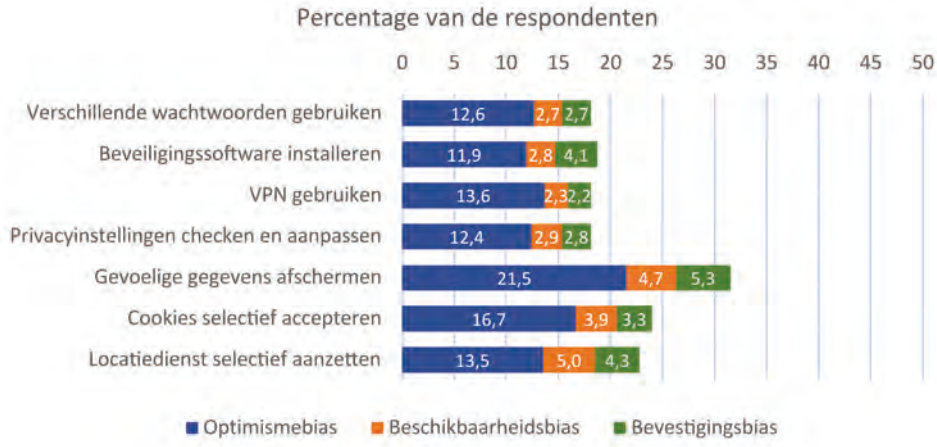
Degenen die een bepaalde gedraging en de impact ervan wel kennen, kunnen toch een door bias vertekende perceptie hebben. We maken per veilige gedraging onderscheid in optimisme-, beschikbaar-



Figuur 3: De uitvoering van veilig gedrag.



Figuur 4: Ontbreken van kennis als oorzaak voor nalaten veilig gedrag.

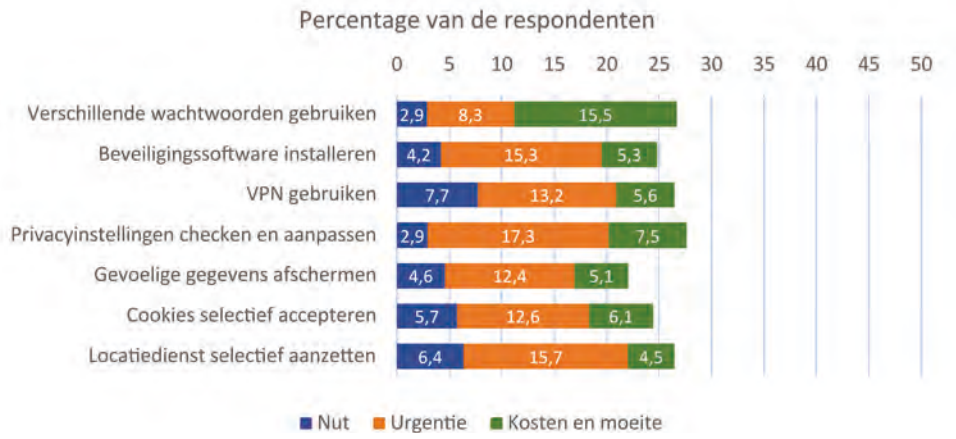


Figuur 5: Bias als oorzaak voor uitblijven veilig gedrag.

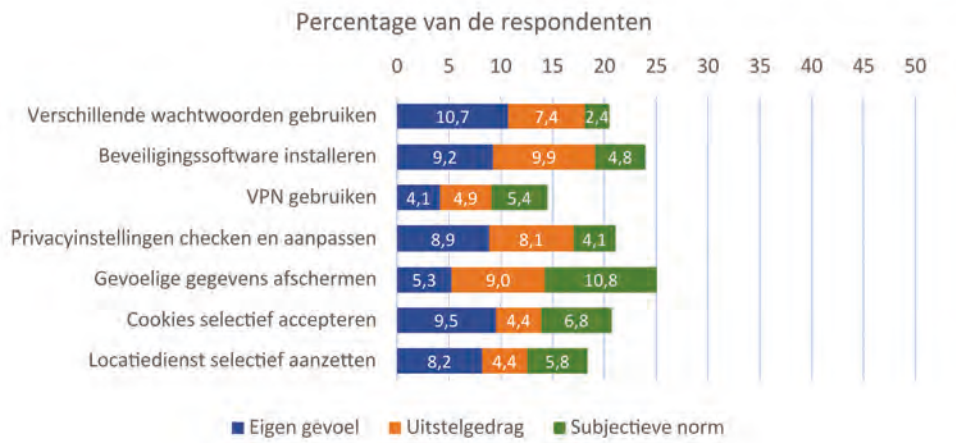
heids- en bevestigingsbias. In figuur 5 zien we alle drie vormen van bias, welke een oorzaak kunnen zijn - vooral optimismebias - voor het niet uitvoeren van veilige gedragingen. Als de perceptie in orde is, dan kan de attitude de oorzaak zijn van het niet uitvoeren van veilige gedragingen. Ten eerste de cognitieve attitude die een aantal rationele deelfactoren omvat, te weten; de mening over het nut van: de gedragingen, het gevoel van urgentie voor het uitvoeren van de gedragingen alsook de kosten en moeite die gemoeid zijn met het uitvoeren van de gedragingen. In figuur 6 zien we dat al deze deelfactoren een oorzaak kunnen zijn van het niet uitvoeren van veilige gedragingen.

