15 PvIB reconnect in cyber security

iB INFORMATIEBEVEILIGING MAGAZINE

- Terugblik op 15 jaar iB-Magazine
- Algemene Rekenkamer geeft overheid onvoldoende voor algoritmegebruik
- Column: De magie van allowlisting

JAARGANG 22 - 2022 - EDITIE 4

WAT IS ISO 27701?

De 15 meest gestelde vragen over de privacy management norm ISO 27701.

De garantie dat persoonlijke informatie door organisaties op de juiste manier beschermd wordt, groeit. Privacyrichtlijnen zoals de AVG verplichten organisaties om de bescherming van persoonsgegevens te garanderen. De internationale ISO 27701 standaard is een uitbreiding op de bestaande informatiebeveiligingsnorm ISO 27001 en biedt richtlijnen voor de bescherming van privacy. De norm helpt organisaties om informatie op een correcte manier te beheren en privacywetgevingen na te leven.

Vraagt u zich af wat de meerwaarde van ISO 27701 certificering is of wilt u weten of ISO 27701 certificering voor uw organisatie verplicht is? Rob Jansen, IT-security auditor en trainer, geeft u antwoord op de meest gestelde vragen als het gaat om privacy management en de ISO 27701 norm.

Lees de antwoorden op de vragen op www.dnv.nl/watisISO27701 of scan de QR-code.

DNV

Geschiedenis schrijven

Nicole van Deursen

Platform voor InformatieBeveiliging (PvIB) bestaat 15 jaar! We kijken allemaal uit naar het lustrumcongres waar we samen terugblikken en vooruitkijken. Ben je nieuwsgierig hoe de wereld is veranderd in die 15 jaar? Lees dan de column van Lex, hij neemt ons mee in vogelvlucht naar diverse onderwerpen die we 15 geleden nog niet allemaal hadden voorzien. Een ander stuk geschiedenis kun je teruglezen in een artikel over het 10 jarige bestaan van het nationaal detectie netwerk (NDN), het detectienetwerk, waar de AIVD, de MIVD en het NCSC samenwerken.

Verder hebben we in dit magazine een artikel over risicomanagement van CoIT (denk om de hoofdletters, anders betekent het iets heel anders): het verschijnsel waarbij nieuwe informatietechnologie eerst in de consumentenmarkt wordt geadopteerd en daarna naar de zakelijke wereld migreert. Voor wie bezig is met websitebeveiliging of pentesten geeft het artikel van Maarten goede informatie over een specifieke aanvalsvorm: de host header injection. Je kunt er direct mee aan de slag. Er zijn nog veel meer interessante artikelen en columns te lezen in deze uitgave. We zijn 15 jaar jong en er is nog zoveel te ontdekken, vertellen en te schrijven dat we vol enthousiasme doorgaan naar het volgende lustrum!

Nicole

IN DIT NUMMER

RECTIFICATIE

In het artikel over ongestructureerde data beveiligen in iB3-2022 is op pagina 6 in het kader over ABN AMRO per abuis een verkeerde tekst geplaatst. Daar had moeten staan:

"Het probleem van het classificeren van grote hoeveelheden ongestructureerde data binnen organisaties bestaat al heel lang. Er zijn een aantal commerciële oplossingen op de markt, maar deze lossen het probleem niet écht op. We hebben gegevens waarvan we geacht worden dat we er zorgvuldig mee omgaan of waarvan we zelf willen weten waar ze blijven, maar in het geval van ongestructureerde data is er geen gemakkelijke manier voor ons om die gegevens op te sporen. We zoeken een oplossing aan de voorkant om de data te kunnen vinden om deze aan de achterkant te kunnen beveiligen."

Auteur: Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van business continuity-managementsystemen conform de norm ISO 22301. Hij is voorzitter van Business Continuity Management en Crisismanagement normcommissie bij NEN. Gert is bereikbaar via gk@bcmplus.nl.

BCM en hoe wij hier werken

Business Continuity Management (BCM) gaat over het beschermen van uw organisatie tegen de gevolgen van omvangrijke verstoringen en (on)bekende risico's. Dit is anno 2022 geen overbodige luxe. Helaas denken velen onvoldoende na over hoe ze een calamiteit gestructureerd dienen aan te pakken en te overleven, terwijl steeds meer organisaties momenteel ondervinden dat niet voorbereid zijn tóch geen goede 'strategie' is. Hadden we nou toch maar een Plan B. Maar 'hadden is wanneer hebben is geweest'.

Gebeurtenissen als Brexit en de coronacrisis hebben we voor uw gevoel misschien al achter ons gelaten, maar is dat wel zo? Sorry, maar er volgt helaas meer. Wat, wanneer en hoe, blijft ongewis, maar op dit moment zien we onder andere door de situatie in Oekraïne spanningen op de grondstoffenmarkten ontstaan, specifiek olie, gas en graan. Kunt u straks nog produceren en gaat men weer hamsteren? Ook op het gebied van cybercrime, mede door de spanningen en houding van Rusland, vindt veel plaats wat ons niet geruststelt. Dat u zich zo optimaal mogelijk dient voor te bereiden lijkt duidelijk. En als er al inspanningen worden verricht in dit kader, dienen organisaties aldus te zorgen voor een effectief Plan B voor wanneer dit nodig is, als het er écht op aankomt. Geen papieren tijgers dus, bijvoorbeeld ter 'geruststelling' van de buitenwacht. Hier spelen naast oefenen en testen, onderhouden en verbeteren ook de interne audits een belangrijke rol. ISO 9001 (kwaliteit), ISO 14001 (milieuzorg) en bijvoorbeeld ISO 27001 (informatiebeveiliging) zijn inmiddels bekende normen binnen organisaties. Deze zijn, met in het vizier het 'Risk Based Thinking' thema van de kwaliteitsnorm, te verrijken door direct aan het bestaande managementsysteem Business Continuity Management toe te voegen, al dan niet gecertificeerd volgens ISO 22301 (BCMS).

'Voorbereiding is 90% van het resultaat'

Bedrijfscontinuïteit kan worden omschreven als het vermogen van een organisatie om tijdens een verstoring producten en diensten met een vooraf vastgestelde capaciteit binnen aanvaardbare tijdskaders te blijven leveren (ISO 22301:2019). Het belangrijkste deel uit deze definitie is 'een vooraf vastgestelde capaciteit binnen aanvaardbare tijdskaders'. Dit betekent dat u dient te weten wat die capaciteit is en wat deze aanvaardbare tijdskaders zijn. 'Voorbereiding is 90% van het resultaat', zouden we op een BCM-tegeltje kunnen zetten; maar dat is wel waar het over gaat: zo optimaal mogelijk voorbereid zijn. BCM is daardoor het complete managementproces dat mogelijke gevaren met betrekking tot de continuïteit van de bedrijfsvoering vaststelt en een kader schept voor het opbouwen van weerstandsvermogen en veerkracht (resilience). Door effectief reageren worden de organisatiebelangen, reputatie en ook het merk bewaakt. Ook wordt de uitvoering van de waarde creërende activiteiten gewaarborgd.

De invulling met betrekking tot 'Wat te doen in geval van een verstoring of calamiteit?' wordt in een belangrijke mate bepaald door een aantal factoren. Welke activiteiten (met de juiste prioriteit) betreft het en vervolgens welke en hoeveel mensen en middelen heeft u daarvoor nodig – wellicht meer of andere ten tijde van een calamiteit? Denk hierbij aan welke data, machines, gereedschappen, IT-applicaties, formulieren, leveranciers, nodig zijn en of er nog eisen zijn aan de werkplek en logistiek. U hoeft wellicht niet altijd direct 100% te functioneren, maar welk percentage dan wel, met welke machines en bezetting, welke producten of diensten voor welke klanten? Gaan bepaalde klanten voor, wilt u uw productportfolio in een bepaalde volgorde beschikbaar hebben en leveren of wilt u eerst bepaalde processen met voorrang hebben opgestart?
Wat hiermee een sterke associatie heeft is het woord 'afhankelijkheid'. Hoe afhankelijk bent u van de aanwezigheid van (alle/specifieke) medewerkers, de beschikbaarheid van IT-applicaties, of die ene leverancier of werklocatie? Voorts antwoord op de vraag: is er sprake van Single Point of Knowledge or Authority (medewerkers), van Single Point of Failure (IT-applicaties, machines of de werklocatie) of van Single Sourcing

(leveranciers)? Vanuit het principe van BCM wil je opties hebben om je scenario te kunnen bouwen met alternatieven, vanzelfsprekend rekening houdend met reële mogelijkheden. Alles drievoudig uitvoeren zou fijn zijn, zoals triple redundant datacenters, maar in de meeste gevallen is dat een onbetaalbare optie. Aan de andere kant alles 'single' uitvoeren lijkt wellicht een goed plan vanuit efficiency, bezetting en kostenbesparing (lean en mean), maar is ongewenst en een onacceptabel risico. Tijdens de coronacrisis hebben veel organisaties dit aan den lijve ondervonden. Plannen maken voor 'als hét gebeurt' is vanzelfsprekend een uitstekende strategie, maar we moeten de kans dat een activiteit wordt geraakt zien te verkleinen en zeker ook de mogelijke impact minimaliseren. Verder is het een voorwaarde de bedreigingen (of risico's) te mitigeren, dus ook daar de kans of impact en eventueel de periode dat we last hebben van de gevolgen. Het uiteindelijke doel is niet verrast te worden, wat er ook gebeurt, en nooit de controle te verliezen over de situatie en uw reactie op de calamiteit.

