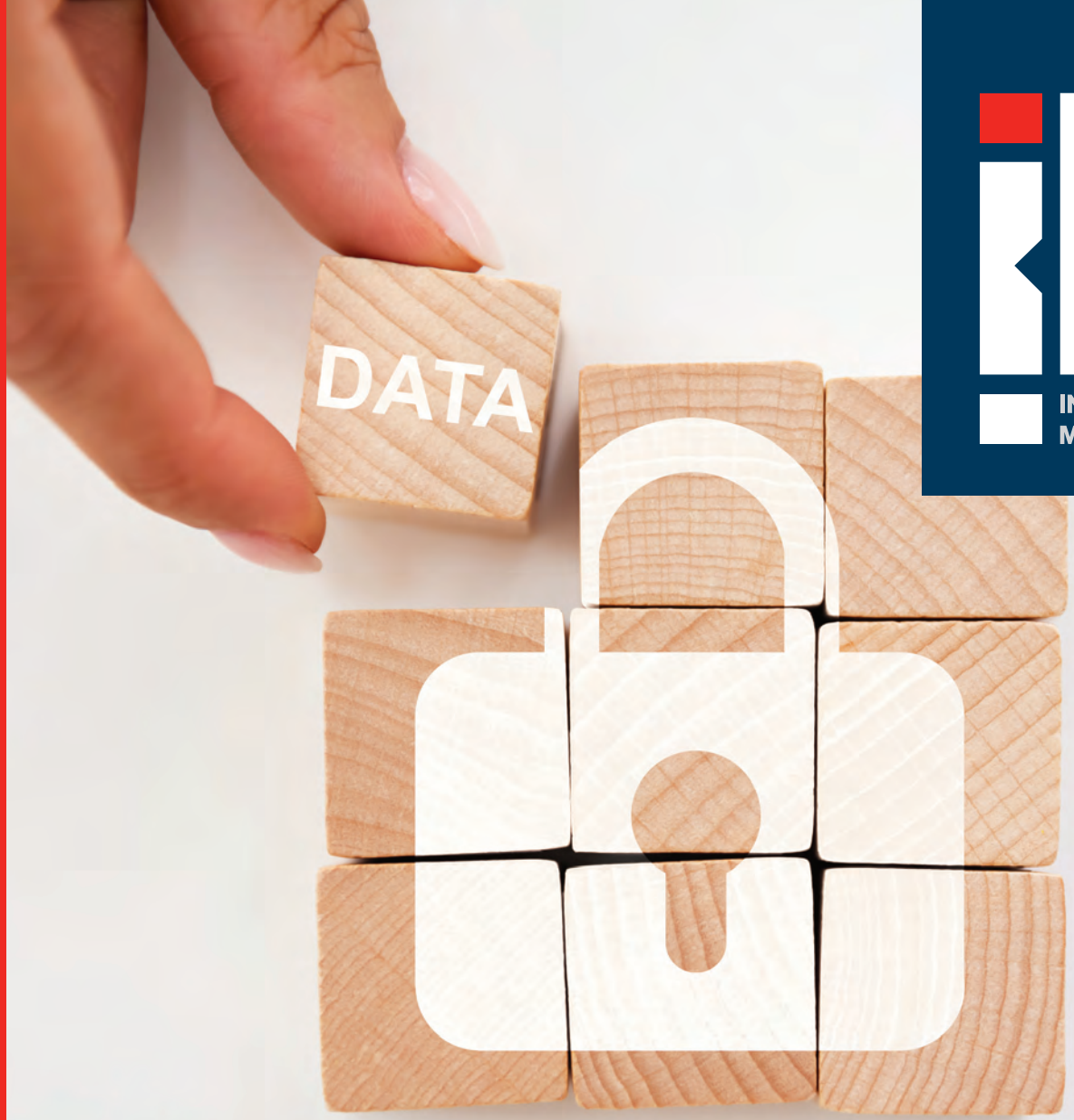


INFORMATIEBEVEILIGING MAGAZINE

Dossier: NIS2

- Trends in cybersecurity voor 2024
- NIS2 stap voorwaarts in Europese cyberbeveiliging
- Blog: Andersom denken in cybersecurity

JAARGANG 24 - 2024 - EDITIE 1

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

'Een nieuwe lente en een nieuw geluid'

Chris de Vries

Met deze woorden begint Herman Gorter zijn gedicht 'Mei'. Het is een van Nederlands bekendste gedichten, alhoewel ik niet weet of dat ook geldt voor de jongere generatie(s). Dichter Garmt Stuiveling omschrijft 'Mei' met aspecten van: persoonlijk ritme, beeldspraak, sterke emotie, verbeelding, natuurliefde, melancholie en erotiek. Vol met visionaire symboliek.

Ook wij vormen ons een eigen beeld van 2024. Ook wij? Specialisten in Informatiebeveiliging? Dichten en symboliek staan toch ver van ons af? Ratio tegenover emotie, wetenschap tegenover verbeelding, het werkelijke leven tegenover beeldspraak (eXtended Reality) en de reproduceerbare samenleving tegenover de visionaire symboliek?! Bij doorbladeren van dit magazine ervaar je wellicht de dominante linker hersenhelft (lineair denken, neurotypisch) bij het merendeel van de auteurs in onderwerpen als: awarenessmeting onderwijs & onderzoek, de NIS2-richtlijn, BIO, Incident response en ICT & Recht. Nadere beschouwing toont ons ook de werking van de rechter hersenhelft (conceptueel denken, neurodivergent) in toevoegingen zoals: Connect2Trust Foundation, culturele verschillen bij NIS2, Chief INsecurity officer, non-lineaire cyberwetgeving, massa-opinie en het begrip ethische discussie. Niet alleen door neurodivergente persoonlijkheden, ook neurotypische personen kunnen dat, en omgekeerd.

Ik breek dan ook een lans voor flexibel denken met mijn 'kriktaal'. Een door A. van Neijnatten verzonnen Nederlands woord ter vervanging van in onze taal binnengeslopen Engelse begrippen (wedstrijd van dagblad De Tijd, 1965) en in dit specifiek geval ter vervanging van het woord 'peptalk'. Bron: Wim Daniëls.

In dit nummer spreiden wij ons vangnet wijd. In komende uitgaven van 2024 willen wij verdiepend ingaan op: Artificial Intelligence, Onderwijs & Onderzoek, Supply Chain en Quantum Computing. Voor 2025 staan thema's als Business Continuity, Security (Auditing), Architecture, Hacking en Privacy gepland.

Wij zoeken het contact en interactie met jullie. Dus de oproep om artikelbijdragen, hoe eerder jouw aanmelding, des te eerder je aan de slag kunt en hoe meer tijd voor een hoogwaardige bijdrage aan ons magazine (door ons en voor ons). Ik vraag aandacht voor het artikelen jaaroverzicht 2023; doe suggesties voor de prijs van de 'beste 3 artikelen van 2023'. Deelnemen in de jury kan ook, laat het ons weten! Wij zoeken kandidaten.

Dacht ik eind 2023 dat het door de feestdagen moeizaam zou worden het eerste nummer te vullen, de werkelijkheid bleek positiever. Uitgave iB-1 liep onverwacht snel vol. Dank daarvoor aan de auteurs. We hopen op een succesvol 2024 met jullie actieve participatie!

Chris

IN DIT NUMMER

Auteurs: Rosanne Pouw, Product Manager Awareness & Training bij SURF rosanne.pouw@surf.nl. Marijke Stokkel, senior manager team Cybersecurity en verantwoordelijk voor de propositie security & privacy awareness marijke.stokkel@bdo.nl. Susanne van 't Hoff-de Goede, criminoloog en sr onderzoeker bij het Centre of Expertise Cyber Security, Haagse Hogeschool m.s.vanthoff-degoede@hhs.nl. Maaike van der Wal, criminoloog en junior onderzoeker bij het Centre of Expertise Cyber Security, Haagse Hogeschool m.l.vanderwal@hhs.nl.

Van twijfel naar enthousiasme

Innovatie in het meten van awareness en daadwerkelijk veilig gedrag

'Is het een idee om de awarenessmeting dit jaar anders aan te pakken?' Deze vraag groeide uit tot een unieke samenwerking tussen drie verschillende organisaties: SURF, BDO en de Haagse Hogeschool. Ondanks weerstand en complicaties maakten we een innovatieve gedragsmeting, onderdeel van de awarenessmeting bij onderwijs- en onderzoeksinstellingen. Een inspanning die naast het meten van kennis, ondersteuning en motivatie inzicht geeft in de voorspelling van daadwerkelijk cyberveilig en privacybewust gedrag.

SURF en BDO begonnen in 2021 met het meten van awareness bij onderwijs- en onderzoeksinstellingen. De meting is gebaseerd op het COM-B model voor gedragsverandering. Kort samengevat: hoe mensen zich gedragen wordt bepaald door wat zij weten en kunnen (bekwaamheid), willen (motivatie) en of zij gefaciliteerd worden (gelegenheid).

De deelname was op vrijwillige basis en voor maximaal 30 instellingen. De metingen bestonden uit onlinevragenlijsten voor medewerkers aangevuld met interviews. Deze rapportages werden vervolgens geanalyseerd om tot een sectorrapportage te komen. Met deze resultaten konden onderwijsinstellingen richting geven aan awarenessactiviteiten en het belang van awareness ondersteunen.

Toen Marijke Stokkel (BDO) in 2022 een presentatie gaf over deze meting, ontdekte ze dat er een nog een spreker op het programma stond die over het COM-B model zou spreken. Susanne van 't Hoff-de Goede (de Haagse Hogeschool) had gedragsmetingen ontwikkeld die ze afzette tegen het COM-B model. De link werd snel gelegd: de gedragsmeting combineren met de SURF-awarenessmeting zou voor beide partijen waardevolle inzichten kunnen opleveren.

Sterk wachtwoord

Hoe ging de gedragsmeting in zijn werk?

- Aan de deelnemers van de SURF-awarenessmeting werd bij aanvang gevraagd om een account aan te maken, inclusief een wachtwoord. Zonder account was het niet mogelijk om de meting te voltooien.
- Vervolgens werd aan de hand van 20 indicatoren gemeten hoe sterk het wachtwoord was (het wachtwoord zelf werd niet opgeslagen in de onderzoekstool). Voorbeelden van indicatoren zijn het aantal karakters, aantal cijfers, hoofdletters, speciale karakters en het aantal brute force pogingen nodig om het wachtwoord te kraken.
- Aan de hand van deze indicatoren werd een score (0-4) vastgesteld. Wachtwoorden met score 3 of 4 worden als 'sterk' bestempeld.

Delen van persoonsgegevens

Hoe ging de gedragsmeting in zijn werk?

- Aan het eind van de vragenlijst van de SURF-awarenessmeting kregen de respondenten het verzoek om een aantal persoonsgegevens in te vullen.
- Het betrof zeven soorten persoonsgegevens:
- Naam
- Adres
- Postcode
- Plaats
- Telefoonnummer
- Geboortedatum
- Medewerker nummer

Vervolgens werd gekeken of, en zo ja hoeveel, gegevens de respondenten deelden. Respondenten die helemaal geen persoonsgegevens deelden, kregen het stempel 'niet ongewenst delen persoonsgegevens'.

Start van de samenwerking

Toch waren er wat bedenkingen vanuit SURF. Deze aanpak zou de meting complex maken en mogelijk vertragingen opleveren. En wat als de instellingen hierdoor helemaal zouden afzien van de meting? Voor productmanager Rosanne Pouw (SURF) was dit de eerste keer dat ze de meting zou coördineren. Met enige twijfel en na een gesprek met Marijke en Susanne besloot ze toch mee te doen. SURF is een partij die graag innovatieve ideeën uitvoert en samenwerkt.

Het plan was om samen met de awarenessmeting daadwerkelijke ook het onlinegedrag te meten, en wel in de volgende (gefingeerde) situaties:

1) het aanmaken van een veilig wachtwoord en
2) het delen van persoonlijke informatie.

Het doel van de meting was om de relatie tussen daadwerkelijk gedrag en awareness te onderzoeken op basis van COM-B.

Weerstand

Dit plan werd met gemengde gevoelens ontvangen door de deelnemende instellingen. Sommige zagen dit als een mooie kans, terwijl andere zich zorgen maakten. Er ontstond onrust omdat dit plan de vertrouwensband tussen de security- en privacy-professionals en de rest van de organisatie kon schaden; medewerkers zouden 'genept' worden met zo'n gedragsmeting, vergelijkbaar met een phishingtest. Medewerkers zouden mogelijk sneller afhaken als zij een (fictief) account moesten aanmaken, met als gevolg een lagere response. Besloten werd dat de gedragsmeting optioneel zou zijn. Instellingen konden ook kiezen voor de awarenessmeting met vragenlijsten zoals zij die de voorgaande jaren hadden uitgevoerd.

Daarnaast stelden we een handleiding op om met negatieve reacties van medewerkers om te kunnen gaan (beloon opmerkzaamheid, wees transparant, vraag om geheimhouding tijdens de looptijd). En schreven we begeleidende teksten om instellingen te helpen het management te overtuigen om met de meting mee te doen. Van de 29 deelnemende instellingen kozen er uiteindelijk 20 om ook aan de gedragsmeting mee te doen.

Parallel meten

Nu het besluit genomen was, konden we aan de slag. De gedragsmeting gebruikte een andere testomgeving en het klaarzetten van die omgeving bracht nieuwe vragen met zich mee. Welke URL gebruiken we en hoe betrouwbaar oogt de URL voor medewerkers? Is deze omgeving zowel in het Nederlands als in het Engels beschikbaar? En voldoet deze omgeving aan de strenge securityeisen van SURF?

Gelukkig kon de technisch beheerpartij deze vragen oplossen. De meting startte half mei en liep tot begin juni. Tijdens de meting kregen instellingen elke twee weken een update van het aantal respondenten. Instellingen kozen zelf hoe zij de meting onder de aandacht brachten, bijvoorbeeld via intranet of door medewerkers een e-mail te sturen met het verzoek aan de meting mee te doen.
Tijdens de meting pakten SURF, BDO en De Haagse Hogeschool elk een andere rol. SURF deed vooral de communicatie en beantwoordde de vragen. BDO voerde de awarenessmeting uit en stelde instellingsrapporten op en de Haagse Hogeschool voerde de gedragsmeting uit.

Onderzoekers en consultants

Na afloop van de meting was het tijd om de data te onderzoeken. Het samenvoegen van de verschillende datasets bleek een praktische uitdaging. Vervolgens was de vraag hoe we het verband tussen het COM-B en de gedragsmeting helder konden neerzetten. Bij het duiden van de resultaten bleek dat onderzoekers de neiging hebben heel voorzichtig te zijn in hun uitspraken, terwijl consultants juist concrete adviezen willen meegeven. Dat leidde tot interessante gesprekken. Bovendien wilde SURF graag dat de sectorrapportage ook gebruikt kan worden om het management van instellingen te wijzen op het belang van awareness. Dat alles onder hoge tijdsdruk, want de instellingen ontvingen hun instellingsrapportage vlak voor de zomervakantie.
Er volgden meerdere meetings waarbij we elk onze punten inbrachten en van daaruit uiteindelijk tot een compromis kwamen. Zoals het besluit om de resultaten van de gedragsmeting in de sectorrapportage verder uit te diepen omdat het lastig was om per instelling correlaties te leggen vanwege het lage aantal respondenten.
Naast de metingen per instelling werd er ook een sectorrapport opgesteld. Hierin werden niet alleen de resultaten van de SURF-instellingen meegenomen, maar ook die van 41 MBO-instellingen. Dit jaar voerde MBO Digitaal namelijk dezelfde awarenessmeting uit.