Ten tweede de affectieve attitude die een aantal gevoelsmatige deelfactoren omvat, te weten: het eigen gevoel (onderbuikgevoel), het uitstelgedrag en de subjectieve norm. In figuur 7 zien we dat alle drie de deelfactoren een oorzaak kunnen zijn voor het niet uitvoeren van veilige gedragingen.

Als we de gegevens uit de figuren 4 tot en met 7 met elkaar combineren, zie figuur 8, dan zien we dat er onderlinge verschillen zijn tussen de invloed die de verschillende factoren uitoefenen op de bevraagde gedragingen. Het gemis van relatief vaak de



Figuur 6: Cognitieve attitude als oorzaak van nalaten van veilig gedrag.



Figuur 7: Affectieve attitude als oorzaak van nalaten van veilig gedrag.

oorzaak van het niet uitvoeren van gedragingen. Dit speelt met name bij het niet gebruiken van VPN. Uit figuur 4 kunnen we opmaken dat het daarbij vooral gaat over functionaliteitskennis. Bij het niet goed beschermen van gevoelige gegevens op sociale media speelt met name bias een rol. Uit figuur 5 kunnen we opmaken dat het vooral de optimismebias betreft. Het meest opvallende in figuur 8 is echter dat geen van de factoren onbelangrijk blijkt te zijn. Alle factoren spelen in de praktijk een rol van betekenis. In de figuren 4 tot en met 7 zien we dat dit ook geldt voor de deelfactoren.