Hoe wij werken

Waar helaas vaak minder aandacht voor is, is het borgen van BCM in ons DNA, in 'hoe wij hier werken'. Een voorbeeld is het samen met Supply Chain Management beoordelen van al onze leveranciers, de belangrijkste eruit filteren en deze beoordelen op hún vermogen om ons onder alle omstandigheden te kunnen leveren wat wij nodig hebben. Beoordelen wat hún BCM-vermogen is, gekoppeld aan onze eisen in dat kader. Of we wel of niet een vuist kunnen maken en eisen kunnen stellen ligt mede aan onze omvang en positie, maar een project uitvoeren om deze mogelijke zwakke plekken in onze verdediging aan te pakken mag niet worden verzaakt. Wanneer we echter niet tegelijkertijd BCM meenemen in het inkoopproces als cruciaal selectie- en beoordelingsonderwerp en BCM-gerelateerde contractvoorwaarden opstellen voor (nieuwe) contracten die worden onderhandeld of herzien, dan laten we de achterdeur openstaan en komen er mogelijk weer nieuwe problemen bij die we nou net aan het oplossen zijn. Voorkom 'afhankelijkheid' van (nieuwe) leveranciers en grotendeels onnodige risico's of kom tot de conclusie dat dit lastig tot onmogelijk is en mitigeer dit op een andere wijze (voorraadniveaus, alternatieven voor wat ingekocht wordt).

Mensen

Wanneer uit analyses binnen het BCM-programma Single Points of Knowledge or Authority naar boven zijn gekomen, dient dit te worden aangepakt. U heeft deze wellicht opgelost door het mogelijk te maken dat meerdere mensen bepaalde taken kunnen uitvoeren (crosstraining) of u hebt werkzaamheden dusdanig ingericht dat mensen rouleren over de afdeling en meerdere rollen kunnen vervullen (jobrotation) of er is aandacht voor betere vastlegging van taken en werkvoorschriften. Wat kan gebeuren is dat na een reorganisatie of voortgaande automatisering bespaard kan worden op personeelskosten door functies te laten vervallen en werkzaamheden samen te voegen. De kans is groot dat, wanneer u geen oog heeft voor BCM in dit kader, u toch weer afhankelijkheid van mensen en functies creëert die net opgelost zijn. Wanneer dit niet binnen afdelingen geregeld kan worden kijk dan hierbuiten of zelfs naar externe back-up, maar accepteer dit niet zonder alternatieven voorhanden te hebben voor het geval dat.

ICT

Als laatste voorbeeld ICT. In de ICT is het managen van continuïteit dé nummer één prioriteit. Sterker nog, wij eisen van de ICT-functie binnen onze organisatie minimaal 99,99% betrouwbaarheid en beschikbaarheid (CIAC: Confidentiality, Integrity, Availability, Currency). Zeker wanneer deze is uitbesteed aan een derde partij, wat steeds vaker het geval is. De bekende cloud, oftewel de opslagruimte van iemand anders. Er mag niets gebeuren en als er iets gebeurt, moeten we zo snel mogelijk verder kunnen zonder al te veel vertraging en dataverlies. De afgelopen jaren is men zich gaan realiseren dat dit eigenlijk zou moeten gelden voor álle belangrijke functies binnen de organisatie. Met de ICT-eisen vanuit de kritische, geprioriteerde activiteiten die in geval van een calamiteit het eerst hersteld moeten worden, kunnen we wederom samen met ICT werken aan de snelle beschikbaarheid van de juiste applicaties. Ook voor de benodigde toegang tot schijven, het intranet en vanzelfsprekend anno 2022 het onmisbare internet. Ook hier is Single Point of Failure, een applicatie zonder dat we daar een redelijk alternatief voor hebben bij uitval, weer een aandachtspuntje (understatement). Sluiten de eisen (requirements) vanuit de organisatie over deze ICT-elementen wel aan op de mogelijkheden c.q. het vermogen (capability) van de ICT-afdeling? Zo niet, hoe gaan we dat oplossen? Wederom een project om ervoor te zorgen dat eisen en verwachtingen worden afgesteld op mogelijkheden en realiteit. Ook hier geldt weer dat u over nieuwe applicaties die geïntroduceerd worden of die één of enkele anderen gaan vervangen, na dient te denken over de BCM-kant van de medaille. Sluit de hersteltijddoelstelling (RTO Recovery Time Objective) en het verlies aan data wanneer de betreffende applicatie faalt als gevolg van de gekozen back-upstrategie vertaald in het herstelpunt (RPO Recovery Point Objective) aan op de eisen van de organisatie en creëer niet wederom een afhankelijkheid. De schouders ophalen en stellen dat dit nu eenmaal zo is, kan nooit een acceptabele conclusie zijn. Een

andere manier van werken als alternatief bij falen wel.

Het woord 'afhankelijkheid' zo blijkt, is onlosmakelijk verbonden met BCM. U wilt streven naar zo min mogelijk afhankelijkheden in uw organisatie. Dit verlaagt uw risico op onacceptabele impact tijdens en na ernstige verstoringen. Wellicht zelfs het verschil tussen overleven als organisatie of onherstelbare schade oplopen.

Naast deze drie voorbeelden is het uitermate verstandig ook dezelfde denk- en werkwijzen los te laten op middelen als de werkplek, machines en installaties en de vervangingsprojecten daarvan in het bijzonder (twee oude machines vervangen door één grote nieuwe klinkt goed, maar is dat ook zo?). Denk ook in het verlengde van leveranciers aan uw zakenpartners, eventuele dealers en mogelijk logistiek en transport. Een managementexercitie met als doel: alle afhankelijkheden binnen uw organisatie helder krijgen en die vervolgens door deze denk- en werkwijze heen halen is naast leerzaam, mogelijk het begin van het verhogen van uw weerstandsvermogen en veerkracht, uw resilience.

Aanbevelingen

Binnen BCM wordt in ieder geval van de kritische, geprioriteerde activiteiten een blauwdruk gemaakt. Welke mensen en middelen zijn nodig om deze activiteit uit te voeren? Wat zijn eventuele interne en externe afhankelijkheden? Waar in de keten (binnen een proces) is de activiteit geplaatst? Alles om hiermee aan de slag te kunnen zoals hierboven vermeld, maar bij 'Hoe wij hier werken' hoort ook het beschikbaar hebben van alternatieven en verminderen van kans en impact op de activiteit als het een keer goed misgaat. Denk niet dat het u niet gebeurt, want dat het iedereen kan overkomen hebben de afgelopen twee jaren ons wel geleerd. Voor de voornaamste mensen en middelen (Resources) kun je in dit kader denken aan:

Mensen: denk aan meerdere mensen die iets kunnen en zorg ervoor dat voor alles wat moet gebeuren meerdere mensen beschikbaar zijn. Het 1-3 en 3-1 principe wordt dit wel genoemd in de productie. Iedereen moet drie rollen kunnen uitvoeren, machines kunnen bedienen of aan drie lijnen kunnen werken, terwijl voor elke rol, machine of lijn u een driedubbele bezetting moet hebben (back-up). Zoals hiervoor genoemd zijn cross-training, jobrotation en soms zelfs het gebruiken van externen (naast onze eigen Technische Dienst bijvoorbeeld) opties. Het goed vastleggen van taken en werkvoorschriften lijkt een open deur, maar onderzoek dit eens in uw organisatie en kijk vooral naar hoe recent de laatste update hiervan is. Succession planning, opvolging van de vergrijsde populatie in veel organisaties, mag ook niet ontbreken op de lijst van mogelijkheden.

Informatie, gegevens en ICT: hier is al op ingegaan. Dit is te allen tijde nodig en dus is de focus op betrouwbare, actuele gegevens die beschikbaar zijn als u ze nodig hebt (CIAC). ICT-afhankelijkheid is eerlijk gezegd bij veel organisaties op een onacceptabel niveau en men geeft zelfs grif toe dat áls ICT plat gaat, men hele grote, serieuze problemen heeft. Hoe dat dan? Verminder de afhankelijkheid, zorg voor alternatieven, soms manueel wellicht, denk ook aan anderen die u kunnen helpen, maar regel dit van tevoren en niet pas als het misgaat.