Resultaten gedragsmeting

Wat komt er naar voren uit de gedragsmeting? Onveilig online-gedrag blijkt veelvuldig voor te komen onder medewerkers. Zo koos slechts 61% van de medewerkers een sterk wachtwoord en koos 18% van de medewerkers een wachtwoord dat al gelekt was. Ook deelde 25% van de medewerkers persoonlijke gegevens, zoals naam (21%) en geboortedatum (11%). Uit de analyse blijkt dat de componenten bekwaamheid en motivatie een zeer beperkt positief verband hebben met daadwerkelijk veilig gedrag. Het component gelegenheid laat een zeer beperkt negatief verband zien met het delen van persoonlijke gegevens. Deze factoren verklaren echter slechts is 1-2% van het gedrag. Dat betekent dat 98-99% van de variantie tussen medewerkers in het informatieveilige gedrag wordt verklaard door andere factoren die niet zijn meegenomen in dit onderzoek.

Wat is het effect van de gedragsmeting op response? Omdat er bij de start van het traject twijfels waren, hebben we ook

Onderzoekers hebben de neiging voorzichtig te zijn in hun uitspraken, terwijl consultants juist concrete adviezen willen meegeven

gekeken of het vermoeden dat mensen zouden afhaken bij de gedragsmeting juist was. Door de responsepercentages te vergelijken tussen de groep zonder gedragsmeting en de groep met gedragsmeting zagen we dat het responsepercentage in beide groepen vergelijkbaar is.

Ook wilden we weten of er veel vragen en reacties van medewerkers waren. Dit bleek mee te vallen: er werden wel vragen gesteld, maar de voorgestelde route om dit gedrag te belonen, transparant te zijn en om geheimhouding te vragen, haalde de scherpste randjes ervan af. We zijn de instellingen die het aandurfden om de gedragsmeting uit te voeren hiervoor dankbaar en zijn tevreden dat de negatieve reacties meevielen.

Terugblik

Het was de eerste keer dat deze meting uitgevoerd werd met input vanuit SURF, BDO en De Haagse Hogeschool. De samenwerking verliep soepel en we konden snel schakelen. Bijvoorbeeld voor het maken van aanpassingen in vragen of het uitwerken van het proces. Desondanks hadden we elk ook onze eigen unieke expertise en blik op het onderzoek. Dat leverde interessante discussies op, bijvoorbeeld over het advies dat we mee konden geven aan instellingen. Tijdens het opstellen van de rapportage brachten we elkaar op nieuwe ideeën om de resultaten duidelijker weer te geven. We hebben die multidisciplinaire aanpak als verrijkend ervaren omdat het onze blik verruimd heeft.

Ondanks de verschillende belangen en achtergronden hebben we door communicatie en compromissen een manier gevonden om de gedragsmeting succesvol uit te voeren. We zijn tevreden over het proces. De resultaten wijzen er op dat het daadwerkelijk gedrag complexer is dan binnen het COM-B model kan worden aangegeven, extra onderzoek in welke factoren een rol spelen zal hier nieuwe inzichten in geven.
Het is nog te vroeg om een uitspraak te doen of deze samenwerking een vervolg krijgt. SURF is in elk geval van plan om ook in 2024 een awarenessmeting uit te laten voeren. We reviewen met de deelnemers van de gedragsmeting hoe zij dit proces ervaren hebben en hoe zij de extra gegevens in de rapportages kunnen inzetten. Voor ons was deze samenwerking in elk geval een groot succes.

Belangrijkste conclusies sectorrapportage

1. Over de hele linie zijn de resultaten beter dan vorig jaar, maar deze zijn nog niet voldoende;
2. Er is een zeer beperkt verband tussen 'COM-B' en daadwerkelijk informatieveilig gedrag;
3. Informatieveilig werken lijkt een individuele aangelegenheid: een sterke security cultuur ontbreekt.

De rapportage kun je hier terugvinden:
https://sec.surf.nl/awareness-meting-sector-rapportage/
Of hier: https://edu.nl/jgnhn

Auteur: Vincent van Dijk, eigenaar van Security Scientist. Hij is bereikbaar via: vincent@securityscientist.net.

NIS2 stap voorwaarts in Europese cyberbeveiliging

In het cyberbeveiligingslandschap komt de NIS2 richtlijn naar voren als een cruciale ontwikkeling, die het beschermingskader binnen de Europese Unie een nieuwe vorm geeft. Deze richtlijn gaat verder dan zijn voorganger en stelt verbeterde protocollen op om de steeds complexere aard van cyberdreigingen, waarmee entiteiten in verschillende sectoren worden geconfronteerd, aan te pakken en tegen te gaan.

Softwareontwikkelingsbedrijven opereren in de voorhoede van de technologische innovatie en ondervinden in het bijzonder de gevolgen van deze nieuwe regelgeving. Hun werk is inherent verweven met cyberbeveiliging en omvat veel processen die gevoelig zijn voor digitale bedreigingen. Deze bedrijven zijn verantwoordelijk voor het ontwikkelen van geavanceerde softwareoplossingen en het beschermen van de integriteit en privacy van de gegevens die deze oplossingen beheren.

Dit artikel ontleedt het proces van integratie van de nalevingseisen met betrekking tot de NIS2 richtlijn bij softwareontwikkelingsbedrijven.

Software-ontwikkelingsbedrijven onder de NIS2

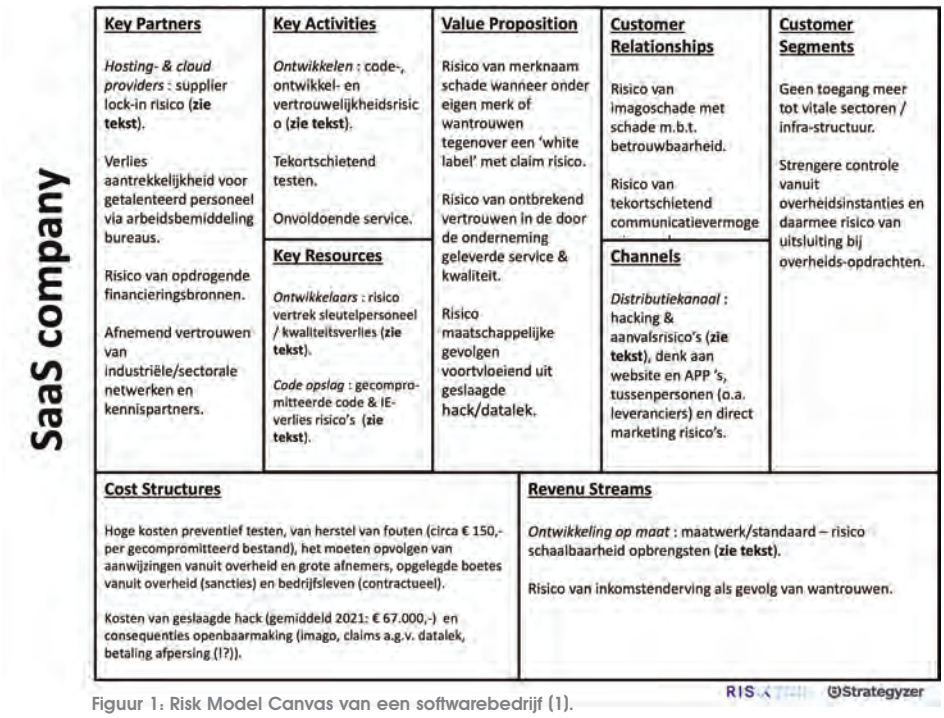
De NIS2 richtlijn werpt een breed net uit en richt zich op veel entiteiten die volgens de richtlijn 'essentieel' en 'belangrijk' zijn voor het maatschappelijk en economisch welzijn. Softwareontwikkelingsbedrijven vallen precies in deze categorie, als ze ook beheerde diensten leveren op de software die ze ontwikkelen (zoals SaaS-bedrijven). Als ruggengraat van de digitale infrastructuur zijn ze een integraal onderdeel wat het functioneren van verschillende sectoren betreft: van de gezondheidszorg tot de financiële sector. Hun platformen en applicaties verwerken vaak enorme hoeveelheden gevoelige gegevens, waardoor ze een spil vormen in het digitale ecosysteem en dus 'essentieel' zijn in de ogen van de richtlijn.

Risicogebaseerde benadering van cyberbeveiliging

NIS2 is een voorstander van een risicogebaseerde benadering van cyberbeveiliging. Dit betekent dat organisaties, in plaats van een pasklare oplossing voor te schrijven, hun specifieke kwetsbaarheden moeten evalueren en beveiligingsmaatregelen moeten bedenken, die in verhouding staan tot deze risico's. Deze benadering erkent de gevarieerde, dynamische aard van cyberbedreigingen en stelt softwareontwikkelingsbedrijven in staat om middelen plus verdedigingsmechanismen daar in te zetten waar ze het meest nodig zijn.

Belangrijkste vereisten voor naleving, gespecificeerd in artikel 21

Artikel 21 van NIS2 is de hoeksteen voor naleving; beschrijft de basismaatregelen die organisaties moeten nemen op het gebied van beveiliging en incidentrespons: van elementaire cyberbeveiligingspraktijken tot het opzetten van incidentresponsteams. Voor softwareontwikkelaars betekent dit dat ze ervoor moeten zorgen



Figuur 1: Risk Model Canvas van een softwarebedrijf (1).

dat hun ontwikkellevenscyclus, van ontwerp tot ingebruikname, is beveiligd tegen inbraak en gegevensschending.

Beveiliging toeleveringsketen en rapportage volgens NIS2

NIS2 gaat verder dan de direct betrokken organisatie, zij omvat de gehele toeleveringsketen. Softwareontwikkelaars moeten hun leveranciers en partners controleren op robuustheid van de cyberbeveiliging, waardoor een rimpeleffect van beveiligingsbewustzijn ontstaat. Bovendien is in het geval van een beveiligingsincident onmiddellijke rapportage verplicht - een vereiste die de nadruk van de richtlijn op transparantie en verantwoordingsplicht onderstreept.

Het bedrijfsmodel voor softwareontwikkeling

In het technologielandschap zijn softwareontwikkelingsbedrijven de architecten van digitale vooruitgang. Hun bedrijfsmodel is veelzijdig en gebouwd op een fundament van innovatie, technische bekwaamheid en strategische marktpositionering. Voor het ontleden van het businessmodel van een softwarebedrijf gebruiken we een Risk Model Canvas van de website riskmodelcanvas.net, zie figuur 1.

Kern bedrijfsstructuur softwareontwikkelingsbedrijf

Elk softwareontwikkelingsbedrijf moet beschikken over een goed geolied ontwikkelingsteam, verantwoordelijk voor de software-oplossingen; een operationeel team, dat zorgt voor soepele interne workflows en productlevering; en een marketingteam, die het bedrijf een stem geeft binnen een drukke markt. De combinatie van deze elementen bepaalt de huidige prestaties van het bedrijf en zet de koers uit voor de toekomstige groei.

Ontwikkeling is de drijvende kracht achter het aanbod van een softwarebedrijf en zet abstracte ideeën om in concrete producten. Operations ondersteunt de ontwikkelingscyclus, zorgt ervoor dat het eindproduct voldoet aan de kwaliteitsnormen en op tijd wordt geleverd. Aan de andere kant is marketing de stem van het bedrijf, belast met het positioneren van het product in de markt, het opbouwen van naamsbekendheid en het genereren van vraag. Samen ondersteunen deze drie pijlers de ambitie van het bedrijf om te innoveren en zijn bereik in het digitale domein uit te breiden.

Grote innovatie gaat echter ook gepaard met aanzienlijke risico's. Softwareontwikkelingsbedrijven bevinden zich in een

NIS2 erkent de complexiteit en het dynamische karakter van moderne cyberbedreigingen en biedt een flexibel, maar gestructureerd kader om deze aan te pakken

mijnenveld van potentiële bedreigingen, variërend van technische bedreigingen — zoals het handhaven van de kwaliteit van de code en bescherming tegen cyberbedreigingen – tot strategische dreigingen, zoals het voorblijven op snelle marktveranderingen en technologische vooruitgang. Diefstal van intellectueel eigendom, datalekken en verlies van menselijk kapitaal zijn ook belangrijke punten van zorg die het evenwicht van het bedrijfsecosysteem kunnen verstoren.

De risico's van het bedrijfsmodel

In het navolgend overzicht zijn de canvas thema's, gerelateerd aan risico's welke geclassificeerd zijn naar kans en impact. Dus van hoog (dagelijks tot maandelijks, regelmatig voorkomend) naar medium (enkele keren per jaar) naar laag (zelden). Daarbij de classificatie afgezet tegenover de impactklassen: financiële -, imago-, (wettelijke) regelgeving -, organisatorische - en veiligheidsrisico's. Ik ga hierbij niet in op de onderbouwing van het gehanteerde SaaS-classificatie voorbeeld.
Het Risk Model Canvas voor softwareontwikkeling beschrijft de bijbehorende bedrijfsrisico's (in het canvas indicatief voor de 9 thema's, hierna daarvan 5 thema's summier uitgewerkt):

Canvas thema: key partners

Canvas subthema: hosting- en cloud providers
Gerelateerd risico: supplier lock-in risico
Classificatie: medium
Beschrijving: bij de start vinden de kleinere SaaS-bedrijven en de providers elkaar, maar bij groei van het SaaS-bedrijf groeit niet altijd de provider mee. De provider moet aan nieuwe standaarden voldoen, maar dat lukt hen dan niet. De provider wordt dan de zwakste schakel. Een goed, volwassen leverancier selectie- en evaluatieproces is dan vereist.

Canvas thema: key activities

Canvas subthema: ontwikkelen
Gerelateerd risico: code- / ontwikkel- en vertrouwelijkheidsrisico
Classificatie: hoog
Beschrijving: problemen met de kwaliteit van de code leiden tot bugs, kwetsbaarheden en noodzaken tot patches en/of herstelwerkzaamheden. Niet daaraan verbonden problemen kunnen leiden tot cyberrisico's. Kwalitatief, goed codeerwerk leidt tot minder herwerking, meer innovatie en hogere bedrijfsinkomsten. Dat laatste verschil kan meer dan 10% uitmaken en dus behoort codering van goede kwaliteit tot de kern van de dagelijkse activiteiten van een SaaS-bedrijf. Denk echter ook aan vitale sectoren (hoog strategische/fatale incidenten impacts), waar overheid regulerend optreden zal.

Canvas thema: key resources

Canvas subthema: ontwikkelaars
Gerelateerd risico: risico vertrek sleutelpersoneel/kwaliteitsverlies
Classificatie: medium
Beschrijving: een bureaucratische benadering van de schaarse ontwikkelaars, waaronder de hooggekwalificeerde en -getalenteerde Neuro Diverse Persoonlijkheden, zullen deze verjagen. Vaak zijn deze conceptueel gerichte denkers wars van (werk)procedures en documentalisering, terwijl ze tegelijkertijd als geen ander de noodzaak van informatiebeveiliging begrijpen en als persoonlijke noodzaak ervaren. Een pragmatische benadering van deze tegenstrijdigheid bij implementatie van informatiebeveiliging en de eis van compliance moet worden gevonden.