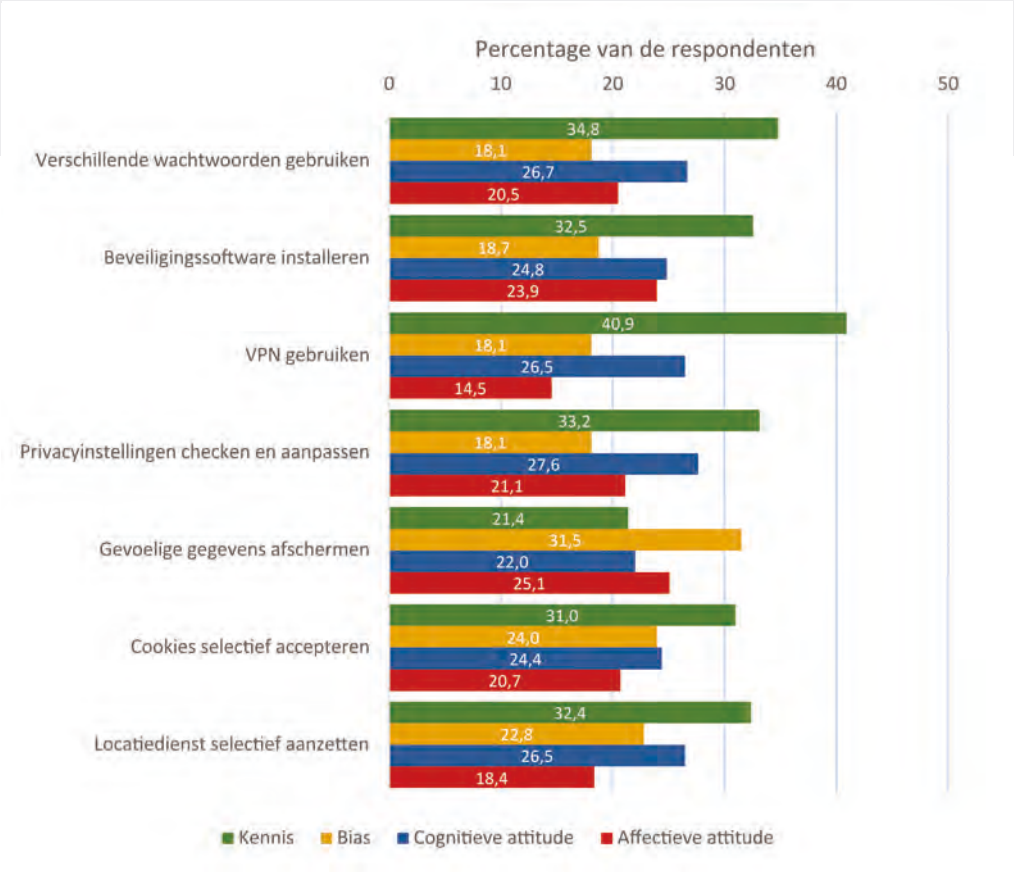
Implicaties voor organisaties

In de vorige paragraaf hebben we gezien dat alle bevraagde gedragsbeïnvloedende factoren een duidelijke invloed op veilig gedrag kunnen hebben. Aangezien iedere factor voor het verbeteren ervan om een specifieke aanpak vraagt, zijn er meerdere verschillende aanpakken nodig. Zo kan bijvoorbeeld iemands kennis worden verbeterd door de betreffende persoon een cursus te laten volgen. Bias kan bijvoorbeeld worden aangepakt door de betreffende persoon een simulatie of spel te laten doen, waardoor de persoon een beter beeld krijgt van de werkomgeving en de daarin relevante risico's en benodigde gedragingen (4). De cognitieve attitude, oftewel de mening die iemand heeft over het nut en de urgentie van het benodigde gedrag en de kosten en de moeite die daarvoor nodig zijn, kan bijvoorbeeld worden verbeterd door de informatiebeveiligingsmaatregelen in de organisatie goed in te richten en het daarvoor benodigde gedrag te integreren in de dagelijkse werkprocessen (5). De affectieve attitude, oftewel iemands eigen gevoel, uitstelgedrag, subjectieve norm en eigen betrokkenheid, kunnen bijvoorbeeld worden verbeterd door peers in te schakelen en medewerkers te betrekken bij informatiebeveiligingszaken (6,7). Hieronder is per gedragsbeïnvloedende factor aangegeven welke aanpakken daarbij passen (4,5,6,7). De opsomming beoogt niet volledig te zijn, maar geeft voor iedere factor één of meer geschikte aanpakken voor verbetering. De (deel)factoren die in cursief zijn weergegeven, zijn niet in de enquête meegenomen, omdat ze niet relevant zijn voor de veilige omgang met persoonlijke mobiele digitale media. Maar binnen een organisatie zijn ze wel relevant.

Gedragsbeïnvloedende factoren en bijpassende verbeteringen (4,5,6,7).

Kennis

- Functionaliteit:
  - Laat de medewerkers die het betreft één of meer relevante



Figuur 8: De relatieve invloed van de factoren op al of niet veilig gedrag.

cursussen volgen en toets of de benodigde kennis er daarna wel is.

- Impact:
  - Voorzie de medewerkers van relevante informatie met betrekking tot de informatiebeveiliging. Voor een manager kunnen dat bijvoorbeeld test-, audit- en incidentrapportages zijn.
  - Laat interne of externe autoriteiten de medewerkers uitleggen wat de impact van bedreigingen kan zijn. Voor een uitvoerend medewerker kan diens manager dit oppakken. Voor een strategisch manager kan dit de CISO, de auditor, of de toezichthouder dit oppakken.

Bias

- Bevestigings¬-, beschikbaar¬heids-, of optimismebias:
  - Geef de medewerkers die het betreft inzicht in hun bias zodat ze deze kunnen bijstellen. Hiervoor kunnen ze daarvoor bedoelde simulaties of spellen doen, waarin ze leren om hun werkomgeving en de daarin relevante risico's en het benodigde gedrag beter in te schatten.

Cognitieve attitude

- Nut:
  - Implementeer de beveiligingsmaatregelen zodanig dat ze effectief en logisch zijn voor alle medewerkers die ermee te maken hebben.
- Urgentie:
  - Laat managers en ervaren collega's de medewerkers uitleggen welke maatregelen waarom en wanneer nodig zijn en wat er kan gebeuren als de maatregelen niet of niet goed worden uitgevoerd. Om dat te staven, dienen de managers en ervaren collega's zelf het goede voorbeeld te geven.
- Kosten en moeite:
  - Integreer het voor informatiebeveiliging benodigde gedrag in de 'gewone' werkprocessen zodat het uitvoeren van beveiligings¬maatregelen een natuurlijk onderdeel van het 'gewone' werk is.
  - Implementeer de beveiligingsmaatregelen zodanig dat daarvoor geen onnodig lastig of tijdrovend gedrag nodig is.