Werkplek en faciliteiten (nutsvoorzieningen): denk aan een uitwijklocatie, binnen of buiten de organisatie. Niet voor alles en iedereen is thuiswerken een optie. Dit vergt voorbereiding, zoals we allemaal hebben gemerkt in het begin van de coronapandemie, toen we niet meer mochten werken op onze vaste werkplek. Gaat u voor een tweede locatie waar u hetzelfde gaat doen, dus verdelen van de werkzaamheden (diversification), of zorgen dat u op een andere locatie direct kunt overschakelen (replication) of dat u op korte termijn de werkzaamheden kunt overdragen (stand-by)? Pas gaan bedenken wat te doen als het gebeurt, is niet verstandig. U kunt ook gaan voor het laten uitvoeren van werkzaamheden door andere mensen op een andere locatie, bijvoorbeeld in noodsituaties uitbesteden van callcenteractiviteiten aan een derde gespecialiseerde partij. Ook hier is een gedegen voorbereiding nodig. Qua faciliteiten kan gedacht worden aan een voorraad water, gas of olie als u daar afhankelijk van bent of een noodaggregaat op de locatie die in ieder geval de kritische activiteiten kan bedienen.

Machines en installaties: voorkom zoveel als mogelijk de Single Point of Failure situaties en beknibbel niet (té veel) op voorraden reserveonderdelen. Niet té snel of makkelijk de oude machine inruilen bij aanschaf van een nieuwe als deze een onderdeel vormt van een kritisch proces. Denk ook hier aan eventuele externe mogelijkheden. In de zuivelindustrie worden voor complexe verpakkingslijnen vaak afspraken gemaakt met concullega's over het gezamenlijk houden van voor de voorraad peperdure onderdelen. Op deze wijze kun je de kosten in de hand houden. Ook in dit geval gaat het weer om betrouwbare leveranciers en voldoende alternatieven.

Transport en logistiek: het begint op elkaar te lijken, maar ook hier geldt dat één vervoerder, waar u misschien al jaren zaken mee doet, een risico kan vormen. Wanneer u transport en

Als u in een situatie zit waarbij u weinig kunt sturen, deal daar dan mee en bedenk op welke andere wijzen u zich kunt voorbereiden op het (on)verwachte.

logistiek in eigen hand hebt is het tóch verstandig een alternatief achter de hand te hebben. Denk na over de gevolgen van extreem weer, vervoersstaking (ook OV) en hoe u eventueel personeel verplaatst. Regel vooraf met externen hoe het proces is ingericht rond het op stel en sprong verplaatsen van voorraden en de normale goederenstromen van en naar uw uitwijklocatie.

Leveranciers en partners: ook dit onderwerp is in een eerder voorbeeld rond Supply Chain Management besproken. Het is als rode draad door dit verhaal duidelijk geworden dat externe afhankelijkheden lastig kunnen zijn. Heeft u alternatieven, is dit mogelijk? Als u in een situatie zit waarbij u weinig kunt sturen, deal daar dan mee en bedenk op welke andere wijzen u zich kunt voorbereiden op het (on)verwachte.

Ergo, net als bij onderwerpen als kwaliteit, veiligheid en informatiebeveiliging moet ook continuïteit onderdeel worden van 'Hoe wij hier werken' en dat is nu écht nog niet het geval. Hoe is dat bij u?

Dit artikel is eerder verschenen in Kwaliteit in Bedrijf mei/juni 2022

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Privacypraat

Privacy is een levend aspect van ons dagelijks leven. Vooral als het onder druk komt te staan geeft het ruimte tot mooie discussies. Waarna en waardoor ons beeld over wat we privaat vinden weer bijgesteld wordt. Discussie is niet alleen nuttig, maar ook essentieel om samen te begrijpen waar de grenzen zitten aan inmenging in het leven van iedereen. Welke zaken moet je de komende tijd in de gaten houden? Ik zet er vier voor je op een rij.

Ten eerste is daar het voorgestelde plan van de EU om kindermisbruik terug te dringen. In de voorstellen zijn voorzieningen opgenomen om online berichten te monitoren, denk aan het inhoudelijk kunnen bekijken van chatberichten van diensten zoals Whatsapp en Signal. Hoewel het doel nobel is, zal de kern van de discussie zich gaan richten op het feit dat dit een forse privacyinbreuk oplevert voor iedereen omdat hiermee de end-to-end encryptie doorbroken moet worden. Daarnaast zal ook ongetwijfeld het 'wij hebben geen boodschap aan de boodschap' argument met dit voorstel weer nieuw leven worden ingeblazen.

Een tweede interessante ontwikkeling werd zichtbaar in recent onderzoek van de Autoriteit Persoonsgegevens (AP). Er is een explosieve toename van het aantal datalekken dat veroorzaakt wordt door cyberaanvallen waarbij vooral IT-leveranciers een gewilde aanvalsplek zijn. Daarmee wordt immers snel toegang verschaft tot veel persoonsgegevens bij een veelvoud aan afnemers van de betreffende diensten. De discussie zal zich zeker gaan richten op vragen als aansprakelijkheid en verwijtbaarheid, waarbij het te makkelijk is die alleen op de rug van de IT-leveranciers te plakken. Ook afnemers van diensten hebben immers de verplichting zich ervan te verzekeren dat ze met partijen in zee gaan die de zaken goed op orde hebben.

Een derde zorg zit hem in wetgeving rondom bestrijding van witwassen en terrorismefinanciering. Recent sprak de European Data Protection Board (een orgaan waar alle Europese privacytoezichthouders in vertegenwoordigd zijn) diens grote zorgen uit over de negatieve privacyimpact van dergelijke wetgeving. Daarnaast opperde zij zorgen over onterechte labels die op personen worden geplakt. Iets waar wij in Nederland in de Zorgtoeslagaffaire helaas veel ervaring mee hebben. Hier zal zeker de vraag spelen of je wel zomaar allerhande gegevens mag verzamelen om een bepaald kwaad te bestrijden en waar dan precies de grenzen liggen.

Een vierde belangrijk punt komt uit het in april gepubliceerde jaarverslag van de AP. Zij stellen dat zij te vaak Nederlandse wetsvoorstellen voorbij zien komen waarin het verzamelen van gegevens centraal staat, het ging om maar liefst 95 voorstellen in 2021. 'De AP heeft de indruk dat het kabinet wetsvoorstellen vaak ziet als een vrijbrief voor de overheid om bijna ongelimiteerd persoonsgegevens van burgers te verzamelen, op te slaan of te verspreiden.' Onlangs heeft de Eerste Kamer al een startsein gegeven voor een maatschappelijke discussie door het verlengen van de coronanoodwet te blokkeren omdat zij geen enkele noodzaak meer zag voor een wettelijke vrijbrief tot het nemen van extreem inbreukmakende maatregelen.

Ik wens jullie veel wijsheid en discussieplezier, maar vooral ook veel privacy voor eenieder!

Rachel

Auteur: Peter van Schelven is zelfstandig IT-adviseur bij BIJ PETER – Wet & Recht te Oudewater.
Peter is te bereiken via: linkedin.com/in/petervanschelven.

Security-geschillen: arbitrage als alternatief voor de rechter?

Uiteraard wens je dat de nieuwste bedreigingen op het vlak van informatiebeveiliging voor jouw organisatie dagelijks in de gaten worden gehouden, zodat je zoveel mogelijk beschermd blijft. Je kunt vanzelfsprekend besluiten zelf de nodige hard- en software in huis te halen, maar je kunt er ook voor kiezen om bepaalde 'managed security services' aan een gespecialiseerd bedrijf uit te besteden. Wat je ook kiest, in alle gevallen ga je met een externe leverancier van producten of diensten een of meer contracten aan. Dat kan een eenvoudige licentie- of koopoverkomst zijn, maar ook een complex security-contract met op security toegesneden SLA-afspraken. De praktijk kent inmiddels een veelheid aan complexe security-diensten met bijbehorende specifieke contracten, bijvoorbeeld voor kwetsbaarheidsanalyses, monitoring van netwerken en end-points, pentesten, forensische dienstverlening en het verlenen van SOC- en SIEM-diensten.

Ook als je de opslag en verwerking van bedrijfsgegevens aan een andere partij wenst uit te besteden, bijvoorbeeld een hostingbedrijf of cloudprovider, dan maak je, als je verstandig handelt, in het contract passende afspraken over de security die je verlangt. Gaat het om persoonsgegevens, dan biedt de Algemene Verordening Gegevensbescherming (AVG) daarvoor, zoals bekend, aanknopingspunten. Kortom, contractuele afspraken over security zijn belangrijke, maar niet zelden ook zeer complexe aandachtspunten. Als afnemer neem je in het contract niet alleen op wat je precies van de security-producten en -diensten verwacht, maar ook wat er gebeurt als je onverhoopt in die verwachtingen teleurgesteld wordt, bijvoorbeeld omdat de producten en diensten niet de betrouwbaarheid en kwaliteit blijken te bieden die je hebt afgesproken.

Security-geschillen

Een bijzonder punt van aandacht bij het aangaan van contracten op het gebied van security is de geschillenregeling. Naar welke geschilleninstantie stap je als er een conflict tussen de leverancier en afnemer ontstaat wegens vermeende gebrekkigheid van een aangeschaft security-product of -dienst of wanneer sprake is van een ernstig security-incident dat aanleiding geeft tot claims? Of, aan wie leg je de beslechting voor wanneer je als afnemer meent dat de leverancier ernstig in zijn zorgplicht is tekortgeschoten.