Canvas subthema: code opslag
Gerelateerd risico: gecompromitteerde code en IE-verlies risico's
Classificatie: medium
Beschrijving: kleinere SaaS-bedrijven (MKB) concentreren hun aandacht te veel op de operatierisico's (productieomgeving/werkterrein) in plaats aandacht te behouden voor de code repository, waarvan compromittering kan leiden tot Intellectueel Eigendom (IE-)verlies. Ontwikkelaars en hun laptops zijn een belangrijke risico-aspect. Een concreet voorbeeld: de consequenties van de Russisch-Oekraïense oorlog voor bedrijven met zowel Russische als Oekraïense ontwikkelaars. Een ander essentieel risico: bedrijfsdiscontinuïteit bij verlies van toegang tot de code repository! De beschikbare oplossingen zijn er, maar zeker niet eenvoudig te implementeren.

Canvas thema: channels

Canvas subthema: distributiekanaal
Gerelateerd risico: hacking- & aanvalrisico's
Classificatie: hoog
Beschrijving: een geslaagde hack of aanval schaadt de beschikbaarheid, vertrouwelijkheid en/of integriteit van de informatie. Afhankelijk van de aard van de op het SaaS-platform opgeslagen informatie kan gerichte aanvallen plaatsvinden. Herstel daarvan is vaak kostbaar, gezien de gemiddelde herstelkosten - per gecompromitteerd bestand circa 150 euro - en dat los van de imagoschade. Hackers mogen niet eenvoudig toegang kunnen verkrijgen. Kosten en imagoschade leiden tot inkomstenderving, het risico is dus hoog.

Canvas thema: revenu streams

Canvas subthema: ontwikkeling op maat/standaard
Gerelateerd risico: maatwerk/standaard – risico schaalbaarheid opbrengsten
Classificatie: hoog
Beschrijving: op korte termijn levert software-aanpassing snel inkomsten, op lange termijn kan het lastiger uitvallen en inkomsten doen verminderen. Denk aan de verder ontwikkeling van het kernproduct, leidende tot noodzakelijk onderhoud van de al gerealiseerde aanpassingen, dat voor rekening van het bedrijf komt tenzij er een onderhoudscontract is overeengekomen. In geval van maatwerkoplossingen zal onderhoud aandacht en tijd claimen, waardoor innovatie van het kernproduct kan stagneren. Maatwerk kan vanuit beveiligingsoogpunt riskant blijken te zijn, doordat risico's op bugs en operationele problemen toenemen.

Minimale vereisten NIS2 richtlijn en risico's

NIS2 gaat over risicobeheer. Dus om de minimale maatregelen van NIS2 correct te implementeren, moeten we risico's afstemmen op de minimale vereisten van de NIS2 richtlijn. Laten we de typische risico's analyseren waarmee dergelijke bedrijven te maken hebben en hoe ze zich verhouden tot de richtlijnen, gevolgd door suggesties voor het implementeren van deze vereisten. Let op: dit is een voorbeeld; risico's zijn voor elk bedrijf anders.

Risicothema: kwaliteit van code(-ontwikkeling)

Minimum eis NIS2 - e: veiligheid systemen
Classificatie: hoog
Analyse en implementatie: coderingsstandaarden en regelmatige codebeoordelingen toepassen om kwaliteit te waarborgen. Beleidsintegratie voor het omgaan met en het openbaar maken van kwetsbaarheden, dat aansluit bij de focus van NIS2 op beveiliging bij het verkrijgen, ontwikkelen en onderhouden van systemen.

Risicothema: hacking en aanval

Minimum eis NIS2 - b: incidentafhandeling
Classificatie: hoog
Analyse en implementatie: ontwikkel een incidentbestrijdingsplan met directe beheersings- en uitroeiingsstappen. Train het incidentresponsteam regelmatig, volgens de protocollen voor incidentafhandeling van NIS2, om aanvallen effectief af te handelen.

Risicothema: aanpassing versus standaardisatie

Minimum eis NIS2 - f: effectiviteit cyberbeveiligingsmaatregelen
Classificatie: hoog
Analyse en implementatie: stel een raamwerk op om de beveiliging van aangepaste ontwikkelingen continu te evalueren. Voer effectbeoordelingen uit voor elke aanpassing, rekening houdend met onderhoud op lange termijn en de extra risico's die ze kunnen introduceren.

Risicothema: behoud van gekwalificeerd personeel

Minimum eis NIS2 - g: basis cyberhygiëne en -training
Classificatie: medium
Analyse en implementatie: bevorder een beveiligingscultuur, die de inbreng van ontwikkelaars waardeert. Bied cyberbeveiligingstrainingen aan op maat voor ontwikkelaars om ervoor te zorgen dat beveiligingspraktijken hun tevredenheid niet in de weg staan, zodat talent behouden blijft.

Risicothema: code repository en IE

Minimum eis NIS2 - a: risicoanalyse en beveiliging informatiesysteem
Classificatie: medium
Analyse en implementatie: beveilig code-opslagplaatsen met toegangscontroles. Maak regelmatig back-ups van de repositories en controleer ze om IE-verlies te voorkomen, dit in overeenstemming met de risicoanalyse en het systeembeveiligingsbeleid van NIS2.

Risicothema: hosting- en cloudproviders

Minimum eis NIS2 - d: veiligheid van de toeleveringsketen
Classificatie: medium
Analyse en implementatie: grondige beveiligingsbeoordelingen van hosting- en cloud providers uitvoeren. Ervoor zorgen dat ze voldoen aan de NIS2-nalevingsnormen of deze overtreffen en continue bewaking voor compliance-afwijkingen inbouwen.

Suggesties voor implementatie op basis van risico

Besluit op basis van de in kaart gebrachte risico's de volgende maatregelen voor elk risico op hoog niveau:

1. **supplier lock-in risico:**
   - o Neem clausules op in contracten met hosting- en cloudproviders die naleving van specifieke beveiligingsstandaarden en regelmatige rapportage verplichten.
   - o Plan regelmatige bijeenkomsten met providers om de beveiligingsmaatregelen en naleving van de nieuwste standaarden te bespreken.
2. **code- / ontwikkel- en vertrouwelijkheidsrisico:**
   - o Stel strikte coderingsrichtlijnen op en voer regelmatig controles uit om naleving te garanderen.
   - o Continue integratie en implementatie (CI/CD) pipelines borgen, die geautomatiseerde beveiligingsscans bevatten.
3. **risico vertrek sleutelpersoneel/kwaliteitsverlies:**
   - o Ontwikkel een aantrekkelijk trainingsprogramma voor cyberbeveiliging met gamification en beloningen om naleving van de beveiliging te stimuleren.
   - o Flexibele beveiligingstools en -praktijken implementeren die integreren met de workflows van ontwikkelaars, waardoor wrijving en weerstand worden verminderd.
4. **gecompromitteerde code en IE-verlies risico's:**
   - o Gebruik veilige, gerenommeerde platforms voor codeopslagplaatsen met multi-factor authenticatie en regelmatige toegangscontroles.
   - o Stel als beleid vast, dat alle code wordt beoordeeld en getest voordat het wordt samengevoegd in het kernproduct.
5. **hacking- & aanvalrisico's:**
   - o Ontwikkel een robuust kader voor incidentafhandeling met detectie-, rapportage- en herstelprocessen ten aanzien van mogelijke inbreuken.
   - o Voer regelmatig penetratietests en red team-oefeningen uit om aanvallen te simuleren en responsstrategieën te verfijnen.
6. **maatwerk/standaard – risico schaalbaarheid opbrengsten:**
   - o Voordat een project start is het te adviseren een protocol voor aangepaste ontwikkeling te introduceren, dat ook een risicobeoordelingsfase omvat.
   - o Realiseer een versiecontrolesysteem dat alle wijzigingen logt en in geval van problemen het systeem terug kan zetten naar een stabiele staat.

Taken voor reactie op incidenten en rapportage

Artikel 23 van de NIS2 richtlijnen geeft duidelijk aan hoe en hoe snel organisaties incidenten moeten melden. Deze vereisten zijn geweldig om op te nemen en te bekijken in jouw incident response plan.

Hieronder volgt een samenvatting:

- **Melding van incidenten:** instanties moeten elk belangrijk incident, dat een impact heeft op hun diensten onmiddellijk melden. Dit omvat een vroegtijdige waarschuwing binnen 24 uur en een gedetailleerde melding van het incident binnen 72 uur.
- **Communicatie:** als er een significante cyberdreiging is, moeten entiteiten de beschikbare tegenmaatregelen communiceren naar de getroffen ontvangers van services.
- **Criteria voor een belangrijk incident:** een incident wordt als significant beschouwd als het resulteert in ernstige operationele verstoring of financieel verlies of als het andere partijen kan treffen door aanzienlijke schade te veroorzaken.
- **Terugkoppeling:** het CSIRT of de bevoegde autoriteit moet binnen 24 uur na een vroegtijdige waarschuwing reageren naar de aanmeldende entiteit.
- **Bewustmaking van het publiek:** als bewustmaking van het publiek nodig is, kan het CSIRT of de bevoegde autoriteit van een lidstaat het publiek informeren of de entiteit vragen dit te doen.
- **Samenvattende verslagen:** elke drie maanden moet het centrale contactpunt een samenvattend verslag indienen bij ENISA.
- **Uitvoeringshandelingen:** tegen 17 oktober 2024 zal de Commissie specificeren in welke gevallen een incident als significant wordt beschouwd.
- **Begeleiding:** het CSIRT of de bevoegde autoriteit zal begeleiding of operationeel advies geven over de implementatie van mogelijke risicobeperkende maatregelen.

Conclusie

Na een grondige verkenning van de NIS2 richtlijn en de implicaties ervan op software-ontwikkelingsbedrijven, is het duidelijk dat deze richtlijn een aanzienlijke stap voorwaarts betekent in de evolutie van cyberbeveiliging binnen de Europese Unie. De risicogebaseerde benadering, die centraal staat in NIS2, is een krachtige strategie die bedrijven stimuleert om een meer op maat gemaakte, dynamische benadering van cyberbeveiliging te hanteren. Dit is niet alleen effectiever in een steeds veranderend dreigingslandschap, maar het moedigt ook innovatie en proactieve beveiligingspraktijken aan.

Een ander sterk punt van NIS2 is de nadruk op de beveiliging van de toeleveringsketen. Door de focus te verbreden van individuele organisaties naar hun netwerk van leveranciers en partners, versterkt NIS2 de algehele veerkracht van de digitale infrastructuur tegen cyberbedreigingen.

Hoewel de richtlijn een kader biedt, blijft de specifieke uitvoering ervan in veel gevallen open voor interpretatie. Dit kan leiden tot inconsistenties in hoe bedrijven de richtlijn naleven en hoe toezichthouders deze handhaven. Persoonlijk vind ik een groot gedeelte van de richtlijn maar vaag en de minimale eisen lijken niet sterk te zijn opgezet: elke eis bestaat eigenlijk uit meerdere eisen en het is maar vreemd in elkaar verweven.

Toch ben ik van mening dat NIS2 een positieve stap voorwaarts is in het versterken van de cyberbeveiligingsinfrastructuur binnen de EU. De richtlijn erkent de complexiteit en het dynamische karakter van moderne cyberbedreigingen en biedt een flexibel, maar gestructureerd kader om deze aan te pakken. De uitdagingen in de implementatie zijn echter niet te negeren en vereisen voortdurende aandacht en mogelijk aanpassingen om te zorgen voor effectieve en haalbare naleving, vooral voor kleinere organisaties. Zoals met elke grootschalige regelgevende inspanning, zal het succes van NIS2 afhangen van de samenwerking tussen alle belanghebbenden, de duidelijkheid van richtlijnen en de bereidheid om te leren en aan te passen naarmate de tijd vordert.

Referentie

(1) https://riskmodelcanvas.net/saas-company

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

De veranderlijke identiteit

Het begrip identiteit en hoe we daarmee omgaan speelde een prominente rol in mijn gedachten de laatste tijd. Identiteit en privacy zijn nauw met elkaar verweven en de begrippen komen elkaar in heel veel aspecten van het dagelijks leven tegen. Bijvoorbeeld bij minister Yeşilgöz die onlangs als grootste privacyschender van het jaar werd aangemerkt. Ze is er verantwoordelijk voor dat de identiteit van tachtig Nederlanders onterecht op internationale terroristenlijsten staan, maar ze wil er niets aan doen. Zoek het zelf maar uit, zegt ze. En kaatst zo keihard de bal terug naar de slachtoffers.

Op Europees niveau is aan het einde van het jaar nog verhit gediscussieerd over een voorstel voor een Europese identiteit. Met deze identiteit kunnen burgers zich straks via een app in de hele EU identificeren en elektronisch documenten delen, zoals paspoorten, rijbewijzen en huwelijksaktes. Gebruikerscontrole zorgt ervoor dat enkel noodzakelijke informatie wordt gedeeld. Heel privacyvriendelijk dus ook nog eens.

Rondom identiteit wordt nogal eens desinformatie verspreid – dat hebben we vooral rond de afgelopen verkiezingen tot grote hoogtes gestuwd zien worden. Daarmee wordt een inbreuk gemaakt op de identiteit van personen door er onterechte kenmerken aan toe te voegen of ook te ontkennen dat de identiteit als zodanig bestaat zoals gebeurt bij non-binaire en transpersonen. Om nog maar te zwijgen over het feit dat aan transpersonen vaak zeer privacy invasieve vragen worden gesteld over diens identiteit – vaak gericht op welke geslachtsdelen iemand heeft en of die persoon dat dan gaat opereren.

Het onderwerp identiteit is onderdeel van ons dagelijks leven en soms leidt een beetje boze mail nog eens tot een ethische discussie. Zo wendde zich pasgeleden iemand tot het privacyteam waarmee ik werk. Om aan diens 'Verzoek tot het wissen van persoonsgegevens' te kunnen voldoen moeten we wel eerst de identiteit vaststellen. Want we moeten echt zeker weten dat het niet iemand is die zich zomaar als jou voordoet. Daarnaast moeten wij ook nog om adresgegevens vragen omdat we bij een Universiteit werken en we onder de Algemene wet bestuursrecht (Awb) vallen. Hetgeen tot dubbele verontwaardiging leidde bij de verzoeker. En waar we geen begrip hebben voor de toon waarop dat gebeurde, stelde het ons wel voor de vraag: wat als het moet van de wet, maar je best de vraag kunt opwerpen of het wel goed is? Het vaststellen van de identiteit is echt noodzakelijk, je wilt niet dat een rancuneuze ex of boze buurman zomaar even een verzoek tot het wissen van jouw gegevens kan indienen. Maar dat adres wat de Awb wil, is dat nou echt wel proportioneel en gepast bij een verzoek tot wissen op grond van de AVG?

Identiteit is vloeibaar en hoe we daarmee omgaan is afhankelijk van tijd en plaats. Dat heb ik niet zelf bedacht hoor, vele sociologen hebben daar mooi onderzoek naar gedaan. Maar het geeft ons wel een extra zekerheid in het leven: over identiteit zal nog vaak gediscussieerd worden.

Rachel

Auteurs: Dit artikel is geschreven door het team Informatieveiligheid, onderdeel van de directie Digitale Samenleving bij het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK). We werken met alle bestuurslagen (Rijk/ZBO's, provincies, gemeenten en waterschappen), private partners en wetenschap aan de maatschappelijke taak dat overheden adequaat omgaan met informatiebeveiliging. Voor informatie kijk op: www.digitaleoverheid.nl/contact.