Affectieve attitude

- Eigen gevoel, Uitstelgedrag:
  - Verlaag drempels voor het uitvoeren van de benodigde beveiligingsmaatregelen en richt de maatregelen in als 'hapklare brokken'.
  - Werk in teams waarin een sfeer ontstaat van 'we doen dit samen'.
  - Pas (zachte) dwang toe om de medewerkers die het betreft te stimuleren de benodigde maatregelen direct uit te voeren.
  - Beloon goed gedrag.
- Subjectieve norm:
- Schakel gewaardeerde collega's ('peers') van de medewerkers die het betreft in voor het geven van het goede voorbeeld en het stimuleren dat de betreffende medewerkers de benodigde beveiligingsmaatregelen ook goed uitvoeren.
- Eigen betrokkenheid:

- betrek de medewerkers bij het selecteren, uitwerken en evalueren van de benodigde beveiligingsmaatregelen. Doordat de maatregelen dan meer 'eigen' zijn, worden ze beter nageleefd.

Lage uitvoerbaarheid

- Implementeer de beveiligingsmaatregelen zo dat het uitvoeren ervan goed te doen is voor alle medewerkers die ermee te maken hebben.

Lage zelf-uitvoerbaarheid

- In het algemeen veroorzaakt deze factor met betrekking tot de beveiligingsmaatregelen op de werkvloer weinig problemen. Mocht dat toch het geval zijn, overweeg dan om de medewerkers die het betreft coaching te geven, waardoor ze het zelfvertrouwen op kunnen bouwen dat ze zelf de benodigde maatregelen uit kunnen voeren.

Positieve en negatieve gevolgen

- Implementeer de beveiligingsmaatregelen zodanig dat het uitvoeren ervan niet leidt tot represailles; en dat het niet - of niet goed - uitvoeren van de beveiligingsmaatregelen niet wordt beloond. Het belonen van goed gedrag kan een positieve invloed hebben.

Onvoldoende vaardigheden

- Verbeter de vaardigheden van de medewerkers die het betreft door het herhaald en onder begeleiding uitvoeren ervan in training, in simulatie of op de werkvloer.

Onvoldoende gelegenheid

- Implementeer de beveiligingsmaatregelen zodanig dat voor de medewerkers geen hindernissen worden opgeworpen om ze uit te voeren.

De genoemde gedragsbeïnvloedende factoren zijn persoonsgebonden en kunnen in een organisatie dan ook voor verschillende medewerkers in verschillende mate een probleem zijn. Daarom zal eerst vastgesteld moeten worden welke gedragsbeïnvloedende factoren bij welke medewerkers een probleem veroorzaken (1). Als bij een bepaalde medewerker is geconstateerd dat één of meer factoren een probleem zijn, dan kunnen die factoren voor die medewerker, met daarbij passende aanpak, gericht worden verbeterd. Sommige aanpakken worden op medewerkerniveau ingevuld, zoals het laten volgen van een cursus. Andere worden groepsgewijs opgepakt, zoals het inschakelen van peers. En soms aanpak voor de organisatie of een onderdeel ervan, zoals het goed inrichten van informatiebeveiligingsmaatregelen. Als bij een bepaalde medewerker meerdere factoren niet op orde zijn, dan geldt voor de aanpak ervan een bepaalde volgorde (1). Eerst dient bij de medewerker de kennis op orde te worden gebracht, want als de medewerker de benodigde gedragingen niet kan plaatsen of de relevantie er niet van inziet, dan komt het veilige gedrag er ook niet. Als de kennis op orde is, dan kunnen respectievelijk de bij de betreffende medewerker geconstateerde bias- en attitudeproblemen worden aangepakt. Organisatiefouten met betrekking tot de informatiebeveiliging, zoals een ongelukkige keuze van de beveiligingsmaatregelen of het niet betrekken van medewerkers bij de informatiebeveiliging, zouden al in een eerder stadium aangepakt en opgelost moeten zijn (1,5).

Conclusie

Op basis van het gedragsverklarend model dat we in ons vorige artikel hebben beschreven (1), hebben we gemeten welke gedragsbeïnvloedende factoren een rol spelen bij het niet uitvoeren van het benodigde, veilige gedrag. We hebben het onderzoek gericht op het veilig omgaan met mobiele digitale media, zoals smartphones en laptops.
Uit het onderzoek blijkt dat geen van de meegenomen gedragsbeïnvloedende factoren en deelfactoren onbelangrijk is. Alle factoren en deelfactoren spelen in de praktijk een rol van betekenis. Bij het ontwerpen van verbeteringsaanpakken voor veilig gedrag zal hier terdege rekening mee moeten worden gehouden. De in ons onderzoek opgestelde vragenlijst, of een variant daarvan, kan gebruikt worden om te bepalen welke gedragsbeïnvloedende factoren bij welke medewerkers niet op orde zijn. Op basis daarvan kunnen dan daarop toegespitste verbeteringsaanpakken worden ingezet bij de betreffende medewerkers, groepen, of organisatieonderdelen.