De juridische 'default' aanpak is dat, als partijen niet zelf in staat zijn hun geschil op te lossen, een hunner de kwestie aan de overheidsrechter kunnen voorleggen. Dan stap je veelal naar de rechtbank en vraag je de overheidsrechter te oordelen. Maar aan die aanpak zitten bij security-geschillen haken en ogen. Zo is het ten eerste de vraag of de rechters zelf wel capabel zijn alle technische 'ins & outs' van de security te doorgronden. Dat is vaak niet het geval. Rechters zijn specialisten in het recht en doorgaans niet of veel minder in informatietechnologie, laat staan in IT-security. Daar komt bij: als partij heb je geen enkele zeggenschap welke rechter van de rechtbank op de zaak wordt gezet.

Het is voor de gemiddelde overheidsrechter geen sinecure om zich te moeten buigen over zoiets als bijvoorbeeld de vraag of een webapplicatie in voldoende mate is ontwikkeld met de bedreigingen uit de OWASP Top 10 als uitgangspunt. En wat kan de rechter zeggen over 'de stand van de techniek' op het gebied van IT-security? Of welke mate van schuld heeft een gebruikersorganisatie die geraakt is door een ernstig ransomware-aanval terwijl zij geen adequaat CMDB (Configuration Management Database) in huis heeft – iets wat de response van zelfs een zeer gespecialiseerde dienstverlener ernstig kan frustreren? Hoever gaat in dat laatste geval de zorgplicht van een forensisch bureau dat in huis wordt gehaald om de puinhopen van de aanval op te lossen? En

Rechtspraak bij de overheidsrechter en IT-security zijn dus als water en vuur.

wat weet de rechter nou eigenlijk over nut en noodzaak van meerfactorauthenticatie als beveiligingsmiddel?
De overheidsrechter moet zich in een procedure door doorgaans dure externe deskundigen laten voorlichten. De rechter vaart veelal blind op de bevindingen van die deskundigen. Deze onzekerheden maken security-geschillen bij de overheidsrechter al snel tot een kansspel, met het risico van 'nieten'.

Vuile was

Een veel groter bezwaar van de stap naar de rechtbank is dat overheidsrechtspraak openbaar is. Dat staat nu eenmaal zo in onze grondwet. De zogeheten externe openbaarheid van rechtspraak is belangrijk omdat de samenleving de rechtsgang moet kunnen controleren. Consequentie: een netelig security-geschil ligt daarmee al snel op straat of komt wellicht in de publieke media terecht. Dikwijls zit de leverancier van een benedenmaats security-product daar niet op te wachten en ook de gebruiker ervan hangt niet graag de vuile was buiten. Dat past nou eenmaal niet bij security. Zo wens je als IT-dienstverlener de security-architectuur die je in huis hebt niet aan het publiek bekend te maken. Zelfs niet aan jouw wederpartij. Wordt een geschil aan de overheidsrechter voorgelegd, dan loop je het risico dat dat echter wel gaat gebeuren.
Rechtspraak bij de overheidsrechter en IT-security zijn dus als water en vuur. Illustratief is dat er momenteel een zaak rondom een fors datalek van de Bulgaarse belastingdienst bij het Europese Hof van Justitie loopt. Dat lek was een gevolg van, naar een Bulgaarse burger stelde, een benedenmaatse IT-security aan de zijde van de belastingdienst, wat in de ogen van die burger een schending van de AVG inhield. De Europese rechter in Luxemburg is onder meer gevraagd een uitspraak te doen over de wijze waarop de belastingdienst in de procedure aan de burger en de rechter inzicht moet geven in de details van haar IT-security. Kernvraag is daarbij: moet je als belastingdienst het achterste van je tong laten zien over de inrichting van de security? Het is afwachten welk ei de Europese rechter gaat leggen.

Arbitrage als alternatief?

Vanwege al deze bezwaren wordt er in security-contracten meer dan eens voor gekozen om de overheidsrechter op voorhand buiten spel te zetten door in de geschillenclausule van het contract te kiezen voor arbitrage bij een onafhankelijk en onpartijdig arbitrage-instituut. Arbitrage is een in de wet gewaarborgde vorm van rechtspraak waarbij particuliere scheidslieden tot een vonnis komen volgens een formele rechtsgang. Gespecialiseerde arbiters zijn, veel meer dan rechters, zelf deskundig en hebben vaak jarenlange ervaring op het genoemde probleemgebied. Zo ook op het gebied van IT-security.
In Nederland wordt met name de onafhankelijke en onpartijdige Stichting Geschillenoplossing Automatisering (SGOA) al ruim dertig jaar ingeschakeld bij IT-kwesties, waaronder ook geschillen op het gebied van IT-security. Wil je als partijen kiezen voor arbitrage, dan doe je er verstandig aan dit al direct in het contract te regelen, door middel van een zogeheten arbitraal beding. Een voorbeeld van zo'n beding is hier apart opgenomen.

Als gekozen is voor arbitrage bij de SGOA is het eindproduct van het proces een 'arbitraal vonnis' met in beginsel dezelfde rechtskracht als een 'gewoon' vonnis van de overheidsrechter. Arbitrage levert dus geen vrijblijvend eindoordeel op. Het arbitragereglement van de SGOA, dat onlangs nog in 2021 stevig is herzien, waarborgt niet alleen een eerlijke procedure voor alle partijen, maar ook de vertrouwelijkheid. Het nieuwe reglement voorziet binnen de SGOA in een aparte Privacy- en Securitykamer. De behandeling van de zaak geschiedt achter gesloten deuren en partijen en arbiters zijn gebonden aan eisen van vertrouwelijkheid. En dat is in menige security-kwestie geen overbodige luxe. Arbitrage… de moeite om nog voordat je een handtekening onder een security-contract zet stevig te overwegen.
Voor meer informatie over de SGOA zie: ww.sgoa.eu.

Voorbeeld arbitraal beding

'Alle geschillen welke tussen leverancier en cliënt ontstaan verband houdende met deze overeenkomst dan wel naar aanleiding van nadere overeenkomsten die van deze overeenkomst het gevolg zijn, worden beslecht door middel van arbitrage overeenkomstig het Arbitragereglement van de Stichting Geschillenoplossing Automatisering, statutair gevestigd te Den Haag. Deze bepaling doet niets af aan het recht van elk der partijen een voorziening in arbitraal kort geding te vragen, onverminderd het recht van elk der partijen tot het treffen van conservatoire rechtsmaatregelen.'

Even voorstellen

Ik ben Siep van Sommeren (30 jaar), de nieuwe voorzitter van Jong PvIB en daardoor ook betrokken bij het bestuur van het PvIB. Tijdens de Algemene Ledenvergadering van afgelopen najaar heb ik deze rol formeel overgenomen van Lodewiek Jansen. Op dit moment ben ik werkzaam als Information Security Officer bij de Rabobank. Daar ben ik verantwoordelijk om gevraagd en ongevraagd te adviseren over cybersecurity-gerelateerde vraagstukken binnen een aantal organisatieonderdelen.

In 2013 ben ik aan het begin van mijn opleiding Information Security Management aan de Haagse Hogeschool in contact gekomen met het platform. Via de bijeenkomsten heb ik een mooi netwerk op kunnen bouwen waaruit ik toen de nodige (stage)opdrachten heb kunnen regelen voor mijn opleiding. Al snel ben ik toegetreden tot de commissie waar ik nu voorzitter van ben geworden. Mijn doel is om jongeren dezelfde kans te bieden om het juiste netwerk op te bouwen.