Over risico's en kansen: BIO2 & NIS2

Als we willen dat digitale technologie voor onze samenleving toegevoegde waarde heeft, moet digitalisering waardengedreven en mensgericht zijn. *De Werkagenda Waardengedreven Digitaliseren (1) (zie het kader op pagina 19)* van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (geactualiseerd in 2023) gaat uit van vijf principes. Als we deze principes willen realiseren moeten we als maatschappij met elkaar flinke stappen zetten. In de fysieke wereld hebben we wetten en regels die onze veiligheid waarborgen. Het principe van regels vooraf en toezicht hierop is ook wenselijk in de digitale wereld.

In dit artikel gaan we in op de positie van de Baseline Informatiebeveiliging Overheid (BIO) als belangrijk basis-normenkader voor informatiebeveiliging bij de overheid. Ook geven we een kijkje in de keuken ten aanzien van de recente ontwikkelingen rondom de Europese richtlijn Network and Information Security 2 (NIS2).

Aanloop naar een nieuwe BIO

De Rijksoverheid, Provincies, Waterschappen en Gemeenten werkten allemaal met verschillende baselines (BIG, BIR, BIWA en IBI) (2). Dit was geen ideale situatie. De behoefte groeide om tot één uniforme baseline te komen: de BIO, met een verplichtend karakter op basis van zelfregulering (besluit Ministerraad 2018). Belangrijk is te weten dat de BIO is gebaseerd op de internationale normen: NEN-EN-ISO/IEC 27001:2017 en NEN-EN-ISO/IEC 27002:2017. Ze zijn als verplicht te gebruiken normen opgenomen in de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie.

Doel van de BIO

De BIO is een kader en geeft handvatten om de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen. Invulling daarvan is daar waar mogelijk risicogestuurd. De gedachte is dat ketenpartners in de overheidssector op deze manier elkaar kunnen vertrouwen bij eventuele gegevensuitwisseling. Doel van de BIO is om de informatieveiligheid overheidsbreed op een acceptabel basisniveau te brengen. Daarnaast hebben overheidsorganisaties met de BIO een instrument in handen om extern en intern transparant te zijn over het beveiligingsniveau. Met de invoering van de BIO hanteert de overheid één gezamenlijke taal en doel voor informatiebeveiliging.

Evaluatie en de BIO2

Bij de beslissing om de BIO via zelfregulering te verplichten voor de overheid, werd ook bepaald dat de BIO in 2023 moest worden geëvalueerd en vernieuwd. Ontwikkelingen, zoals de vernieuwde NEN-EN-ISO 27002 haalde de beoogde evaluatie naar voren. Ook werd ondertussen duidelijk dat de NIS2-richtlijn (3) van kracht zou worden. Deze richtlijn biedt de gelegenheid om de BIO wettelijk te verankeren: de zorgplicht van NIS2 wordt grotendeels ingevuld door de BIO. In december 2022 is de evaluatie van de BIO versie 1.04 (4) afgerond. In de analyse zijn de beleidsdoelen opgenomen, de opzet van het instrument BIO en de toetsing en verantwoording. Om ervoor te zorgen dat de huidige BIO meegaat met de ontwikkelingen en dat er wordt aangesloten op de nieuwe nummering en inrichting van de NEN-EN-ISO 27002, is op 1 juni 2023 de handreiking BIO2.0-opmaat (5) opgeleverd. In deze handreiking is dezelfde indeling toegepast: de controls, doelstellingen en overheidsmaatregelen. Ook is er een aantal overheidsmaatregelen geactualiseerd, vanwege nieuwe dreigingen, zoals ransomware.

Ontwikkeling van de BIO2

De ontwikkelingen buitelen over elkaar heen. De overheid moét meebewegen. Een aantal van deze ontwikkelingen zijn bepalend voor de BIO2:

1. Risicomanagement: in de nieuwe BIO komt meer aandacht voor risicomanagement en worden de beveiligingsniveaus (BBN's) losgelaten. Het toepassen van de BBN's werkte in de hand dat de focus op het classificeren van de individuele systemen op de BBN kwam te liggen en daardoor minder op algemeen risicomanagement en de specifieke risico's voor informatiesystemen. Risicomanagement als uitgangspunt van de organisatie is ook in lijn met doelen uit de NEN-EN-ISO 27001 en de NIS2.
2. Voldoen aan wet- en regelgeving: uit de evaluatie blijkt dat het opnemen van verwijzingen naar wet- en regelgeving onduidelijkheid oproept bij de gebruikers. Deze expliciete doelstelling zal daarom verdwijnen uit de BIO2. Verwacht mag worden dat in lijn met risicomanagement een organisatie zelf haar context met de daarin van toepassing zijnde wet- en regelgeving analyseert.
3. Invulling maatregelen NIS2: de NIS2 schrijft de zorgplicht van een entiteit voor en geeft ook definities voor digitale basishygiëne. De maatregelen uit de NIS2 bestaan uit verplichte maatregelen en maatregelen die situationeel zijn. Een gedeelte wordt niet gedekt door de BIO. Vanuit een interbestuurlijke werkgroep BIO is een inventarisatie gemaakt van de aanvullende, noodzakelijke en wenselijke maatregelen op basis van de NIS2.
4. Aandacht voor andere IT-omgevingen: de BIO is een norm voor alle overheidslagen en sluit geen systemen uit. Het is dus belangrijk dat de BIO ruimte geeft om alle omgevingen veilig te maken. Overwogen wordt bijvoorbeeld het aandachtsgebied zorg en Internet of Things (IOT) onder de paraplu van de BIO te brengen.

Vervolgacties doorontwikkeling BIO

De eerste acties zijn gericht op afstemming met de vier overheidslagen. In estafettesessies zijn de CISO's binnen de overheid meegenomen en betrokken in de verdere ontwik-

Toezicht speelt een belangrijke rol in de naleving van wet- en regelgeving

keling van de BIO. De resultaten daarvan worden nu verwerkt in het functioneel ontwerp voor de BIO2. Daarna wordt tot de zomer 2024 gewerkt aan het omzetten van de huidige 'BIO opmaat' naar de BIO2. Als het functioneel ontwerp vastgesteld is, zullen we dit in een vervolgartikel in het iB-Magazine delen.

Toezicht informatieveiligheid bij de overheid

Toezicht speelt een belangrijke rol in de naleving van wet- en regelgeving en meer algemeen in het beschermen van publieke belangen. Toezicht op informatieveiligheid is niet nieuw bij de overheid. Een voorbeeld zijn de DigiD-assessments bij gemeenten; gemeenten moeten vooraf aantonen dat hun informatieveiligheid op orde is om diensten te kunnen aanbieden via DigiD. Wel is het bestaande toezicht versnipperd. Overheidsorganisaties en met name medeoverheden hebben daardoor een forse administratieve last. In de Werkagenda Waardengedreven Digitaliseren is toezicht op informatieveiligheid opgenomen als actie met als doel de bestaande auditlast te verlagen (7). Het organiseren van toezicht wordt verder geholpen door NIS2, waarin toezicht verplicht wordt gesteld. Bij de uitwerking van het toezicht is een aantal uitgangspunten relevant:

1) Het toezicht moet proportioneel zijn en aansluiten bij de te beschermen belangen;
2) Het toezicht wordt vormgegeven op basis van bestaande verantwoordings- en toezichtstructuren in alle overheidslagen;
3) Het toezicht vindt plaats op basis van de BIO;
4) Het toezicht moet onafhankelijk zijn.

Het risico bestaat dat de BIO wordt gebruikt als checklist en dat leidt af van het verbeteren van de feitelijke veiligheid van overheidsorganisaties. Dat wordt een belangrijk aandachtspunt bij de inrichting van het toezicht. In het toezicht zal centraal staan dat overheidsorganisaties risicomanagement hanteren en maatregelen treffen op basis van risicoafweging.

Tot slot

Met de eerdergenoemde Werkagenda wordt hard gewerkt aan een veilige digitale wereld waarin iedereen mee kan doen. De BIO2, in lijn met de NIS2, legt hier een belangrijke basis voor. Er is veel in ontwikkeling: de implementatie van de NIS2 in nationale wetgeving, de ontwikkeling van een nieuwe BIO en de inrichting en het uitwerken van toezicht. Met dit artikel is een inkijkje gegeven in deze ontwikkelingen. De digitale wereld is continu in beweging en het kan verleidelijk zijn om af te wachten hoe deze ontwikkelingen verder gaan.
Ons advies: ga en blijf aan de slag, dreigingen wachten niet op nieuwe wet- en regelgeving. Dus blijf werken aan het verbeteren van de informatieveiligheid binnen je organisatie!

- Hanteer de bestaande BIO om je informatieveiligheid binnen de organisatie op orde te brengen en maak daarbij gebruik van de verplichte standaarden;
- Volg de communicatie over de bredere thema's zoals CSIRT en toezicht. www.digitaleoverheid.nl is dé plek waar alle informatie te vinden is;
- Start in ieder geval met een risicoanalyse, inclusief je leveranciers en andere partijen in de keten.

Werkagenda Waardengedreven Digitaliseren in thema's

1. Iedereen kan deelnemen aan de digitale wereld. We moeten zorgen voor digitale vaardigheden bij iedereen, inclusief het bewustzijn over kansen en risico's van digitale technologie. Online overheidsdiensten zijn makkelijk te begrijpen en toegankelijk voor iedereen.
2. Iedereen kan de digitale wereld vertrouwen. Er is bescherming tegen online criminaliteit, discriminatie en haat zaaien. En online-informatie is betrouwbaar. Overheidsorganisaties zijn weerbaar tegen digitale aanvallen en hebben herstelmaatregelen georganiseerd voor als het toch mis gaat.
3. Iedereen heeft grip op het digitale leven. Iedereen heeft inzicht in en controle over de eigen persoonlijke gegevens en online aanwezigheid. Door gegevens in te kunnen zien, te kunnen delen en te kunnen corrigeren.
4. Als digitale overheid geven we het goede voorbeeld door open en waardengedreven te werken. Hiermee zetten we als overheid de standaard als het gaat om het verantwoord inzetten van digitale technologie.
5. Versterken van de digitale samenleving in het Caribisch deel van het Koninkrijk. Hiermee zetten we als overheid in op verantwoorde inzet van digitale technologie in het Caribisch deel van het Koninkrijk.

Referenties

(1) www.rijksoverheid.nl/documenten/rapporten/2023/12/22/geactualiseerde-werkagenda-waardengedreven-digitaliseren-2024
(2) BIG staat voor Baseline Informatiebeveiliging Gemeenten, BIWA voor Baseline Informatiebeveiliging Waterschappen, IBI voor Interprovinciale Baseline Informatiebeveiliging en BIR voor Baseline Informatiebeveiliging Rijksdienst.
(3) NIS staat voor Network and Information Security. Dit is de nieuwe Europese cybersecurityrichtlijn die organisaties beter moet beschermen tegen cyberaanvallen.
(4) De evaluatie vind je op www.digitaleoverheid.nl
(5) De handreiking BIO2.0-opmaat beschikbaar op www.BIO-overheid.nl
(6) www.digitaleoverheid.nl/werkagenda-waardengedreven-digitaliseren/#Versterken-cybersecurity-Acties

Auteur: Drs. Robert Metsemakers RA RE CISSP is als ervaren auditor en informatiebeveiligingsexpert beschikbaar voor securityadviesopdrachten en bereikbaar op robert.metsemakers@gmail.com.

BLOG

Andersom denken in security

Een Engelse edelman speelde zo graag urenlang kaart, dat hij zijn spel niet wilde onderbreken voor iets onbenulligs als eten. Hij vroeg daarom zijn kok om zijn boterhammen te beleggen met komkommer, zalm en jam, maar bovenop een extra boterham te plaatsen. Dat at gemakkelijker met één hand, zeker omdat de broodkorstjes verwijderd werden door deze medewerker van de Graaf van Sandwich.

Een tweede Engelsman ging graag op jacht. Hij had daarbij wel behoefte aan een warm bovenlijf maar wilde bewegingsvrijheid voor zijn armen bij het schieten. Daarom verwijderde hij van een trui de mouwen. Zo vond de heer Spencer het kledingstuk uit dat men in Vlaanderen meestal 'debardeur' noemt.

Een Engelse uitvinder ging verhuizen, kocht vloerbedekking van vijf meter breed en ontdekte dat zijn nieuwe woonkamer slechts 4.74 meter breed was. Als hij nu eens een klein, maar vlijmscherp mes had waarbij je, wanneer je een tijdje niet hoeft te snijden, het lemmet veilig kunt opbergen in het heft! Ook de heer Stanley verbeterde dus nut en effectiviteit van een bestaand voorwerp (het tapijt) door iets ervan weg te halen.

Piloot en schrijver Antoine de Saint-Exupéry stelde in dit kader (in het Frans): "Perfection is achieved not when there is nothing more to add, but when there is nothing left to take away." Het verschil tussen het topmodel met alle opties van een Duitse automobielfabrikant en de ultrasimpele stapelstoel van een Zweedse meubelleverancier.

Voor securityprofessionals is dat een interessante benadering: kijken of je iets uit het pakket van getroffen beheersmaatregelen kunt weglaten, terwijl het geheel toch nog blijft werken. Kort maar krachtig. Less is more.

Omdenken

Met een Stanleymes kun je ook cabinepersoneel in een vliegtuig bedreigen, zodat ze de cockpitdeur voor je openen. Waar de piloten kunnen worden gedwongen om plaats te maken voor aanvallers. Volgens een populaire complottheorie konden ongeveer 14 samenzwerende kapers van vier vliegtuigen op één dag (11 september 2001) zo de vier cockpits binnendringen. Redteams bij allerlei luchtvaartmaatschappijen bedachten een dag later dat er veel meer levensgevaarlijke voorwerpen in de passagierscabine aanwezig kunnen zijn. Met een hoofdtelefoonkabel of de

'Perfection is achieved not when there is nothing more to add, but when there is nothing left to take away'

85 meter tape in een C60-cassette in een Walkman (loopt op 4,75 cm/s) kun je iemand wurgen of knevelen. Een doorgebroken CD levert vlijmscherpe scherven. Het bij de maaltijd verstrekte plastic bestek of een meegebrachte tandenborstel vormen doorgebroken dodelijk steekwapens. Met een (make up) potlood of balpen in je neusgat of oor snapt iedereen meteen hoe kwetsbaar je hersens eigenlijk zijn. En de geplastificeerde kaart met veiligheidsinstructies kun je als een frietzak oprollen, zodat je met de harde en scherpe punt een purser of stewardess op zijn/haar strottenhoofd of slaap kunt slaan.

Een stukje 'andersom denken' dus. Want zaken, die in beginsel nuttig of plezierig zijn of zelfs een pure securitymeasure zoals die veiligheidsinstructies, kunnen met de verkeerde bedoelingen in tegengestelde richting werken. Het is daarom goed om je als securityprofessional af te vragen: kan die super gebruikersvriendelijke password-reset-via-telefoon-procedure misschien ook misbruikt worden?