Referenties

(1) Spruit, M. & Kreffer, C. (2024). Informatie(on)veilig gedrag van medewerkers. IB Magazine, 5, 8-13.

(2) Spruit, M., Oosting, D. & Kreffer, C. (2024). Factors that influence secure behaviour while using mobile digital devices. Information and Computer Security. Https://marcelspruit.nl/papers/Spruit_Oosting_Kreffer_-_Cybersec_Awareness_-_IACS_2024.pdf

(3) CBS (2024). StatLine - Nederland in cijfers. Https://opendata.cbs.nl/statline/#/CBS/nl/

(4) Korteling, J.E., Gerritsma, J.Y.J., & Toet, A. (2021). Retention and Transfer of Cognitive Bias Mitigation Interventions: A Systematic Literature Study. Frontiers in Psychology, 12:629354.

(5) Spruit, M. (2010). Informatiebeveiliging en bewustzijn. De IT-Auditor, 1, 24-27.

(6) Pramaesti, A.V. et al. (2022). Reducing Laziness in Learning: A Review. The 15th University Research Colloqium 2022 Universitas Muhammadiyah Gombong.

(7) Felkey, A.J., Dziadula, E., & Chiang, E.P (2023). Microcommitments: Mitigating procrastination with more than a nudge. Southern Economic Journal, 90 (2), 497-509.

COLUMN RONALD

Muizenjacht door jigglers

De laatste maanden hebben we veel last van jigglers. Mouse jigglers komen uit de gamewereld en zijn bedoeld om schermbeveiliging te omzeilen. De jiggler doet dit door de bewegingen van een muiscursor te simuleren op een scherm. De jiggler voorkomt dat de computer in slaapstand terecht komt en dat de schermbeveiliging geactiveerd wordt.

Er zijn verschillende types mouse jigglers, te weten software en hardware jigglers en zelfs jiggler apps. Software jigglers vind je op internet, de Microsoftstore staat er vol mee. Het vervelende is dat er jigglers zijn die je kunt installeren zonder admin rechten. Maar ook op andere plekken dan de Microsoftstore vind je mouse jigglers en er zijn ook open source jigglers.

Ook zijn er slow movement jigglers. Deze slow movement jigglers verplaatsen de muispointer afwisselend naar links en rechts met één pixel. Doordat het tempo laag is en de pointer slechts één pixel van plek verspringt, kan je gewoon doorwerken met de normale muis.

Er zijn ook apps voor op je mobiele telefoon. Bij het starten van de app verschijnen er blokpatronen of strepen op het scherm van de telefoon. Door nu de computermuis op het scherm van de telefoon te leggen werkt de muis als een jiggler. Veel computermuizen werken op basis van lichtreflectie (meestal infrarood). Door de reflectie te beïnvloeden komt de muis in de jiggler status. Het zijn mooie apps met timers, powersafes en patrooninstellingen, maar ja het blijven jigglers.

Naast de software jiggler is er ook nog de hardware variant. Een hardware mouse jiggler wordt op een USB-poort aangesloten en gedraagt zich als een standaard muis, ook hier zijn geen software-drivers voor nodig. De mouse jiggler wordt in Windows, Mac OS en andere operating systems ondersteund met een muisaansluiting.

Hardware jigglers vind je op internet bij Ali express en vele andere stores. Deze jigglers zijn er in verschillende uitvoeringen. Zo zijn er jigglers in de vorm van een klein USB-plugje tot complete muizen in allerlei kleuren en maten. Bij Ali zijn zelfs normaal ogende computermuizen te koop met op de onderkant een extra schakelaartje om de muis in jiggler stand te zetten.
Het zal duidelijk zijn dat het gebruik van jigglers ernstige veiligheidsrisico's met zich meebrengt, doordat het computers kwetsbaar maakt voor ongeoorloofde toegang. De beveiliging tegen jigglers is erg lastig. Veel leveranciers geven aan dat mouse jigglers met USB-aansluiting niet detecteerbaar zijn.

Voor ons als security verantwoordelijken blijft er niet anders over dan de fysieke muizenjacht. Vang ze…

Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via ronald@eygendaal.com

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.

SIG terug van weggeweest

Het zal midden jaren 80 van de vorige eeuw geweest zijn dat ik een bijeenkomst bijwoonde van de FIG Forth. De Forth Interest Group, een Special Interest Group van Forth-adepten. Forth was een bijzondere programmeertaal en inmiddels vergane glorie. Net zoals de SIGs! Althans dat dacht ik.