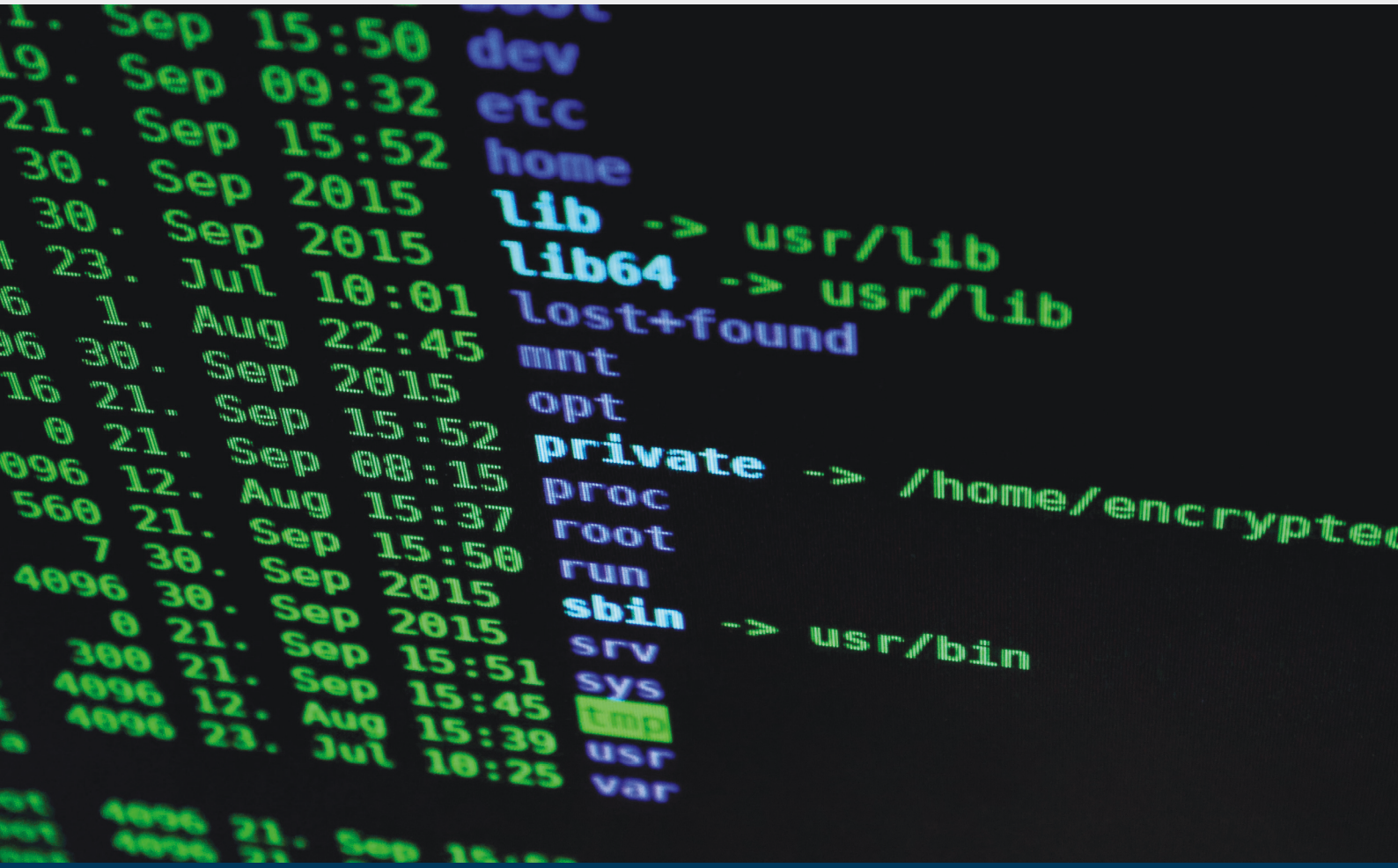
De oplettende lezer is het wellicht al opgevallen: Jong PvIB. Het is de nieuwe naam van de commissie die voorheen de Young Professionals commissie heette. De reden is dat we ervoor gezorgd hebben dat er een aantal versimpelingen zijn of worden doorgevoerd. Zo is Jong PvIB tegenwoordig voor leden tot 36 jaar en dus niet meer voor leden die minder dan vijf jaar in het vakgebied zitten zoals voorheen het geval was. Hierdoor verwachten wij onze activiteiten beter aan te laten sluiten op de behoefte van onze leden. Ook werken we binnen het bestuur aan de vereenvoudiging van de contributiestructuur wat ook effect zal hebben op onze leden. Om deze wijzigingen kracht bij te zetten hebben we besloten de naam te veranderen.

Een ander belangrijk doel is dat we meer in verbinding willen staan met onze leden. Om die reden willen we netwerkborrels organiseren om op een laagdrempelige manier met elkaar in contact te komen en elkaar te leren kennen. Ook is het streven om in 2022 onder andere twee bedrijfsbezoeken te organiseren. Verder is het onze intentie om zoveel mogelijk krachten te bundelen met zowel de andere commissies binnen het PvIB alsook met huidige en nieuwe partners. Een mooi voorbeeld hiervan is CyberSQUAD. Dit evenement organiseert Jong PvIB samen met Connect2Trust en DIVD. Dit betreft een exclusief invite only evenement dat speciaal gericht is op jongeren die actief zijn in de cybersecurity in Nederland.

Ik hoop jullie snel tegen te komen op een van de PvIB-bijeenkomsten!

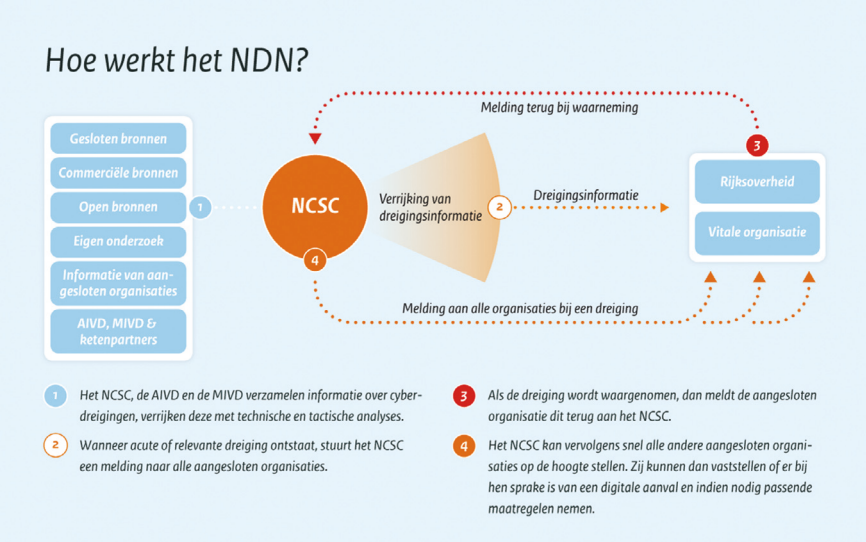
Siep van Sommeren

Auteur: Noortje Henrichs is Team manager Cyber Threat Intelligence (CTI) & Threat Analysis. Dit artikel verscheen eerder als blog op NCSC.nl. De auteur is bereikbaar via info@ncsc.nl.



Trots op 10 jaar Nationaal Detectie Netwerk

Cybersecurity is een woord dat je nog niet vaak in geschiedenisboeken terugvindt. Daarentegen is het mijn bescheiden mening dat het Nationaal Detectie Netwerk (NDN) een plekje in de Nederlandse geschiedenis verdient. Vanaf het eerste ruwe concept in 2011 is het inmiddels uitgegroeid tot een uniek en effectief digitaal verdedigingsmechanisme van nationaal belang.



Figuur 1 - ©NCSC Hoe werkt het NDN?

Voor lezers die niet bekend zijn met het begrip Nationaal Detectie Netwerk: het NDN is een detectienetwerk waar de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en het Nationaal Cyber Security Centrum (NCSC) samenwerken om kwaadaardig internetverkeer naar overheidsorganisaties en organisaties in vitale sectoren tijdig te herkennen. Bij overheidsorganisaties gebeurt dit door middel van netwerksensoren die speuren naar technische kenmerken van kwaadaardig verkeer. Ook richt het NDN zich op het onderling delen van dreigingsinformatie om cybersecurityrisico's en -gevaren sneller op te kunnen sporen. De technische kenmerken (Indicators of Compromise) en andere dreigingsinformatie worden bijvoorbeeld met vitale organisaties gedeeld, zodat organisaties vervolgens veiligheidsmaatregelen kunnen treffen om schade te voorkomen of te beperken.

2011-2013: het concept

In 2011 werd op een whiteboard ergens in Den Haag het eerste plan uitgetekend tot wat zich nu heeft ontwikkeld tot het NDN. Het was oorspronkelijk een heel beperkt concept dat GOVCERT (de voorloper van het NCSC) opperde om inzicht te krijgen in overheidsnetwerken, met als doel de weerbaarheid van deze netwerken te verhogen. Omdat GOVCERT zich primair richtte op overheidsorganisaties, werden de vitale sectoren in de initiële plannen nog buiten beschouwing gelaten.

Onder het motto 'Om meer te zien, moet je beter kijken', werden er de jaren daarna verkenningen uitgevoerd door onder andere TNO, Fox-IT en de TU Delft. De AIVD, MIVD en het (inmiddels kersverse) NCSC vormden samen een werkgroep om deze netwerkmonitoring op nationale schaal vorm te geven. Dit vereiste niet alleen een heel politiek en juridisch traject, maar ook een technisch ontwerp van de eerste netwerksensoren en het informeren van talloze belanghebbenden. Het is daarom niet zo vreemd dat het enkele jaren gekost heeft, voordat in 2013 de eerste pilot binnen het NCSC van start ging. Deelname aan het NDN was, en gebeurt nog steeds, geheel op vrijwillige basis.

Niet lang daarna gebeurde er iets dat niemand had kunnen voorspellen, maar wat het piepjonge NDN ineens onder een vergrootglas plaatste: de publicaties van Edward Snowden vestigden niet alleen de aandacht op surveillance van buitenlandse mogendheden, maar benadrukten ook het belang van privacy voor personen en berichtenverkeer. Daardoor werden ontwikkelingen rondom het NDN door organisaties soms met argusogen bekeken. Immers, in hoeverre tastte deze manier van overheidsmonitoring de privacy van werknemers aan? Menig ondernemingsraad stelde zich terughoudend op tegen de mate van netwerkinzicht die via het NDN verkregen zou kunnen worden.