Afsluiten

Hobbymessen of 'boxcutters' mag je sinds 11 september 2001 niet meer meenemen in je handbagage. Om de andere genoemde zaken niet óók te moeten verbieden en een toxische sfeer van 'je mag tegenwoordig ook niks meer' te vermijden, besloot men de cockpitdeur in elk vliegtuig te verstevigen, ze naar de passagierscabine toe te laten opendraaien en ze af te sluiten vanuit de cockpit. Hoewel vliegmaatschappijen de klanten en bemanning wel als hun 'crown jewels' zien, koos men ervoor juist de besturing van het vliegtuig door piloten af te schermen van de aanvallers. Daardoor ontstaat in elk geval een 'bottleneck' en in het slechtste geval een SPOF (Single Point of Failure). Je kunt deze oplossing zien als een extreme vorm van netwerksegmentatie. Of als een plaatsgebonden autorisatiemaatregel: alleen de tweede piloot of de gezagvoerder (authenticatie) mag de deur immers openen (autorisatie) en alleen vanuit de cockpit (plaats).

Afsluiten van de cockpitdeur van binnenuit kan op diverse manieren:

1. simpele schuif of haakje;
2. fysieke sleutel;
3. iris- of vingerafdruk-scanner;
4. wachtwoord of pincode.

Schuifje

Een mechanisch schuifje wordt op toiletten veel gebruikt en geeft de gebruiker van de ruimte een bepaalde mate van vertrouwelijkheid door andere mensen de beschikbaarheid van de ruimte te ontzeggen. Mooi is dat een mechanische schuif ook werkt na uitvallen van alle elektriciteit, zoals bij een landing op zee. Dat een eenvoudige schuif of haak niet van buitenaf te openen is, is 'lastig' bij twee bewusteloze piloten tegelijk. Want een passagier met vliegbrevet kan dan niet de besturing even overnemen.

Sleutel

Een fysieke sleutel is een vorm van tweefactor-autorisatie. Behalve wie je bent (de piloot, dus in de cockpit) moet je ook iets 'hebben' om het slot te openen. Een contactloze sleutel, zoals veel personenauto's tegenwoordig hebben is in het vliegtuig ongewenst. Daarmee is immers een relay-attack mogelijk, door met een speciale antenne het radiosignaal van de sleutel op te vangen en dat versterkt opnieuw uit te zenden. Bij een fysieke sleutel is het verder van belang dat het slot niet vanaf de cabinekant toegankelijk mag zijn voor een handige 'lockpicker'. Omdat een vliegtuig (volgens mijn informatie) gestart wordt met een knop, dus zonder contactsleutel, is dit geen pilootvriendelijke oplossing: die lui moeten al aan zoveel dingen denken!

Lockpicker

Vingerafdruk

Een scanner van een iris of vingerafdruk is wel heel hip, maar niet praktisch. De bemanning van vliegtuigen wisselt steeds en je moet dan een database met irisscans en vingerafdrukken van alle piloten in dienst van de vliegtuigmaatschappij in elk vliegtuig opslaan. Of om het echt moeilijk te maken: een aparte database per type vliegtuig waarvoor een deel van de piloten gebrevetteerd is, rekening houdend met wanneer de piloot op herhalingsoefening (examen) moet. Bovendien moet je al deze databases bijwerken bij personeelsmutaties. Daarbij komt dat bij een noodgeval (landing op zee of brand) de scanner niet werkt door gebrek aan elektriciteit.

Pincode

Een pincode bestaat uit cijfers (vaak vier). Een wachtwoord is meestal langer en bevat naast cijfers ook hoofdletters, kleine letters (soms uit andere talen) en bijzondere tekens. Zoals het liggende streepje, maar meestal niet de 'schuine streep' of 'asterisk' — probeer die maar eens. Daarmee is een wachtwoord moeilijker te raden, maar ook veel lastiger om snel in te voeren voor een piloot, die in het algemeen bij een ramp (of plotse diarree) de cockpit snel zal willen verlaten. Ook een pincode werkt helaas alleen zolang er 'stroom' is.

Oude meuk

Met elke gekozen oplossing voor het cockpitslot, komen er dus nieuwe problemen die zelf ook opgelost moeten worden. Vraag je dus als securityprofessional af: welke extra securityproblemen worden veroorzaakt door mijn nieuwe securityoplossing?
Het antwoord op die vraag kan ertoe leiden dat je kiest voor gebruik van een ouderwetse (maar bewezen) securitymaatregel.

Bij alle genoemde afsluitmogelijkheden werkt de eis dat de deur alleen vanuit de cockpit geopend mag worden, als extra beveiligingsmaatregel. Als het beter lijkt dat de deur in noodgevallen toch ook van buitenaf geopend moet kunnen worden, kunnen we het simpele haakje aan de binnenkant van de cockpit niet gebruiken. Daar kun je immers niet bij vanuit de cabine. Men werkt in Amerika aan een elektronische scanner met een 'fail safe' waardoor het slot automatisch opent bij een cabinetemperatuur boven 40 graden Celsius (brand) of bij meer dan 1.20 meter water in de cabine (landing op zee). Deze bestaat echter nog niet.

Het ouderwetse wachtwoord wordt bij tweezijdige toegang echter aantrekkelijker. Het is namelijk de enige optie waarbij degene die het slot opent, het zelf ook echt moet willen. Een vingerafdruk of irisscan kan worden afgedwongen, zeker als het slachtoffer vastgebonden of bewusteloos is. Een fysieke sleutel kan worden afgepakt, door een zakkenroller of gauwdief zelfs ongemerkt. Maar een wachtwoord kan je, ondanks bedreiging of marteling van jezelf of je collega of een passagier, toch voor jezelf houden of bewust drie keer verkeerd invoeren. Omdat het iets is dat alleen jij wéét. In plaats van iets dat je hebt (fysieke sleutel) of bent (biometriescans). Ook dit is daarom een nuttige vraag aan jezelf om je creativiteit te prikkelen: is ouderwetse meuk misschien toch nog steeds de beste oplossing voor mijn actuele securityprobleem?

Of stel die vraag gewoon aan ChatGPT?!

Even voorstellen: Farida Chotkan

Op 9 november 2023 hebben jullie mij aan tafel kunnen zien met de andere bestuursleden tijdens de ALV. Ik ben toen benoemd tot secretaris. Ik neem het stokje over van Erwin Bosma, die na tien jaar stopt met deze rol. Erwin blijft als algemeen bestuurslid tot eind 2024 om de overgang te ondersteunen.

Ik ben inmiddels al twintig jaar werkzaam in het informatiebeveiligingsvakgebied en heb verschillende rollen ingevuld als Risk Manager, Compliance Officer en de Chief Information Security Officer. Deze ervaring heb ik opgebouwd bij verschillende corporates in de sectoren industrie, telecom, logistiek, als in de publieke sector en de juridische sector. Het vakgebied trekt mij aan omdat het vooral 'met mensen werken' betreft. Om de techniek goed in te richten en om de processen op de juiste manier uit te voeren, hebben we mensen nodig die daarbij de juiste kennis en het nodige gedrag met betrekking tot informatiebeveiliging uitdragen. Ik kijk vooral naar het belang van de organisatie, wat het beste in de context past en ik pas het liefst een pragmatische aanpak toe.

Vorig jaar ben ik door Erwin gevraagd of ik zijn rol wil overnemen. Erwin en ik hebben in het verleden samengewerkt. Wat mij vooral drijft om voor PvIB bezig te zijn en een steentje te mogen bijdragen, is het belang van de informatiebeveiligingskennis. Ik heb zelf ervaren hoe je kennis en ervaring opbouwt en ook weet uit te dragen binnen organisaties. Informatiebeveiliging is niet iets wat je 'maar' implementeert, het is de hele organisatie meenemen, het kunnen vertalen en uitleggen in de taal en cultuur van de organisatie en de juiste mensen in de governance ervan te kunnen plaatsen. Met deze bagage kan ik zeker een bijdrage leveren aan dit kennisplatform en haar doelen en ik heb daarom toegezegd deze rol in het bestuur te vervullen.

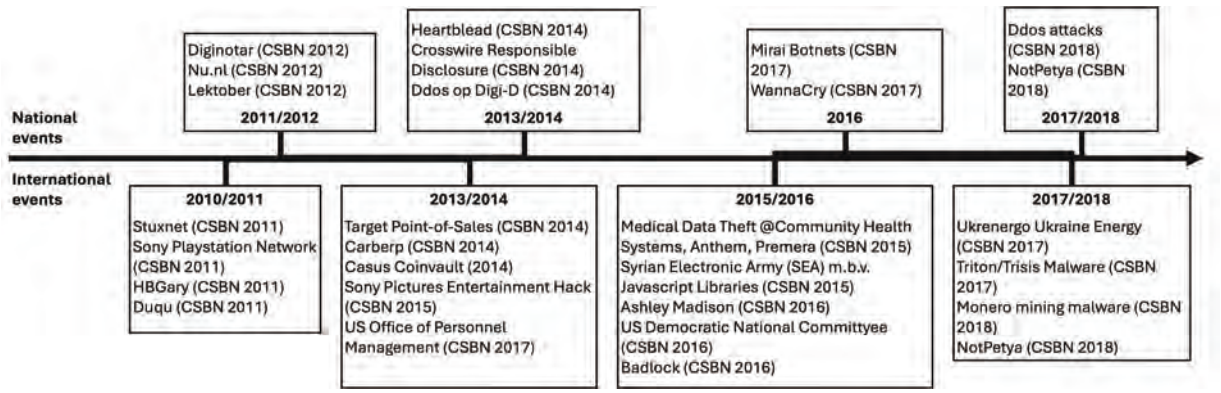
Binnen het PvIB-bestuur zal mijn rol als secretaris ook betekenen 'met mensen werken'. Het lijkt mij een mooie uitdaging om met het huidig bestuur alle betrokkenen en geïnteresseerden in het vakgebied te verenigen, waarbij informatie, kennis en ervaring worden verzameld, verbeterd, verrijkt en weer worden gedeeld. In dit totale proces zal mijn rol als secretaris inhouden het bestuur ondersteunen, informeren en adviseren. Mijn toegevoegde waarde zal vooral liggen in de rol als gesprekspartner voor alle bestuursleden. Samen te werken om het mooiste informatiebeveiliging kennisplatform te mogen verrijken. Het kan alleen maar interessanter worden!
Heb je een vraag of wil je met me sparren over het vakgebied, neem dan gerust contact met me op. We zien elkaar ook vast tijdens een van onze activiteiten!

Farida Chotkan
secretaris@pvib.nl

Auteur: Raymond Bierens is parttime promotieonderzoeker en docent bij het Amsterdam Business Research Instituut van de Vrije Universiteit van Amsterdam. Daarnaast is hij onafhankelijk strategisch adviseur en voorzitter van de stichting Connect2Trust die cross-sectorale dreigingsinformatie deelt uit open en gesloten bronnen. De focus van Raymond bij al deze activiteiten ligt op het beheersen van digitale risico's en cybersecurity bij grote digitale transformaties. Hij is bereikbaar via: raymond.bierens@connect2trust.nl.

Meten is weten… als je weet wat je meet

Cybersecurityincidenten spelen een belangrijke rol bij het schrijven van cyberstrategieën als onderbouwing voor de gevraagde investeringen. Het meten van de effectiviteit van diezelfde cyberstrategieën berust veelal op compliance raamwerken die weer worden bijgesteld aan de hand van diezelfde cybersecurityincidenten. Maar wat als de technologie zich sneller ontwikkeld dan die cyberstrategieën en raamwerken? Rekenen we ons dan niet veiliger dan we werkelijk zijn? Een kijkje in de keuken van een lopend promotieonderzoek.



Figuur 1: Analyse (inter)nationale incidenten in CSBN's Nederland t/m 2019.

In 2022 presenteerde de Nederlandse overheid haar meest recente nationale cybersecuritystrategie. Het jaarlijkse Cybersecuritybeeld Nederland (CSBN) vormt een belangrijk basiselement voor deze strategie en biedt inzicht in de ontwikkeling van dreigingen en risico's in Nederland. Het Cybersecuritybeeld Nederland wordt sinds 2011 uitgegeven wat samenviel met de eerste Nationale cybersecuritystrategie. Daarvoor (in 2007) was cybersecurity nog onderdeel van de Nationale Security Strategie. In 2014 verscheen de tweede cybersecuritystrategie, gevolgd door de Nederlandse Cybersecurity Agenda in 2019 en de nieuwste strategie in 2022.

Van cyberincident tot cyberstrategie

De ondertitels (1) van deze vier cybersecuritystrategieën laten zien hoe de focus van deze strategieën is verschoven van samenwerking en betere bekwaamheden, naar de gevolgen van de steeds sneller digitaliserende samenleving. Onderzoek (2), uitgevoerd in samenwerking met de universiteit ETH Zürich laat zien welke Nederlandse en internationale incidenten worden genoemd en uitgelicht in de diverse dreigingsbeelden. De opkomst van de aanvallen op procesautomatisering (startend met Stuxnet) hebben de noodzaak voor meer bekwaamheden gecreëerd, de gebruikmaking van IoT (o.a. Mirai Botnet) de risico's van het gebruik van IoT.

Het onderzoek, uitgevoerd met ETH Zürich, vergeleek de ontwikkeling van nationale cybersecuritystrategieën in diverse landen (3) en concludeert dat deze strategieën zich hoofdzakelijk reactief ontwikkelen, gedreven door (inter)nationale incidenten. Nieuwe technologische ontwikkelingen worden veel genoemd, maar de meeste aandacht gaat toch naar het voorkomen van deze incidenten. De bestuurlijke inrichting van een land blijkt van grote invloed op de uitvoering van deze strategieën in de onderzochte landen. Een voorbeeld hiervan is de scheiding in Nederland tussen nationale en economische veiligheid, die heeft geleid tot het ontstaan van het Digital Trust Center bij het Ministerie van Economische Zaken en Klimaat, naast het Nationaal Cyber Security Center. Ook al worden deze twee organisaties in de toekomst gebundeld tot één, de bestuurlijke verdeling tussen nationale en economische veiligheid blijft in stand in de vorm van twee opdrachtgevers. In andere landen is deze veiligheidsscheiding er niet en wordt dit ook vertaald in een andere inrichting of ophanging van het Nationaal Cyber Security Center.

De incidenten, en daarmee de nationale cybersecuritybeelden die door veel landen jaarlijks worden gepubliceerd, hebben ook een ander doel. Door de aandacht te vestigen op deze incidenten ontstaat er sociale druk op een overheid om richting te geven aan het voorkomen (of verminderen) van deze incidenten. Dit is tenslotte de basis van ons democratisch bestel en is verankerd in allerlei sociale contracten, zoals bijvoorbeeld de Nederlandse grondwet en het Internationaal Verdrag voor de Rechten van de Mens. Onderzoek (4) toont aan dat de dynamiek van het sociaal contract, of het sociaal cyber contract, ook in de digitale wereld onverminderd van toepassing is. In dat onderzoek werd duidelijk dat dit zich niet alleen beperkt tot de relatie tussen de overheid en de maatschappij, maar ook dat er sprake is van een indirect sociaal cyber contract waarbij de markt enerzijds, en de overheid anderzijds, gezamenlijk proberen organisaties in de private sector te dwingen om maatregelen te nemen om cybersecurity incidenten te voorkomen. Om meer kracht bij te zetten in

De focus van cybersecuritystrategieën is verschoven van samenwerking en betere bekwaamheden, naar de gevolgen van de steeds sneller digitaliserende samenleving

de uitvoering daarvan, werken overheden internationaal samen zoals in Europe rondom de AVG, de CER en de NIS2. Wel blijft er altijd sprake van een zekere geopolitieke spanning, omdat het internet nu eenmaal wereldwijd is en er geen sprake is van een wereldwijde governance.