Tot mijn grote verbazing ontving ik in november 2024 een uitnodiging voor een SIG-bijeenkomst over Identity & Access Management (SIG-IAM). Je hebt deze waarschijnlijk ook ontvangen. Het aloude fenomeen van SIG is door twee PvIB- en IAM-goeroes nieuw leven ingeblazen. Je kent ze als gewaardeerd PvIB-lid vast en zeker: Andre Koot en Evert van Zanten. Het is niet dat ik me wil meten met deze beide heren, maar ik was wel geïnteresseerd hoe een SIG anno 2024 er uitziet. Het slechte nieuws is, 'there is nothing new', maar het goede nieuws is, dat er een flinke opkomst was van geïnteresseerden. Vrouwen en mannen, waarvan de eerst groep natuurlijk in de minderheid was, dus ook daar wel het vertrouwde beeld.

Na de kennismaking werd het een soort van brainstormsessie over welke onderwerpen er zoal de revue zouden kunnen gaan passeren in de volgende bijeenkomsten. Wat mij opviel was dat er zoveel verschillende expertises aanwezig waren. Hardcore ICT'ers met een rijke ervaring variërend van RACF tot aan het ABAC. Ook veel expertise vanuit de business variërend van governance tot aan operationeel IAM en privacy. Kortom een interessante groep waar veel kennis te halen, maar zeker ook te brengen zal zijn.
Ik concludeer dat deze eerste SIG-meeting mij niet heeft teleurgesteld, integendeel het enthousiasme was duidelijk voelbaar en ik zag veel zaken terug uit vervlogen jaren, zoals brown paper sessies als opmaat voor een expert brief. Een waardevolle PvIB-activiteit waaraan ik destijds vaker heb deelgenomen. In een SIG staan weer mooie dingen te gebeuren een heel mooi initiatief waarbij kennisdeling, kennisverwerving en -verdieping nader kunnen worden ingevuld. Daar staan we toch voor, als PvIB. Het is dus gewoon even wachten tot er weer een paar PvIB-goeroes opstaan die een volgende SIG het leven laten zien. Het eerste zaadje is gelegd en gekiemd. Ik ben benieuwd.

Fook Hwa Tan – Een springlevende traditie van kennisdeling

Wat een mooi initiatief om de Special Interest Groups (SIG's) nieuw leven in te blazen binnen PvIB! De eerste bijeenkomst over Identity & Access Management ademde energie, betrokkenheid en een gedeelde passie voor kennisdeling. Wat deze SIG meteen krachtig maakt, is de diversiteit aan expertise: van doorgewinterde ICT'ers tot strategische business- en governance-experts. Dit onderstreept dat IAM niet alleen een technische uitdaging is, maar een essentieel onderdeel van veilige en efficiënte bedrijfsvoering.
De ambities liegen er niet om: vier kennissessies in 2025, vijf artikelen, en een breed scala aan onderwerpen, van IGA en PAM tot eIDAS en best practices. Dat belooft een dynamische en impactvolle serie bijeenkomsten!

Wat echt hoopvol stemt, is de openheid van dit platform. Door SIG-IAM ook toegankelijk te maken voor niet-leden, wordt een bredere community aangesproken. Kennis groeit immers het snelst wanneer deze wordt gedeeld. Met zowel fysieke meetings als een online-community in de planning, krijgt deze SIG de kans om uit te groeien tot een blijvend kennisnetwerk. Dit is meer dan een bijeenkomst; dit is een beweging. Het zaadje is geplant en begint te groeien. Nu is het aan de community om het te voeden, te laten bloeien en samen de toekomst van IAM en andere thema's vorm te geven. Op naar een bruisende SIG-traditie binnen PvIB!

Chris de Vries – Een vonk, dat kan uitgroeien tot meer

Een klein vonkje is vaak voldoende om een heel bos of stad in as te leggen. Dat is 'altijd' een ramp, zoiets nietigs dat zoveel moois vernietigd! En toch, gedurende het bestaan van onze aarde hebben vernietigende vuurzeeën ook kansen gecreëerd voor nieuw leven, dus enkel negatief is het ook weer niet óf wij moeten vanuit ons perspectief ons leven of dat van dierbaren verliezen.