Het NDN zal hierin de komende jaren steeds naar een balans moeten zoeken: aan de ene kant zagen de AIVD, MIVD en het NCSC een razendsnelle toenemende digitale dreiging en daarmee een grotere noodzaak voor netwerkdetectie binnen overheids- en vitale organisaties. Aan de andere kant zou de techniek zodanig moeten functioneren dat privacybelangen

Het NDN heeft zich in meerdere opzichten bewezen.

gewaarborgd werden. Alleen op die manier zouden meer organisaties bereid zijn om zich aan te sluiten bij het NDN waardoor de landelijke dekking – en daarmee de effectiviteit – van het detectienetwerk zou toenemen. Met de enorme inzet van veel medewerkers, partijen en deelnemers is het NDN op deze manier geleidelijk gegroeid.

2014-2018: de contouren

In 2014 werden de eerste werkafspraken gemaakt met organisaties in de vitale sectoren. Door de Wet Markt en Overheid is het niet mogelijk om sensoren te plaatsen bij dit soort organisaties, omdat de overheid dan zou concurreren met commerciële partijen die ook netwerksensoren leveren. Daarom is toen besloten dat het NCSC technische kenmerken van kwaadaardig verkeer (IoC's) direct zou delen met de aangesloten vitale organisaties. Voor dit doel werd, en wordt nog steeds, het platform MISP gebruikt. MISP (het Malware Information and Sharing Platform) is een open source oplossing om snel technische dreigingsinformatie met meerdere partijen te delen. Partijen kunnen hun eigen waarnemingen ook in het platform delen, zodat zichtbaar wordt welk soort digitale aanvallen er op Nederlandse organisaties plaatsvinden. 'Wat een incident is bij de een, is een goede waarschuwing voor de ander' werd vanaf nu het motto.

2019-2021: het fundament

Op technisch vlak werkten de NDN-partijen hard aan een sensor die in staat was om internetverkeer in grote hoeveelheden te scannen op kwaadaardige kenmerken. Het NCSC gebruikte in 2016 de NDS (Nationaal Detectie Sensor) die kon scannen op HTTP-, DNS- en SMTP-verkeer. Door de razendsnelle digitale ontwikkelingen werd deze sensor al snel achterhaald en vanaf 2019 vervangen door het huidige NSP. Deze sensor heeft de mogelijkheid om in plaats van naar drie, naar wel 157 protocollen te kijken. Daarbij slaat de nieuwe sensor (afhankelijk van hoe je hem instelt) gemiddeld 50 terabyte aan metadata per dag op. Dat zijn zo'n 800 iPhones van 64 gigabyte vol. Een stuk scherper zicht en een ijzeren geheugen dus! Maar met dit soort ontwikkelingen nam ook het belang toe om NDN-deelnemers in staat te stellen om dit goed te gebruiken. Het NCSC legt zich sindsdien daarom ook toe op het trainen van medewerkers van deelnemende organisaties.

Op organisatorisch vlak daalde sinds 2018 het besef in dat technische gegevens pas echt waardevol werden als je ze ook kon voorzien van de bijbehorende context. Want waarom zou je detecteren op een set technische gegevens als de dreigingen niet gericht zijn tegen jouw organisatie? En wat heb je aan data als je niet weet waar het voor staat en wat het mogelijk doet? Binnen het NCSC begonnen de technisch specialisten onder de paraplu van het NDN daarom steeds nauwer samen te werken met de meer tactisch georiënteerde dreigingsanalisten die zich specialiseren in typen aanvallers, hun werkwijzen en doelwitten. Op die manier konden trendverschuivingen en ontwikkelingen in digitale aanvallen beter herkend worden en ontstond er een completer beeld van de digitale dreigingen waar Nederland mee te maken krijgt.

2021 en verder: doorontwikkeling?

Inmiddels zijn we tien jaar verder. Het NDN heeft zich intussen in meerdere opzichten bewezen: aanvallen werden gedetecteerd, relevante informatie is gedeeld en het vermogen van deelnemers om netwerkverkeer te monitoren is gegroeid.

We moeten niet alleen stilstaan bij het succes van tien jaar Nationaal Detectie Netwerk, maar ook nadenken over de toekomst. De digitale ontwikkelingen gaan immers vliegensvlug en staan nooit stil. Met zekerheid kun je zeggen dat stilstand ook achteruitgang betekent. Als we geen tijd, geld en inzet steken in nieuwe detectietechnieken, zal het NDN minder scherp gaan zien en dus aan effectiviteit verliezen. Dat is de reden dat de AIVD, MIVD en het NCSC blijven investeren in hetgeen waaraan Europarlementariër Bart Groothuis ooit refereerde als 'de verborgen cybersecurityparel'. Eenvoudig, effectief en preventief: het Nationaal Detectie Netwerk is essentieel voor de digitale veiligheid van Nederland. Daar ben ik trots op en dat vier ik graag.

Meer over hoe het NDN werkt en de samenwerking binnen dit netwerk hoor je in aflevering zes van de podcast Let's talk about hacks.https://open.spotify.com/episode/16TlcUFBeEPTqLqgQbenwx?si=Vl2UNBF8QSOPxz7FPQl9fg

COLUMN LEX

Het derde lustrum in een bewogen vakgebied

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

In 2007 ontstond het PvIB. Niet uit het niets, maar uit bestaande professionele organisaties Genootschap van Informatiebeveiliging (GvIB) en Platform Informatiebeveiliging (PI) die de krachten gingen bundelen. Als ik nu terugkijk op de veranderingen in het vakgebied die de afgelopen vijftien jaar op ons afgekomen zijn, zie je dat er in die periode veel veranderd is. Eerder waren we gericht op het definiëren van standaarden voor het vakgebied zelf en het bijhouden van de ontwikkelingen in de cryptografie, nu zijn we veel meer bezig met de ontwikkelingen in het veld. Nieuwe actoren en aanvalsmethoden en bakken met kwetsbaarheden die door hen gebruikt worden.

De oprichting van het PvIB viel bijna samen met de introductie van de iPhone en de eerste Android smartphones. Dit was een cruciaal moment voor software-architectuur: naast de thin client en de fat client hadden we ineens de client app op een smartphone. Drie jaar later volgde de iPad, de tablet-versie van het slimme apparaat. 'Building security in' kreeg nieuwe mogelijkheden. Het smartphoneplatform werd in rap tempo veiliger. De platforms kregen een secure element en biometrische authenticatie - Touch ID in 2012 en Face ID in 2017, mooi uitgelijnd met de lustrumovergangen... Bankierenapps konden veiliger gemaakt worden dan internetbankieren in een browser. En dit was ook hard nodig, gezien andere ontwikkelingen. Complexe cyberaanvallen in opdracht van overheden waren in opkomst. In 2006 werd de term 'Advanced Persistent Threat' voor het eerst gehanteerd. Inmiddels zijn er zo'n veertig APT-groepen geïdentificeerd. Ze werden ook bekend onder koosnamen zoals Fancy Bear en Cozy Bear. Stuxnet werd in 2010 ontdekt, maar was waarschijnlijk al veel langer operatief. En we hadden de grote klokkenluiders: Chelsea Manning in 2010, Edward Snowden in 2013, Reality Winner in 2017. In 2008 werd Wikileaks opgezet, tussen 2012 en 2019 verbleef oprichter Julian Assange in de ambassade van Equador in London, waar hij asiel kreeg. Malware maakte de overstap van kwajongensstreken naar georganiseerde criminaliteit. Conficker en Bredolab (2009) waren botnets die door georganiseerde bendes opgezet, beheerd en verkocht werden. Verdere ontwikkelingen introduceerden het concept ransomware: Cryptolocker-GameOver, Petya, Wannacry, NotPetya. Grote kwetsbaarheden werden gevonden: Heartbleed, Rowhammer, Eternal Blue. Meltdown en Spectre leken ook heel serieuze bedreigingen te zijn, maar tot nu toe bleven die gelukkig beperkt. Veel wachtwoorden en andere vertrouwelijke informatie werd gelekt, onder andere van TJ Maxx, SONY, LinkedIn, Target, Equifax en Yahoo! zelfs meerdere malen. Diginotar werd in 2011 misbruikt om malafide certificaten aan te maken en viel om. In 2015 werd de Oekraïense elektriciteitsvoorziening verstoord, in 2021 kwam de Colonial Pipeline hack groot in het wereldnieuws.

Met deze gigantische lekken van collecties wachtwoorden werd duidelijk dat wachtwoorden complexer moeten zijn en niet hergebruikt mogen worden. De wachtwoordmanager kwam op, ingebakken in browsers en als aparte applicatie. Deze laatsten schoten als paddenstoelen uit de grond: in 2003 KeePass, in 2006 1Password, in 2008 LastPass en in 2016 BitWarden. Ook probeerden we het wachtwoord te elimineren, maar dat is nog niet gelukt, al zijn er ook daar goede stappen gemaakt met authenticator apps.

Dit landschap van kwetsbaarheden, aanvallers en malware bleef niet onbeantwoord. De professionele securitygemeenschap kwam met antwoorden op dit cybergeweld, ondanks het feit dat de wereld ondergedompeld werd in een financiële crisis van 2008 tot ongeveer 2012.