De NIS scope voor de strategie

De NIS richtlijnen zijn om meerdere redenen een interessant en actueel onderwerp. Niet alleen biedt de NIS door de vorm van een Directive (in plaats van een Act) landen de gelegenheid voor een nationale invulling, waarmee de verschillen in bestuurlijke inrichting kunnen worden gehandhaafd en tegelijkertijd ook het effect daarvan zichtbaar maken. Maar ook omdat de scope van de NIS richtlijn de trend volgt die we ook terugzien in de ondertitels van de nationale cybersecuritystrategieën in Nederland. Deze scope uit de eerste richtlijn (uit 2016) in het kader, inclusief de definitie, van de doorverwijzing naar het elektronisch communicatienetwerk. De richtlijn spreekt in lid b nadrukkelijk over apparaten, groep van apparaten en communicatienetwerken, waarmee zowel de traditionele kantoorautomatisering (IT), als IoT en procesautomatisering (ook wel OT of Operationele Technologie genoemd) binnen de scope valt. Ook de NIS richtlijn speelt daarmee in op de steeds digitaler wordende samenlevingen.

NIS1 (richtlijn (EU) 2016/1148) gebruikt de volgende definitie (in art. 4) als scope:

Netwerk- en informatiesysteem:

a) Een elektronisch communicatienetwerk in de zin van artikel 2, onder a), van richtlijn 2002/21/EG;

b) Een apparaat of groep van geïnterconnecteerde of bij elkaar behorende apparaten, waarvan een of meer, overeenkomstig een programma, digitale gegevens automatisch verwerkt of verwerken, of:

c) Digitale gegevens die via in de punten a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

De doorverwijzing naar richtlijn 2002/21/EG definieert dan: Elektronisch communicatienetwerk: de transmissiesystemen en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt, netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de over gebrachte informatie;

Het is interessant om de scope uit de definitie van de eerste NIS richtlijn uit 2016 te vergelijken met die uit de tweede NIS richtlijn uit 2022. Ook deze definitie is, net als de doorverwijzing voor een elektronisch communicatienetwerk, opgenomen in het kader. Er vallen daarin een aantal veranderingen op:

- De definitie van een elektronisch communicatienetwerk is aangepast en lijkt nu beter aan te sluiten op de cloud-ontwikkelingen;
- Het is niet meer één (groep van) apparaten, maar elk apparaat (of groep) en
- Het doel van de (groepen van) apparaten en/of elektronische communicatienetwerken is verwijderd. Dit betreft de zinsnede: 'met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan'.

NIS2 (richtlijn (EU) 2022/2555) gebruikt de volgende definitie (in art. 6) als scope:

Netwerk- en informatiesysteem:

a) Een elektronisch communicatienetwerk in de zin van artikel 2, punt 1), van richtlijn (EU) 2018/1972;

b) Elk apparaat of elke groep van onderling verbonden of verwante apparaten, waarvan er een of meer, op grond van een programma, een automatische verwerking van digitale gegevens uitvoeren, of

c) Digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b).

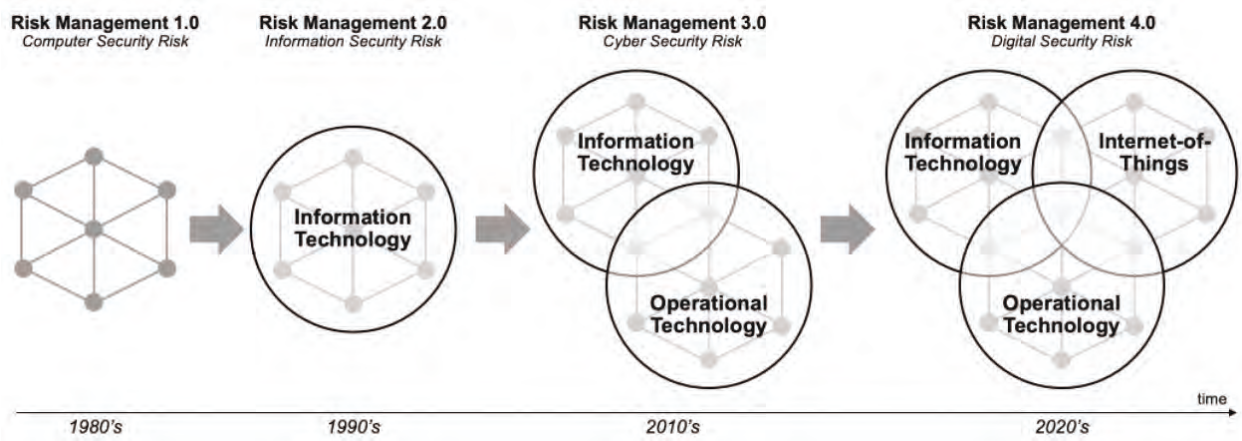
De doorverwijzing naar 2018/1972, artikel 2, punt 1), definieert dan:
Elektronisch communicatienetwerk: de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van signalen worden gebruikt, netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie;

Hiermee is de scope nog iets groter geworden: waren in de NIS1 alle vormen van technologie (IT, OT en IoT) in scope, is dat voor de NIS2 van toepassing op ieder apparaat ongeacht het doel en al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit. Het is deze definitie die de scope vormt van de uitwerking in ieder land naar de nationale wetgeving.

De ontwikkeling van risk management en compliance

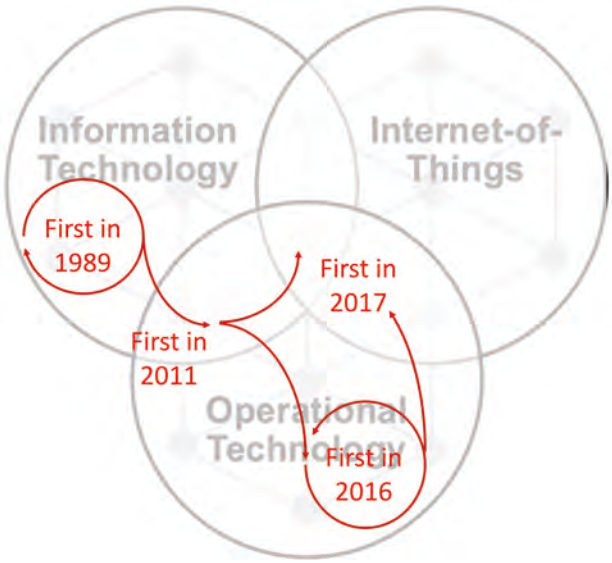
De vraag is nu of de ontwikkeling van compliance gelijke tred houdt met de trends in de internationale wetgeving en nationale cyberstrategieën. Immers, zonder compliance raamwerken, is het niet mogelijk om objectief te meten of er opvolging wordt gegeven aan de strategieën. Hiervoor moeten we kijken hoe, in navolging van de technologische ontwikkelingen en de risico's (en incidenten) die daaruit voortkwamen, compliance en security risk management zich hebben ontwikkeld. Onderzoek (5) naar wetenschappelijke literatuur die ten grondslag ligt aan moderne raamwerken, toont aan dat ook hier een relatie is te vinden met incidenten. Het vakgebied begon in de jaren 80 met het beveiligen van individuele computers. Naarmate deze met elkaar werden verbonden via elektronische communicatienetwerken ontstond een tweede fase van risk management (2.0) waarin nieuwe raamwerken werden ontwikkeld als vakgebied informatiebeveiliging die zich richtte op kantoorautomatisering. De bekendmaking van Stuxnet leidde er in 2011 toe dat er een nieuwe stroming ontstond van risk management (3.0). Deze richtte zich niet op het beveiligen van informatie, maar op het behoud van continuïteit en daarmee kwam ook procesautomatisering (OT) in scope erbij. Vanaf 2016 zijn we, vanuit de steeds digitaliserende samenleving, op weg naar de huidige fase van risicomanagement (4.0). Deze richt zich op elk verbonden apparaat overeenkomstig met de definitie van de NIS1 en NIS2. Figuur 2 (6), hieronder, toont deze ontwikkeling door de tijd, maar ook dat dit geen losstaande risico's zijn. Ze zijn tenslotte veelal aan elkaar verbonden en kunnen dan alleen via een integrale aanpak worden gemanaged.

De vraag is nu of de ontwikkeling van compliance gelijke tred houdt met de trends in de internationale wetgeving en nationale cyberstrategieën



Figuur 2: Transitie van Risk Management door de jaren heen.

Hetzelfde onderzoek (7) dat de ontwikkeling van security risk management heeft onderzocht, keek ook hoe compliance raamwerken zich ontwikkelen als gevolg van diezelfde technologische ontwikkelingen en de risico's (en incidenten) die daaruit voortkwamen. De transitie van risk management 2.0 naar 3.0 laat zien dat er vanaf 2011 sprake is van een 'tussenfase', als nieuwe incidenten bekend worden die worden veroorzaakt door nieuwe technologieën. In deze fase wordt, met behulp van 'oude' maatregelen, geprobeerd om ook deze nieuwe risico's te mitigeren. Een bekend voorbeeld is het omgaan met ransomware bij kantoorautomatisering versus procesautomatisering. Wat bij de ene technologie werkt, kan (veel) grotere gevolgen hebben bij een andere technologie. Pas na het ervaren, soms proefondervindelijk, ontstaan aangepaste of aanvullende raamwerken, als onderdeel van onderkende verschillen tussen de twee. Om die reden gebruiken veel organisaties zowel de ISO27000-serie voor kantoorautomatisering, of de IEC62443 voor procesautomatisering. Sommige sectoren kiezen er soms ook voor om dit nog verder te specificeren naar bijvoorbeeld de Baseline Informatiebeveiliging Overheid (BIO) op basis van ISO, en de Cyber Security Implementatie Richtlijn Objecten, op basis van de IEC62443. Vanaf 2017 zien we hoe, vanuit informatiebeveiliging enerzijds en continuiteitsrisico's anderzijds, er gekeken wordt hoe er met risico's uit andersoortige apparaten, IoT, moet worden omgegaan. Ook hier wordt er dus gestart vanuit de bestaande raamwerken. Figuur 3 geeft deze ontwikkeling grafisch weer.



Figuur 3: Ontwikkeling van compliance in navolging van nieuwe risico's.

Ook op de ontwikkeling van een compliance raamwerk voor het managen van risico's is de werking van het sociaal cybersecurity contract zichtbaar in bij de totstandkoming, de implementatie en handhaving van nationale cybersecuritystrategieën. Bij het schrijven van iedere Nederlandse cybersecuritystrategie is een grote groep bedrijven, non-profit organisaties en overheidsinstel-

lingen betrokken. Bij de ontwikkeling van de CSIR voor procesautomatisering, maar ook bij andere certificeringsprogramma's, is het uitgangspunt 'de markt tenzij' cultureel bepaald. Maar ook bij de ontwikkeling van internationale raamwerken zoals het NIST-raamwerk zijn veel organisaties betrokken, maar volgt het NIST-raamwerk de herkenbare Amerikaanse cultuur; waarbij de president directief (in 2013 en 2021) een opdracht geeft tot het ontwikkelen van een raamwerk en daar dan opvolging aan wordt gegeven. Dit is een duidelijk cultureel verschil met de aanpak in Europa waarbij een richtlijn lokaal wordt vertaald op basis van lokale culture aspecten en kenmerken.

Wat in figuur 3 het meest opvalt, is dat er geen pijltjes voorkomen in de cirkel IoT. We spreken daarom over een vakgebied in ontwikkeling. Het is geen kantoorautomatisering, het is geen procesautomatisering, de risico's en incidenten die het veroorzaakt zijn nog niet grootschalig, en dus is de aandacht voor digital of beter digital-by-design security risk management beperkt. De gevolgen van deze beperking is echter groot: hoeveel cybersecurityoplossingen zijn in staat om alle apparaten zoals de NIS2 voorschrijft: 'elk apparaat of elke groep van onderling verbonden of verwante apparaten' die verbonden zijn met de elektronische communicatienetwerken realtime te inventariseren? En hoeveel organisaties zijn in staat om opvolging te geven aan iedere binnenkomende melding van een kwetsbaarheid en dreiging van al die apparaten?

Ben je dan niet NIS2 compliant als je dat niet kunt? Op dit moment is het antwoord daarop: nee. Want als er geen compliance raamwerk is dat kan worden toegepast of er ontbreken technische oplossingen die het mitigeren van risico's mogelijk maken dan kan een organisatie daar niet verantwoordelijk of aansprakelijk voor worden gehouden. Maar hoeveel bestuurders weten dat ze met compliance op basis van de genomen maatregelen slechts voor een deel hun risico's meten? Om dat te begrijpen moet je weten wat je meet en kun je beginnen met het inschatten wat je restrisico's zijn. En als de geschiedenis van cybersecurity-incidenten ons iets heeft geleerd, is dat er altijd nieuwe incidenten zullen voortkomen vanuit die restrisico's en dat die zullen leiden tot bijgewerkte cybersecurity-strategieën en nieuwe of updates van compliance raamwerken. Maar tegelijkertijd moeten we ons beseffen dat reactiviteit in het proces is ingebakken en we dus altijd achter de feiten aanlopen met restrisico's als onvermijdelijk gevolg. Dat is de prijs die we betalen voor de toenemende afhankelijkheid van technologie in onze maatschappij.

Referenties

(1) 2011: Slagkracht door samenwerking, 2014: Van bewust naar bekwaam, 2019: Nederland digitaal veilig, 2022: Ambities en acties voor een digitaal veilige samenleving

(2) Bierens/Castellon, National Cybersecurity and Cyberdefense - Policy Snapshot of The Netherlands - National Cybersecurity and Cyberdefense Policy_Snapshot of The Netherlands, Center for Security Studies (CSS), ETH Zürich University of Science and Technology, 2019

(3) Oostenrijk, Finland, Frankrijk, Duitsland, Italië, Nederland, Verenigd Koninkrijk en Singapore

(4) Bierens/Van den Berg/Klievink, A Social Cyber Contract Theory Model for Understanding National Cyber Strategies a Social Cyber Contract Theory Model for Understanding National Cyber Strategies, Springer, 2017

(5) Raymond/Shahim, Are We Ready to Manage Digital Risks Today and Tomorrow? Are We Ready to Manage Digital Risks Today and Tomorrow?, Journal of Information Security, 2023

(6) Bierens/Nieuwmeijer, Digital Security Risk Management for data centers, International Federation for Information Processing, 2023

(7) Bierens/Shahim, Are We Ready to Manage Digital Risks Today and Tomorrow? Are We Ready to Manage Digital Risks Today and Tomorrow?, Journal of Information Security, 2023

COLUMN LEX

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

Trends in cybersecurity voor 2024

Wat zal er veranderen en wat kunnen we verwachten in 2024 qua cybersecurity? Artificial Intellegence (AI) is een hype, die ook op dit vlak effect heeft. Ik zie twee aspecten:

1. 2024 wordt een verkiezingsjaar in de VS. Reken er maar op dat dit veel stof zal doen opwaaien in social media. En echt niet alleen in de VS. De hele westerse wereld zal er last van hebben, en het zal moeilijker te herkennen zijn. AI zorgt ervoor dat de slordige rafelrandjes afgewerkt worden. De beïnvloeding wordt subtieler en gerichter. Waar voorheen bot-accounts en misleidende uitingen makkelijk herkenbaar waren, zal dat steeds lastiger worden. Dat heeft uiteindelijk meer effect op de massaopinie.