Fook Hwa Tan


Leo van Koppen


Chris de Vries

Wat echt hoopvol stemt, is de openheid van dit platform. Door SIG-IAM ook toegankelijk te maken voor niet-leden

Niet zo extreem, maar eveneens als een kleine oorzaak met mogelijk grote gevolgen kunnen wij het SIG-IAM initiatief zien. De uitnodiging beschreef het als volgt: "Autorisatiebeheer, beheer van identiteiten en accounts, verlenen van toegang aan allerhande personen en dingen, organisaties kunnen er omheen, omdat goed te regelen. ...We zien dat dat in de praktijk te vaak verkeerd gaat. Aanbestedingen gaan fout, oplossingen leveren niet het voorgespiegelde resultaat, de business case geeft geen goede uitkomst. ... Zonde van de tijd, zonde van het geld en zonde van het imago van het vakgebied IAM." Vandaar het gewaardeerde initiatief van de heren Van Zanten en Koot. Niet alleen haalden zij een behoorlijke groep geïnteresseerden op 28 november naar binnen, ook realiseerden zij een levendig discussie over sterkten, zwakten, kansen en bedreigingen. Redactieleden, Leo van Koppen en Chris de Vries, lieten het zich niet ontgaan om daarbij aanwezig te zijn. Leo heeft zijn bevindingen aan het begin van dit artikel verwoord en de ambities weergegeven. De initiatiefnemers hebben hun gasten gevraagd hoe dit 'vonk initiatief' aangeblazen zou kunnen worden. Daar kwamen goede suggesties naar voren met aanvullingen zoals publicatie in ons magazine, benutting van de LinkedIn-accounts, de nieuwsbrief en wellicht zelfs als start van een PvIB-podcast. Dit laatste niet alleen over het SIG-IAM initiatief, maar ook voor andere thema's. Dus ook op dat terrein werd zaad uitgestrooid. Ik vertrouw op kundige en betrokken virtuele tuiniers.

Een kijkje naar de toekomst

Deelnemers aan de ronde tafel op 19 februari 2025.

Op 19 februari 2025 kwam een kleine twintigtal mensen in Utrecht samen op de TNO-locatie aan de Princetonlaan. Zij bestonden buiten de TNO-medewerkers en redactieleden van IB-Magazine (de initiators) ook uit potentiële auteurs van de IB 3-2025 special: Security Tech-transfer. Zij waren uitgenodigd om geïnformeerd te worden over de special en het thema. Echter, meer dan enkel informatie te ontvangen, werd aan hen gevraagd welke bijdrage zij zouden kunnen/willen leveren in de vorm van artikelen. Onder de deelnemers (en enkelen die niet aanwezig konden zijn, maar wel mee willen werken) waren vertegenwoordigers van: overheid, NCC-NI, NCSC, Cyberveilig NI, het verzekeringsbedrijf, een Venture Capitalist en leden uit het bedrijfsleven. In een boeiende en diepgaande discussie kwamen de aanwezigen tot 11 artikelonderwerpen. Ook stelden kandidaat-auteurs (trekkers) zich beschikbaar. Ook dit initiatief is te definiëren onder het begrip SIG-aanpak. Dit signaal geeft aan dat op dit kennisgebied het IB-Magazine in samenwerking komt met excellente partners (nu: TNO) ten einde een hogere kwaliteit van Informatie Beveiligingskennisdeling binnen onze sector te bevorderen. Het nummer IB 3-2025 wordt dus een aanrader.

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
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
ibmagazine@pvib.nl

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
secretariaat@pvib.nl
www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2025 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

VERSTERK UW ISO/IEC 27001 MANAGEMENTSYSTEEM!

Wilt u zeker weten of uw organisatie klaar is voor certificering volgens ISO/IEC 27001? Doe de online DNV Self-Assessment en ontvang een rapportage in uw inbox. Of volg de Normkennis ISO/IEC 27001