Het vertrouwen in stemcomputers nam af. Sinds 2009 stemmen we weer met het rode potlood. In 2012 werd het NCSC opgericht, waar het tien jaar oude www.GovCERT.nl in opging. In 2016 kregen we de GDPR (AVG) en sinds 2017 kunnen we ons sterk authentiseren aan de overheid met de DigiD-app.

De CISO werd gemeengoed. In 1995 trad de eerste CISO aan (Steve Katz), maar het zou lang duren voordat het hebben van een CISO en een security-organisatie een vanzelfsprekendheid werd. In 2009 is dit anders, nu heeft 85% van de grote bedrijven een CISO.

De focus van maatregelen werd verlegd naar detectie en respons. In 2006 werd het eerste SIEM (security information and event management) product geïntroduceerd, nog vrij beperkt in functionaliteit. In 2015 werden analysefuncties toegevoegd, zoals UEBA (user and entity behavior analytics). Antimalware groeide door naar EDR (endpoint detection and response). Kortom, het securityvakgebied is beweeglijker dan ooit. Ik ben benieuwd wat het volgende lustrum hieraan zal toevoegen.

Auteurs: Nicole van Deursen is hoofdredacteur van informatiebeveiliging magazine en bereikbaar via ibmagazine@pvib.nl

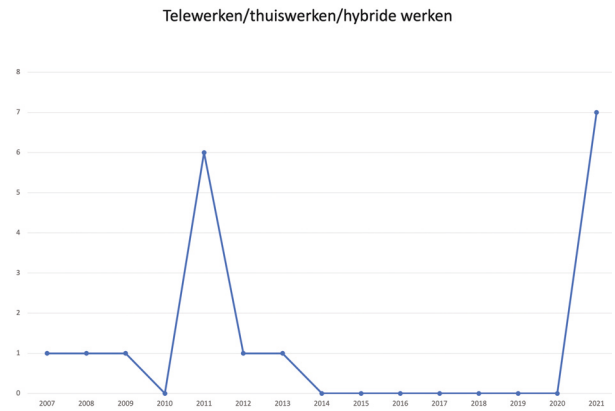
Terugblik op 15 jaar iB-Magazine

Waar komen we vandaan en waar gaan we heen? Voor de gelegenheid van het PvIB-lustrum ben ik in de jaargangen van het informatiebeveiliging magazine (iB-Magazine) gedoken op zoek naar trends van toen en nu.

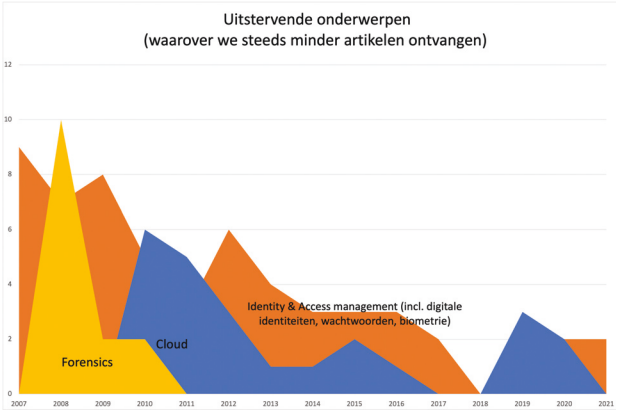
Het is altijd de bedoeling geweest dat iB-Magazine een blad is voor en door leden van het PvIB om kennis en ervaringen te delen. Iedereen mag een artikel schrijven en de redactie is er om de auteurs daarbij te helpen. Tijdens het vorige lustrum is daarom een workshop gegeven voor leden die wel willen schrijven maar niet goed weten hoe te beginnen. Meer informatie over de workshop van toen vind je terug in het blog (1). We hopen op het aankomende lustrum-congres een soortgelijke workshop te kunnen aanbieden.

De eerste uitgave van iB-Magazine verscheen in september 2007 na de fusie tussen de twee verenigingen GvIB en PI. Enkele van de artikelen zouden zo maar in 2022 geschreven kunnen zijn. Maar liefst acht pagina's gaan over telewerken. Na een aantal artikelen in 2011 bleef het stil rond dit onderwerp. Tegenwoordig gebruiken we het woord telewerken niet meer, maar het thema is de laatste twee jaar weer heel actueel geworden. Maar zelfs in 2007 was het geen nieuw thema: het artikel wijst ons op de oliecrisis van de jaren 70 van de vorige eeuw, toen we ons energieverbruik drastisch moesten reduceren. Ook dat klinkt bekend in de oren.

Wat opvallend anders was in 2007 is te zien op een foto van deelnemers van de BlackHat conferentie in 2007. Ik heb goed gekeken met een vergrootglas, en ik denk dat ik misschien één vrouw zag. Gelukkig is het publiek op conferenties tegenwoordig een stuk diverser. Bijna nostalgisch is het onderschrift bij een foto waarop deelnemers aan een ander congres te zien zijn: 'Ieder had zijn laptop bij zich'. De auteur schrijft enthousiast: 'Elke zaal was voorzien van een compleet LAN' en 'elke laptop stond open en aan'. Vandaag de dag valt het juist op als mensen niet met een device bezig zijn en oogcontact maken met andere mensen op een congres.



Figuur 1 - Tijdlijn met aantal artikelen over telewerken/thuiswerken/hybride werken.



Figuur 2 - Drie onderwerpen die door de jaren heen steeds meer of minder in artikelen voorkwamen.

Terugkerende thema's

Door de jaren heen zie ik een constante stroom van ongeveer dertig thema's en onderwerpen die vanaf 2007 altijd blijven terugkomen. Ook onderwerpen die vandaag de dag soms nog als 'nieuw' worden bestempeld zoals gedrag en awareness of OT/IACS waren er in 2007 al bij. Alleen zien we na 2010 geen artikelen meer verschijnen over forensisch onderzoek of virtualisatie (beiden heel populair in 2008). Artikelen over cloudsecurity kwamen in iB-magazine met een knal in 2010 en de aandacht lijkt in de jaren erna wat weggezakt. Identity & access management is heel lang veelbeschreven geweest en tegenwoordig iets minder vaak in een artikel, maar zeker niet verdwenen van de radar van onze auteurs. Architectuur is door de jaren heen een groeiend thema. Omdat we nu de vaste columnist over architectuur missen, zien we het aantal artikelen daarover wel wat afnemen.

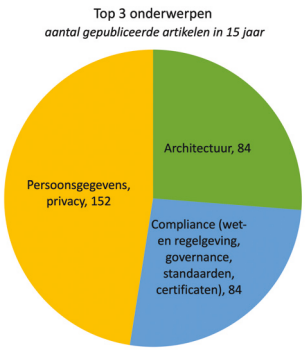
Privacy

De meeste artikelen in de afgelopen vijftien jaar gingen over privacy en persoonsgegevens. Wij publiceerden in totaal bijna twee keer zoveel artikelen over privacy dan over andere populaire onderwerpen als architectuur of compliance (inclusief wet- en regelgeving en governance). Dit zou zo maar te maken kunnen hebben de komst van Rachel in de redactie in 2010 die privacy op de kaart heeft gezet binnen de vereniging (en wellicht een klein beetje veroorzaakt door de AVG…).

De onderwerpen in de magazines van de beginjaren leken over het algemeen wel iets technischer van aard dan tegenwoordig. Er werd tot 2016 meer geschreven over OT en industriële systemen, softwareontwikkeling en pentesten dan de laatste jaren. Onderwerpen waarover we als redactie graag meer zouden willen publiceren. Hierbij dus nogmaals de oproep: wil je kennis delen met andere leden, neem dan contact op met de redactie.

Teruglezen

In het archief op de PvIB-website zijn de pdf's van alle magazines vanaf



Figuur 3 - Top 3 onderwerpen.

2008 terug te lezen. Dat is best wel leuk om te doen als je een keer wat tijd over hebt. Het is helaas niet makkelijk zoeken op specifieke onderwerpen, en achter de schermen werken we aan toekomstige verbeteringen. Recent zijn we begonnen met het los publiceren van alle artikelen op de website (2). De columns en blogs werden al langer zo gedeeld.

Ons redactielid Maarten is ook al vijftien jaar actief voor iB-magazine. Hij schreef een artikel in het septembernummer van 2007. Maarten was naar de BlackHat-conferentie geweest en de slotzin van het artikel luidt: `over een ding bestaat in elk geval geen twijfel: ons vakgebied blijft voorlopig nog interessant'. Anno 2022 kunnen we dat nog steeds beamen.

De dataset met alle thema's en de interactieve versies van de grafieken in dit artikel kun je hier bekijken: https://public.flourish.studio/visualisation/10027878/. In de filter kun je de thema's kiezen.

Referenties

(1) https://www.pvib.nl/actueel/blogs/workshop-artikel-schrijven

(2) https://www.pvib.nl/kenniscentrum/dossier/ib-magazine-artikelen

Auteurs: Peter van Schelven is jurist en arbiter bij BIJ PETER - Wet & Recht en bereikbaar via linkedin.com/in/petervanschelven. Bianca Brooijmans is FG bij Enovation Group en zelfstandige. Bianca is bereikbaar via linkedin.com/in/biancabrooijmans.

Dataprotectie of gedoe over de pecunia?