2. AI kan ook juist helpen met een betere bewustwording. De meeste awarenesstrajecten zijn droge, saaie informatietrajecten. Maar wat als AI een informatietraject op maat kan maken voor elke gebruiker? Ons wellicht veel dichter meenemen naar de bedreigingen, een persoonlijk scenario uitspelen en laten zien dat we erin stinken op het moment dat we het doen? Weg met de standaard phishing e-mails, iedereen zijn eigen leertraject. Hm, misschien ook bewaken dat het in het begin niet te demotiverend wordt.

Een volgend element dat ons veel meer cyberweerstand moet kunnen geven is de Software Bill Of Materials (SBOM). Ik heb er vorig jaar al een column aan gewijd. Het zal geen kwetsbaarheden helpen voorkomen, maar het zal wel helpen ze eerder te vinden en dan hopelijk ook te kunnen oplossen. Maar we staan nog helemaal aan de vooravond van deze beloofde uitkomsten. Dus deze voordelen worden mogelijk pas na 2024 gevoeld. Als software-engineer blijf ik optimistisch over de SBOM.

En dan blijven er twee cyberdreigingen over waarvan ik verwacht dat die in 2024 hun schadelijk werk gewoon blijven voortzetten:

Credential-diefstal is de eerste. Het blijft de grote bron van initiële toegang bij cyberaanvallen. Dat is ondanks het feit dat we weten hoe een sterk wachtwoord eruitziet en hoe een goede tweede factor werkt. Microsoft laat dat met zijn authenticator-app duidelijk zien. Toch worden er nog steeds zwakke wachtwoorden gebruikt en hergebruikt; worden SMS en e-mail als tweede factor gebruikt — en soms worden die als eerste en enige factor ingezet. De grote belofte, die ons hier allemaal vanaf moet helpen, is de inzet van een Zero Trust-architectuur. Maar Zero Trust blijft een complexe zaak, lastig breed te implementeren. En laten we eerlijk zijn: Zero Trust heeft zijn eigen zwaktes.

Als laatste: de ransomware-aanval zal voorlopig nog populair blijven. Grote sommen geld kunnen verdienen met een lage pakkans, met een veilige haven in Rusland — als je je aan de spelregels houdt. Er zijn hele servicetakken opgezet door criminele organisaties. Daar wordt niet zomaar van weggelopen zolang het nog geld opbrengt. Om weerstand te kunnen bieden: zorg dat je goede back-ups hebt. De enige manier waarmee we ransomware echt kunnen uitbannen is geen losgeld meer betalen.

Auteur: Chris de Vries is eigenaar van De Vries Impuls Management een zelfstandige professional, daarnaast is hij hoofdredacteur van iB-Magazine. Hij is bereikbaar via: impuls@euronet.nl.

Titel boek:	**ICT en recht – *Op het snijvlak van legal, security en tech***
Auteur:	mr.ir. Arnoud Engelfriet
Aantal pagina's:	262
ISBN:	978-90-830957-3-8
Uitgever:	Ius Mentis, Amsterdam
Licentie:	Creative Commons
Prijs:	€ 139,50

BOEKREVIEW

ICT en recht – *Op het snijvlak van legal, security en tech*

Boeken over complexe onderwerpen/ domeinen en/of problemen zijn vaak zwaar leesvoer. De deskundigheid van de auteur gekoppeld aan vakjargon is daar vaak de oorzaak van. Hoe interessant het onderwerp ook is, er is dan geen doorkomen aan. Dat blijkt voor dit boek niet op te gaan.

Hoe prettig als een auteur met de voeten in de klei staat en dat ook zo weet te benoemen. Arnoud Engelfriet is zo een man. Hij was mij al opgevallen door zijn blog Ius Mentis waar hij alledaagse problemen en vragen behandelt waarbij recht bij ICT en privacy om de hoek komt kijken. Op heldere en directe wijze benoemt hij het hem voorgelegde (of opgevallen) vraagstuk en geeft vervolgens zijn visie, mening en advies daarop. In het blog stelt hij ook dilemma's aan de orde en daagt hij de lezer uit. Dat leidt niet zelden tot uitgebreide en diepgaande discussies op zijn blogtekst en op andermans reacties. Dit verrijkend voor eenieder, die meediscussieert.
Datzelfde wacht je in het boek. Engelfriet daagt ons allen uit om antwoord te geven op de door hem gepresenteerde casussen en daaraan gekoppelde vragen/opdrachten. En hij gaat zo in gesprek met de lezer, daarmee de klassieke visie doorbrekend dat de lezer passief kennis tot zich neemt en de auteur eveneens passief, achteroverleunend in zijn stoel, tevreden zijn 'magnus opus' bekijkt.

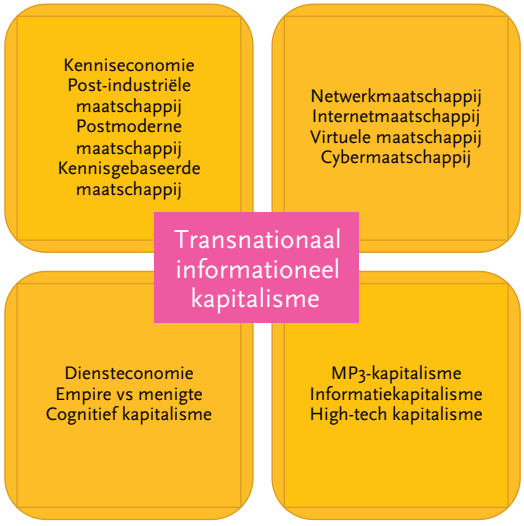
Het boek is verdeeld in 8 hoofdstukken:
1. Naar een afbakening van het begrip 'ict-recht';
2. Internet: de drukpers van de informatiemaatschappij;
3. Het auteursrecht reageert;
4. Via webshop tot cloud: alles wordt dienstverlening;
5. De weg terug naar online privacy;
6. Internet governance en handhaving;
7. Innovatie leidt en de wet volgt;
8. Code as law versus rule of law.

Dit laat zien dat hij het door hem gekozen onderwerp: 'Het snijvlak van legal, security en tech' in de volle breedte benadert, daarbij het juridische aspect als een 'sauce hollandaise' over het gerecht spreidt, maar tegelijkertijd een belangrijk deel van de maatschappelijke betekenis toevoegt als smaakvolle ingrediënten.

Engelfriet acht het aspect van de technologische innovatie belangrijk, hij vertaalt dat als het tot stand komen van grote veranderingen in hoe mensen met elkaar omgaan in reactie op hun angsten en daaruit voortkomende tegenreacties.

Interessant is Engelfriets stelling dat innovaties de basis zijn voor platformvorming, alwaar vele, kleine, incrementele innovaties leiden tot disrupties, zeker wanneer in deze tijd de venture capitalists hun kapitaal erachter zetten. Ik neig ertoe Engelfriet gelijk te geven, getuige de vele hegemonie oorlogen tussen de Amerikaanse multinationals of misschien nog beter geformuleerd tussen de daarachter staande miljardairs die zelfs kooigevechten 'willen' aangaan. Willen is door mij welbewust tussen aanhalingstekens geplaatst. Zie ook navolgende figuur 1.

Engelfriet loopt met ons de industriële revoluties door:
1e: *(Redactie: 1705 Thomas Newcomen & Thomas Savery / 1764 James Watt)*
de stoommachine;
2e: *(Redactie: 1870-1910)* massaproductie, automobielen, communicatietechnologieën met de ontwikkeling van juridische concepten als privacy en auteursrecht. Verder: radar, toepassingen op het terrein van magnetisme en cryptografie, gekoppeld aan elektronica en communicatietechnologie (transistor, ruimtevaart en initieel Kunstmatige Intelligentie;
3e: (1965-2000) de stofzuiger en wasmachine, waardoor de vrouw meer tijd kreeg en daardoor meer ging werken en meer mensenrechten wonnen zoals het verkrijgen van juridische handelingsbekwaamheid. Ook kwamen hier discussies naar boven met betrekking tot het aftappen van privécommunicatie en het vraagstuk van 'eerlijk verkregen bewijs'(?) en
4e: *(Redactie: wij staan er middenin, start 2011 aldus Salesforce, 2016 volgens verkenjegeest (1), die aangeeft dat Klaus M. Schwab, voorzitter van het World Economic Forum het voor het eerst presenteerde)* groei aan mogelijkheden alsook de interactie tussen communicatie- & informatietechnologie. Resulterende in een ongekend brede impact op de maatschappij. Innovatie werd naarmate de tijd vorderde exponentieel, vergelijkbaar met Moores wet aangaande de 'chips'.



Figuur 1: Transnationaal informationeel kapitalisme, pagina 22.

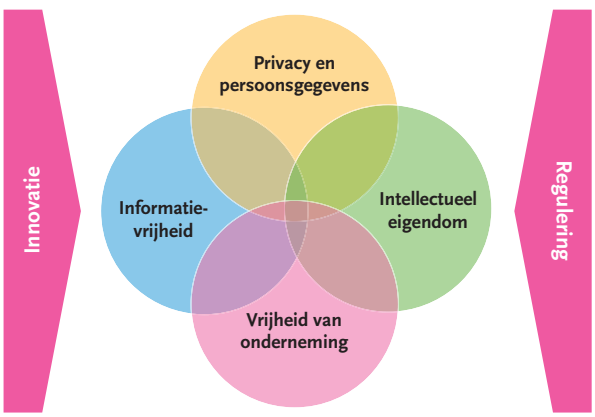
Arnoud Engelfriet gaat vervolgens verder met het omschrijven van zijn 4 grondrechten (hij voegt er zelfs nog een 5e toe) welke de randvoorwaarden zijn voor onze moderne informatiesamenleving. Deze zijn:

1. Informatievrijheid (het mogen vergaren en verspreiden);
2. Privacy (het belang van de burger);
3. Auteursrecht (het belang van de informatieproducent);
4. Intellectueel Eigendom en
5. Ondernemersvrijheid (voortkomende uit het Europees stelsel van grondrechten).

Het 5e grondrecht, wat erop lijkt dat deze is toegevoegd als een achteraf binnengekomen gedachte, lijkt mij van niet te onderschatten belang. Het doelt op de ICT-bedrijven die zich formeren tot platformen, leidende tot gig-economieën op basis van:

- groei van de cloud;
- impact van de IoT en
- transformatie van productie naar cyber-fysieke systemen!

Op pagina 25 laat Engelfriet in een figuur zien hoe de 4 botsende grondrechten (en ik raad de lezer aan hier even goed stil te staan bij de wederkerige werking van deze 4 zo niet 5 grondrechten) beïnvloed worden door innovatie & regulering.



Figuur 2: De vier botsende grondrechten en hun beïnvloeding door innovatie en regulering, pagina 25.

En zo komt Engelfriet uit op het 10-dimensionale model voor regulering van Koops (1). In zijn boek gaat hij er niet diep op in, maar volstaat met een kernachtige samenvatting dat de technische en organisatorische governance van het internet gekenmerkt wordt door:

- het innovatie aspect op de technologie-as;
- het kennis aspect op de regulering-as en
- het discipline definitie aspect op de onderzoek-as.

Het is ook schier onmogelijk om in een boek (dan wel enig ander medium) de 10 dimensies zinvol weer te geven. Maar het intrigerende van een auteur als Arnoud Engelfriet is zijn brede kennis (en belezenheid) en dat riep bij mij dan toch even de nieuwsgierigheid wakker.

Dus als aanvulling op hetgeen Engelfriet schreef hier een toelichting van mijn hand:

- dat er drie spatiale dimensies zijn en
- een tijdsdimensie.

Volgen nu de volle 10 dimensies, op hun beurt weer opgedeeld in:

- technologie gerelateerde dimensies;
- regelgeving gerelateerde dimensies en
- onderzoek gerelateerde dimensies.

Dit leidt tot navolgende figuur:

Technology type	**Technology region**	Research space (multi-dimensional space)
Innovation		
Place		
Time		
Regulation type	**Regulation region**	
Normative outlook		
Knowledge		
Discipline	**Research region**	
Problem		
Frame		

Figuur 3: de 10 dimensies gekaderd in de drie onderzoeksregio's.

Het aardige is dat Engelfriet vervolgens een link legt naar sciencefiction schrijver Arthur C. Clark die in 1968 uitsprak: "Any sufficiently advanced technology is indistinguishable from magic", door te schrijven dat "technologie magie wordt". Het is deze magie, die in dit boek de thema's juridisch, veiligheid en technologie combineert tot een leerzaam, prettig leesbaar boek.

Het boek is onder meer verkrijgbaar via managementboek.nl.

Referenties

(1) E.J. Koops, A.M.B. Lips, Wie reguleert het internet? Horizontalisering en rechtsmacht bij de technische regulering van het internet, in zeven essays over informatietechnologie en recht, SDU 2003, p. 261-315

(2) https://verkenjegeest.com/de-vierde-industriele-revolutie-wat-is-het-en-hoe-zal-het-ons-beinvloeden/

Dimitri van Zantvliet is Directeur Cybersecurity bij de Nederlandse Spoorwegen

COLUMN DIMITRI

Ridder, slijp je veerkrachtzwaard!

De rol van Chief Information Security Officers (CISO's) – vaak vergeleken met heldhaftige digitale ridders – is significant veranderd. Geconfronteerd met een golf van veiligheidsinbreuken bij zowel de grote namen als startups, bevinden deze CISO's zich in een complexe situatie. De vraag rijst of de digitale kastelen zijn gevallen of dat de beschermers van ons informatiekoninkrijk niet voldoende geëvolueerd zijn. Ik begin 2024 daarom met een confronterende bespiegeling die wellicht de goede voornemens kan helpen aanscherpen.

De CISO's staan allemaal voor minstens drie grote uitdagingen:

- Asymmetrische digitale hybride oorlogsvoering: de tegenstanders in de huidige digitale oorlogsvoering zijn vaak krachtiger dan bedrijven, variërend van insiders, cybermaffia tot schurkenstaten. Dit plaatst CISO's in een benarde positie waarbij ze zich onderbemand en onderbewapend moeten verdedigen;
- Exponentiële digitale transities: de digitale wereld evolueert razendsnel en onvoorspelbaar, wat resulteert in verouderende beveiligingskaders en legacy infrastructuur;
- Non-lineaire cyberwetgeving: bedrijven worden inmiddels overspoeld met wet- en regelgeving zoals CSA, NIS2, CER, CRA, etc. wat het lastig maakt voor CISO's om zich te concentreren op hun primaire taak van risico gestuurde weerbaarheid.

Veel CISO's hebben moeite om uit hun geïsoleerde silo's te komen en creëren vaak een lappendeken van beveiligingsoplossingen die in sommige gebieden effectief zijn, maar in andere gevaarlijk tekortschieten. Ze missen soms de essentiële zaken zoals menselijke fouten, interne bedreigingen en basis cybersecurityhygiëne (jawel, daar heb je hem weer).

AI wordt gezien als een veelbelovende ontwikkeling in cybersecurity, maar het is ook een wapen dat door cybercriminelen kan worden gebruikt. De uitdaging voor CISO's is om AI te integreren in hun verdedigingsstrategieën, terwijl ze zich bewust zijn van het potentieel voor misbruik door tegenstanders.
De Zero Trust-benadering, gebaseerd op `nooit vertrouwen, altijd verifiëren', daagt traditionele beveiligingsconcepten uit. Deze aanpak vereist constante verificatie van zowel interne als externe gebruikers, en benadrukt de noodzaak van aanhoudende waakzaamheid.