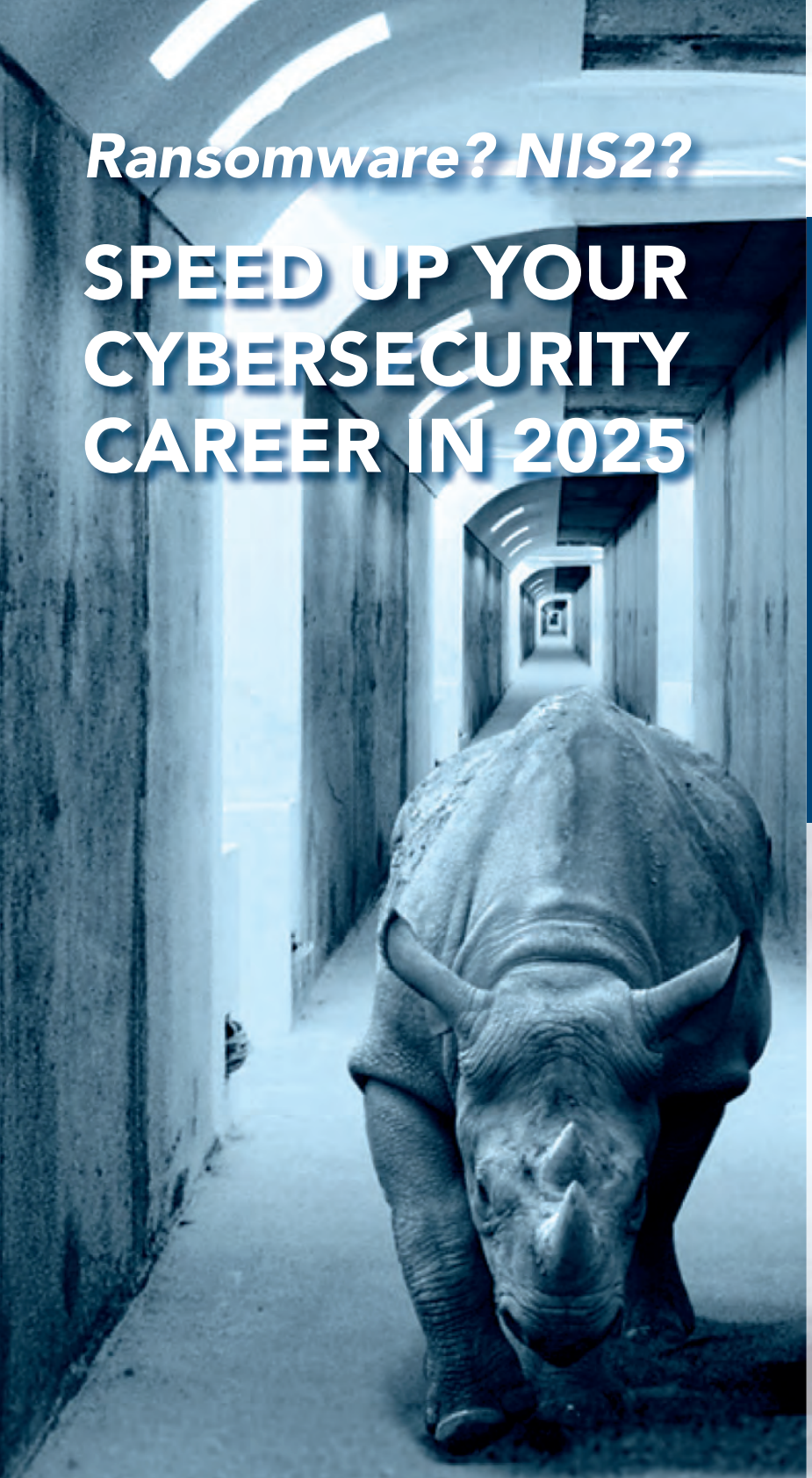
Kent u de DNV Self-Assessment Suite al? Deze tool stelt u in staat te testen hoe goed u ISO/IEC 27001 kent en te beoordelen in hoeverre uw managementsysteem klaar is voor certificering. De evaluatie is op basis van puntenscores en laat zien waar er tekortkomingen bestaan en waar u verbeteringen kunt doorvoeren.

Stel een nulmeting op, stel kwantitatieve doelen vast voor een specifiek aandachtsgebied en meet regelmatig de geboekte vooruitgang. De Self-Assessment Suite biedt u in alle gevallen een gedetailleerd inzicht in uw kennis of prestaties en uw mate van beheersing.

Wilt u graag uw kennis vergroten over ISO/IEC ISO 27001? Volg dan de Normkennis ISO/IEC 27001 training! De trainer geeft u handige tips en voorbeelden uit de praktijk, zo leert u te kijken naar de norm, zoals een auditor dit doet.

Kijk voor meer informatie over de Self-Assessment Suite op dnv.nl/self-assessment of scan de QR-code als u wilt deelnemen aan de training.

DNV



Ransomware? NIS2?

SPEED UP YOUR CYBERSECURITY CAREER IN 2025

Want security start bij mensen!!

TSTC
ICT en Security Trainingen

AIGP	Certified AI Governance Professional
CNIS2	Certified NIS2 Professional
BIO	Certified Bio Professional Foundation/Practitioner
OSCP	OffSec PEN-200
OSEE	OffSec EXP-401
CEH	Certified Ethical Hacker v13 AI

TSTC is een gerenommeerd IT opleidingsinstituut en erkend specialist in informatiebeveiliging en cybersecurity trainingen.

GET SKILLED
WWW.TSTC.NL

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 Offi cer

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 27001	Privacy Management

ONZE TRAININGEN ZIJN KLASSIKAAL OF LIVE ONLINE TE VOLGEN