Laten we het beestje bij de naam noemen: In plaats van `Chief Information Security Officer', is `Chief INsecurity Officer' misschien een passendere benaming. Dit is niet slechts een woordgrapje, maar een realistische weerspiegeling van de huidige situatie. Geen enkel bedrijf kan vandaag de dag beweren 100% veilig te zijn en dat moet men goed beseffen. De doelstellingen zijn veranderd. Het gaat niet langer alleen om verdediging; het gaat om veerkracht. Veerkracht (het vermogen om te anticiperen, weerstand te bieden, te herstellen van en zich aan te passen aan ongunstige omstandigheden) is wat het moderne digitale landschap vereist. Cyberdreigingen zijn een onvermijdelijkheid geworden, geen mogelijkheid.

CISO's, of misschien is Chief Resilience Officers (CRO's) nu wel meer toepasselijk, moeten hun focus verschuiven van enkel `beschermen' naar `aanpassen en herstellen'. Het is mede om die reden dat we met meerdere CISO's de www.cisocommunity.nl zijn gestart om hier verder invulling aan te geven en hier met elkaar best practices over uit te wisselen. Schrijf je in en doe mee!

Want vanaf 2024 ligt de verantwoordelijkheid bij jullie, dappere ridders van de ronde cybertafel: het is tijd om jullie 'veerkrachtzwaarden' te slijpen en je moves te oefenen, zodat je niet slechts een voetnoot wordt in de legendes van digitale verdediging.

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

De hoogste tijd voor een Ministerie van Digitale Zaken

Op het moment dat de kopij van iB-Magazine nummer 1 wordt ingeleverd is het (nog/alweer) verkiezingstijd. Het nieuws wordt gedomineerd door de campagne, de peilingen en de verhalen in de media over achtergronden en deskundigheden van de politici die door hun partij op de lijst zijn geplaatst. Welke kennis van zaken ten aanzien van cyber brengen deze toekomstige volksvertegenwoordigers in voor de komende regeerperiode?

Er is veel digitaal talent uit de Kamer vertrokken en het is nog even afwachten wie de opvolgers zijn. Volt heeft een heel leger ICT-deskundigen op de lijst staan, maar de instroom zal wel beperkt blijven. De vraag is of dat genoeg is. Levert dat beetje deskundigheid dat uiteindelijk in de Kamer actief wordt voldoende input om de uitdagingen die met name uit het digitale domein op ons afkomen aan te kunnen? Moeten we het niet rigoureus anders aanpakken? Het is de hoogste tijd voor een Ministerie van Digitale Zaken!

Leo van Koppen – Sturing nodig

Ik mag hopen dat – op het moment dat je dit leest – er volop ge(in)formeerd wordt. Aan de informateur zou ik graag de volgende boodschap willen meegeven: maak nu ook eindelijk eens een Ministerie van Digitale Zaken mogelijk! De hele samenleving en economie is inmiddels digitaal geworden, zwaar afhankelijk van al die digitale technologieën die over ons worden uitgestort. Met de uitbreiding van AI in het digitale domein, de komst van meer Europese wetgeving voor het digitale domein en de problemen die we dagelijks ondervinden op het vlak van digitale criminaliteit en warfare, neemt de urgentie toe. Het lijkt me in het kader van een 'nieuwe bestuurscultuur' de hoogste tijd om sturing en een passende invulling te geven aan (veilige) digitalisering dat gestalte krijgt via een apart ministerie met een grote reikwijdte.

In het digitale domein is zoveel te doen en met mijn geringe deskundigheid en met het oog op de lezersdoelgroep beperk ik me nu even tot het takenpakket cyber van zo'n MvDZ. Er ligt al een goede


Fook Hwa Tan


Leo van Koppen

cybersecuritystrategie op de plank met een perspectief tot 2028. Dat past dus precies in de beoogde zittingsperiode van vier jaar. Als je dat document (1) erbij pakt dan zie je dat het gaat om vier pijlers:

I. Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties;
II. Veilige en innovatieve digitale producten en diensten;
III. Tegengaan van digitale dreigingen van staten en criminelen;
IV. Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers.

Graag zou ik er dan direct ook aan willen toevoegen: de leefbaarheid in de digitale samenleving of wellicht nog beter te framen als digitale bestaanszekerheid, maar door anderen soms ook wel aangeduid als privacy.

Ik maak de scope van mijn betoog nog weer wat kleiner omdat mijn kennis van zaken zich met name beperkt tot pijler IV. Bij de doelstellingen en de bijbehorende acties van pijler IV staan al enorme uitdagingen geformuleerd zoals (1) het bewustzijn van cyberrisico's bij burgers vergroten. Wat ik wekelijks als vrijwilliger in de bibliotheek (op zo'n digitaal informatiepunt) meemaak is dat het niet gaat om bewustzijn, maar dat enorme gebrek aan digitale kennis en vaardigheden leidt tot angst en grote onkunde. Daar is dus nog een hele lange weg te gaan.

Een ander actiepunt van pijler IV is (2) het aanbrengen van cybervaardigheden in het basis- en voortgezet onderwijs. Dat dient opgenomen te worden in alle curricula! Ja, papier is geduldig, maar hoe zorg je ervoor dat die overbelaste docenten, die toch al steeds nieuwe apen op hun schouders geplaatst zien, deze vaardigheden kunnen aanleren als ze deze zelf onvoldoende beheersen? Daar moet de nodige ondersteuning voor worden ingericht wil dat op korte termijn succesvol kunnen zijn.

En last but not least (3) aandacht voor cybersecurity op de arbeidsmarkt. Cyberspecialisten opleiden is al tijden een enorme uitdaging, via initieel onderwijs, via omscholing en via bij- en nascholing etc. Bijzondere opleidingstrajecten zoals ITvitae of als DIVD-Academy die aansluiten op speciale doelgroepen, zijn prachtig. De vraag die ik al jaren stel is: waar halen we al die deskundigen en de deskundigheid vandaan om de opleiders te ondersteunen in hun taak om al de cyberkennis tussen de oren van de verschillende doelgroepen te krijgen? Formateur en ook PvIB-leden, er wacht u een schone taak!

Fook Hwa Tan – Kritische kijk op de noodzaak van een Ministerie van Digitale Zaken

In een tijd waarin verkiezingskoorts hoogtij viert, blijkt de schaarste aan digitale deskundigheid in de Tweede Kamer een zorgwekkend hiaat. Terwijl de verkiezingscampagnes, peilingen en mediaverhalen over politici de headlines domineren, blijft de cruciale vraag hangen: welke expertise brengen onze toekomstige volksvertegenwoordigers met zich mee op het gebied van cybersecurity? Terwijl de roep om een Ministerie van Digitale Zaken steeds luider klinkt, is het belangrijk om een kritische blik te werpen op de vraag of dit werkelijk de oplossing is voor de digitale uitdagingen waar Nederland voor staat. Hier zijn enkele redenen waarom een dergelijk ministerie mogelijk niet de panacee is die sommigen verwachten.

- Nederland beschikt al over bestaande organen, zoals het Nationaal Cyber Security Centrum (NCSC) en het ministerie van Justitie en Veiligheid, die digitale veiligheid behandelen. Het oprichten van een nieuw ministerie zou kunnen leiden tot overlapping van verantwoordelijkheden en bureaucratie, eerder dan tot een efficiënte aanpak.
- Het digitale landschap evolueert voortdurend, en een statisch ministerie zou moeite kunnen hebben om gelijke tred te houden. Flexibele en snelle reacties zijn cruciaal bij cyberdreigingen, en een nieuw ministerie kan leiden tot trage besluitvorming en implementatie.
- Het pleidooi voor een specifiek ministerie suggereert mogelijk een gebrek aan samenwerking tussen bestaande instanties. In plaats van een nieuw ministerie op te richten, zou de focus moeten liggen op het versterken van samenwerking en coördinatie tussen de reeds bestaande organen.
- Het oprichten van een nieuw ministerie vergt aanzienlijke financiële middelen. In een tijd waarin overheidsbudgetten onder druk staan, moet de vraag worden gesteld of deze middelen niet effectiever elders kunnen worden ingezet, bijvoorbeeld in het versterken van bestaande digitale veiligheidsstructuren.
- In plaats van een algemeen ministerie zou een sectorgerichte aanpak wellicht effectiever zijn. Door samen te werken met experts uit de industrie en het bedrijfsleven kan de overheid gerichte oplossingen ontwikkelen die beter aansluiten bij specifieke behoeften en uitdagingen.

Hoewel de roep om meer aandacht voor digitale veiligheid begrijpelijk is, moeten we voorzichtig zijn met het omarmen van een nieuwe laag van bureaucratie zonder de mogelijke nadelen zorgvuldig te overwegen. Wellicht is het versterken van bestaande structuren en het bevorderen van samenwerking een pragmatischer alternatief.

Referentie

(1) Nederlandse Cybersecuritystrategie 2022-2028 Ambities en acties voor een digitaal veilige samenleving

Jaaroverzicht

Column Privacy

Column Dimitri van Zantvliet

Column Martijn Hoogesteger

Artikelen

(a) artikel (i) interview (o) onderzoek

Jaaroverzicht 2023

(a) Gonzalez Zarzosa, Susana en Villalobos Nieto, Jesus	SOCCRATES – Automation and Orchestration of Security Operations	iB1:26
(i) Guldenaar, Stephan	The Metawar Thesis	iB6:04
(a) Hoogeveen, Abel	Wie bezit GPT-modellen?	iB5:16
(a) Lameir, Dré	AI ofnie?	iB1:18
(a) Langius, Erik en Harmsma, Edwin	Nederlandse partijen bouwen testomgeving voor Gaia-X clouddiensten	iB3:24
(a) Leeuwen van, Marko en Wissink, Wouter	Risicoklassenindeling digitale veiligheid gelanceerd	iB1:30
(a) Muller, Peter	Een bewuste manager is goud waard	iB5:12
(a) Slotman, Jelle	Dark Patterns in cookie consent notices	iB2:16
(a) Stokkel, Marijke en Reijers, Roeland	Hoe je in 10 stappen een cybercrisisoefening organiseert	iB3:18
(a) Tezgel, Stefan	De ontwikkelingen van een vrijwillig cyberleger	iB2:24
(a) Vermeulen Menno	De werking en vele functies van wachtwoordmanagers	iB2:22
(a) Tamo, Saman en Chehin Miguel	Context DrivenData Gathering Framework	iB3:30
(a) Tan, Fook Hwa	The Great 'Risk' Reset	iB1:10
(v) Tan, Fook Hwa	Verbondenheid en kennisdeling op het NSC-One Conference 2023	iB6:10
(a) Schmid, Adrik	Het beheren en beheersen van de moderne informatievoorziening	iB4:14
(a) Verwoerdt, Pasqualle en Borger, Lex	Pre-quantum crypto acties	iB4:20
(a) Wassink, Rob	Ben ik voorbereid op een cyberaanval?	iB5:30
(a) Westerveen, Ronald, Dijk, Rick van e.a.	NIS2: Versterken van Digitale Veiligheid in Europa's Cyberspace	iB5:04

(a) artikel (i) interview (o) onderzoek

Beste lezer,
Ben je enthousiast over een of meerdere bovenstaande artikelen? Laat het ons weten via ibmagazine@pvib.nl Wie weet komen ze in aanmerking voor het Artikel van het Jaar. We zijn benieuwd! Stuur je reactie uiterlijk vrijdag 5 april 2024.

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

COLUMN MARTIJN

Versplintering en oplichting in de georganiseerde cybercrime

Stel je komt in de situatie dat je met cybercriminelen gaat onderhandelen, bijvoorbeeld omdat je bent getroffen door een ransomware-aanval. Vroeger, zes of zeven jaar geleden, hadden criminelen een vaste (kleine) prijs per machine die je wilde ontsleutelen en dat was dat. Tegenwoordig verzinnen ze meer middelen om organisaties onder druk te zetten. Je data wordt gepubliceerd, ze bellen je medewerkers, ze bellen je klanten, voeren DDOS-aanvallen uit, allemaal om je naar de tafel te krijgen om te onderhandelen. Het afgelopen jaar hebben we daarnaast nog wat creatieve uitspattingen gezien. Een bedrijf is bij de Amerikaanse autoriteiten SEC gemeld voor fraude. In een ander geval is het arrestatieteam SWAT ingezet om iemand te intimideren. Het zijn gelukkig zeldzame gevallen, maar we zien dat er creatieve geesten bezig zijn.

Het zijn de grote, georganiseerde groeperingen die deze drukmiddelen verder ontwikkelen. Ze hebben over de afgelopen jaren honderden miljoenen verdiend en zetten dit geld in om nieuwe technieken te ontwikkelen. Maar, hoe groter ze worden, hoe moeilijker het is om de hele groep in het gareel te houden. De afgelopen twee jaar zien we dat steeds meer informatie wordt gelekt uit deze groeperingen. De methodologie als handboek, de code waarmee ze hun ransomware bouwen en zelfs interne communicatie. Het stelt ons in staat om goed te begrijpen hoe deze groepen opereren, maar, er is ook een keerzijde.

Terugkijkend op 2023 hebben we significant meer 'splintergroepen' gezien. Dit zijn vaak kleine groepen criminelen, of soms zijn ze zelfs alleen, die deze tools en technieken hebben gedownload of gestolen en zich voordoen als een geavanceerde groep. Ik heb wel even moeten lachen toen een dergelijke groep zich voordeed als een professionele nieuwe groep, de 'Diamond Ransomware Groep', maar uit de printer bij het slachtoffer nog steeds een losgeldbrief van 'Lockbit' kwam rollen. Dat waren ze even vergeten aan te passen in de code van Lockbit, die je op Github gewoon kunt downloaden. Deze groepen zijn veel minder betrouwbaar en maken soms gekke sprongen. Een interessant weetje: voor veel van deze groepen hebben we gezien dat als je ze helemaal geen aandacht geeft, er een aanzienlijke kans is (47%) dat ze ook niets van je data publiceren.

Recentelijk zagen we nog een variant ontstaan, de 'Scammer in the middle' noem ik hem maar. Ze zien dat een bedrijf gehackt is, bijvoorbeeld op de 'leaksite' (een website waar ransomwarecriminelen hun slachtoffers bij naam noemen). Ze e-mailen vervolgens het bedrijf alsof ze de ransomwaregroep zijn en gaan onderhandelen. Omdat zij alle communicatie onder controle hebben, ook richting de echte ransomwaregroep, kunnen ze zich voordoen als de echte crimineel en proberen zo het geld naar zichzelf toe te sluizen.

Er gaat veel geld om in de criminele cyberwereld en we zien daardoor deze versplintering en opportunisten die wat kruimels proberen op te halen. Het positieve? De gemiddelde kwaliteit van deze aanvallen is zeer laag, dus als je je al goed beschermende, wend je deze kruimeldieven ook af!

PvIB Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

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

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

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

ABONNEMENTEN
De abonnementsprijs in 2023 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E 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

TSTC

ICT en Security Trainingen

Ransomware? Log4j?

ADVANCE YOUR CAREER WITH SECURITY IN 2024

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

GET SKILLED
WWW.TSTC.NL

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

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

SECURITY MANAGEMENT TRAININGEN

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

PRIVACY TRAININGEN

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

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

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

www.tstc.nl

Onze trainingen zijn klassikaal of Live Online te volgen