Sinds de introductie van de AVG is privacy in de volksmond een steeds vaker gebruikte term geworden. Grappig, want de AVG zelf - informeel ook wel aangeduid als de Europese privacywet - spreekt hier met geen woord over. De AVG gaat uit van het beschermen van onze persoonsgegevens en randvoorwaarden voor het überhaupt mogen gebruiken daarvan. Al decennia voor de komst van de AVG bestonden deze randvoorwaarden en de beschermingsplicht natuurlijk ook al. We spraken toen al van dataprotectie of informationele privacy. De term privacy gaat terug tot 1890.

Laten we de daadwerkelijke privacy professionals niet vergeten, want dat zijn de teams achter de knoppen.

Het is nu juist die beschermingsplicht die ons vak zo interessant en met name waardevol maakt. Uiteraard spelen wij – juristen, privacy professionals, FG's en security specialisten – een belangrijke rol bij de bewustwording, het gesprek en het maken van afspraken waar we ons aan moeten houden; het is immers een samenspel. Wat ons echter vooral opvalt is dat sinds de komst van de AVG er sprake is van buitenproportionele aandacht in allerhande privacydocumenten voor afspraken over aansprakelijkheid, financiële vrijwaring en andere manieren om de nadelige gevolgen van dataprotectie op anderen af te wentelen. Met dataprotectie in de strikte zin van het woord heeft dat eigenlijk weinig te maken. Het gaat dan vooral om het afwentelen van de financiële lasten en risico's op de wederpartij. Deze ontwikkeling, die in de praktijk van alledag een forse sta-in-de-weg is bij het soepel aangaan van verwerkerscontracten, lijkt het rechtstreekse gevolg van een naïeve aanname van de AVG-wetgever. De makers van de AVG lijken eraan voorbij te zijn gegaan dat contracten sinds jaar en dag in het westerse economische verkeer niet alleen gebruikt worden om rechten en verplichtingen netjes te regelen zoals de AVG-wetgever kennelijk heeft vermoed toen zij een verplichtende regeling over het verwerkerscontract daarin opnam. Contracten in het algemeen, verwerkerscontracten incluis, zijn mede – en soms zelfs vooral – instrumenten om pecuniaire risico's op andermans bordje te leggen. En die gedachte beheerst niet zelden ook de privacy- en securitypraktijk. Voor wie, zoals wij, de bescherming van mensen én hun gegevens centraal willen stellen is dat een zorgelijke ontwikkeling in de wereld van privacy en security.

Begrijp ons niet verkeerd, het moet uiteraard geregeld worden en goed ook, want in deze tijd is het waarschijnlijk niet de vraag óf er als gevolg van inadequate informatiebeveiliging een datalek voorkomt in je organisatie, maar wanneer. En als het dan gebeurt, dan kun je je zaken maar beter goed geregeld hebben, zeker als de oorzaak van het ontstaan dan buiten de eigen organisatie ligt.

Maar… is het niet veel belangrijker om aan de voorkant de aandacht te leggen op het (zoveel als mogelijk) voorkomen van incidenten? En als het dan toch gebeurt, moeten we dan niet zo snel mogelijk het security-incident (gezamenlijk) mitigeren? Dus, laten we de daadwerkelijke privacy professionals niet vergeten, want dat zijn de teams achter de knoppen: de IT-architecten en systeemontwikkelaars. Zij zijn degenen die de gegevens écht kunnen beschermen.

Nog te weinig zien we in ons eigen privacyspeelveld, echt serieuze aandacht voor de organisatorische en technische maatregelen die de AVG ons gebiedt te nemen. In een eerder artikel in iB-Magazine (1 2022), schreven we al over het belang van samenwerking en de adoptie van de gedachtegang dat privacy valt of staat met adequate informatiebeveiliging. Het gaat immers om 'gegevensbescherming' – die term komt wél voor in de AVG. Alleen zo help je de reputatie en veiligheid van je eigen organisatie te versterken en het vertrouwen bij mensen binnen en buiten je organisatie te vergroten. Een samenleving die afglijdt naar pecuniair gedoe in privacyland ondermijnt het grote belang en de betekenis van effectieve gegevensbescherming, en daar worden maar weinigen – behalve advocaten en ander juridisch volk – beter van. Wie keert het tij ten gunste van de professionals die daadwerkelijk bijdragen aan de bescherming van uw en onze gegevens?

Auteur: Dré Lameir is CISO en CTO bij Enovation Group en is bereikbaar via linkedin.com/in/lameir.

Allemaal goed spul

Stel: ik heb een moestuintje, ik verbouw wat sla en tomaten. Daar gooi ik thuis wat vinaigrette doorheen, misschien wat croutons, beetje avocado, hardgekookt eitje en uitgebakken spekjes. Nog wat toast en een Sauvignon Blanc. Genieten maar!

"Allemaal goed spul bij elkaar dus dat moet lekker zijn!", zou mijn moeder zeggen... allemaal goed spul...

Is dat wel zo? Die avocado, waar komt die nou vandaan? Zuid-Amerika? Is-ie duurzaam getransporteerd? Is de arbeid die ervoor nodig was eerlijk betaald of komt deze van zo'n avocadokartel met louche praktijken? Er staat wel een 'bewuste keuze'-stickertje op, dat wel. En dat eitje? Komt niet rechtstreeks van de boer. Ik heb het gewoon bij de supermarkt in mijn mandje gelegd, ik keek nog wel naar het 'vrije uitloop'-logo. Het zullen best blije, vrije kippen zijn. Wat hebben die dan weer gegeten? Biologisch verbouwd graan of afval uit een of ander schimmig industrieel proces? En hoe vrij is 'vrije uitloop'? Wie controleerde die leefruimte? Was dat echt wel buiten? Dan heb ik het nog niet eens over de spekjes. Kan dat nog wel... spekjes... vlees? Wat is daar de carbon footprint van? Welk dierenleed heeft mijn uitgebakken spek moeten doorstaan? Wat voor antibiotica is er in het varken gegaan? Is dat eigenlijk wel goed voor me? Wat doet dat in combinatie met de kwaaltjes waarmee ik rondloop? En kan ik die Sauvignon Blanc wel mixen met mijn medicijnen? Wat stond er nu in die kleine lettertjes van de bijsluiter? En mijn eigen sla en tomaten?

Wat was er eigenlijk vóór mijn moestuin op deze grond? Is er in 1700 een pottenbakkerij geweest en ben ik eeuwenoud gif aan het eten? Of is er recent een xtc-afval dump geweest in de buurt en is het grondwater vervuild? Oooh, die slazaadjes van de Boerenbond? Zijn die genetisch gemodificeerd of niet? En als ze het niet zijn... stonden ze dan niet in het buurveld van experimentele sla die wel genetisch gemodificeerd was en is mijn biologisch getuinierde sla dat dus nu stiekem ook?

Wikipedia
De uitdrukking: staan op de schouders van reuzen is een metafoor voor 'gebruikmaken van het inzicht dat is verworven door grote denkers die zijn voorgegaan om intellectuele vooruitgang te boeken'.

...allemaal goed spul...

In die salade gaat allemaal goed spul, allemaal perfecte ingrediënten die samen een ultieme maaltijd vormen zonder gevaar voor de volksgezondheid. Toch? Maar eigenlijk kan ik daar, met goed fatsoen, mijn hand niet voor in het vuur steken. Ik kan niet zeker weten dat het goed zit. Voor eigen gebruik kan ik daar nog wel een risicoafweging voor maken. Maar durf ik mijn zieke, zwakke buurvrouw van een maaltje te voorzien? Wat als ze straks omvalt door mijn sla? Is die leuke dochter van haar nou advocaat? Hmmm, dan maar geen goede buur.

"Ja, als je zo gaat redeneren kan je niks meer eten jongen...!" Ook iets wat mijn moeder zou zeggen.

Code copy-pasten

En in software? Ook daar gooien we ingrediënten bij elkaar. Bouwen met blokken is vandaag de dag gemeengoed. Dan heb ik het niet eens over lowcodeplatformen als Mendix of Outsystems. Álle software hangt van honderden complexe libraries en componenten aan elkaar. Open source, closed source, blokken gebouwd door oud-collega's, gekopieerde routines van andere projecten, slimmigheidjes gecopy-pastet van StackOverflow, ga zo maar door. Krapte op de arbeidsmarkt, druk op prijzen en de stijgende vraag naar nieuwe features vragen nu eenmaal om meer snelheid en slimheid bij het bouwen. Het is noodzaak om bestaande ingrediënten of componenten te gebruiken. Een software-architect of -engineer leeft simpelweg te kort om al die kennis op te doen, om al die blokken zelf te ontwikkelen of ze te testen. We realiseren die nieuwe features omdat we voortbouwen op de collectieve vooruitgang. We are standing on the shoulders of giants!

En eerlijk, die componenten zijn dus gebouwd door andere giants, met andere compilers op andere systemen. Die hebben misschien minder getest, mogelijk zijn ze gezwijnd tijdens de audit. Of ze worden onderhouden door een hele leuke groep vrijwilligers die samen een klein Log4J-achtig codebibliotheekje onderhouden in hun vrije tijd. Twee keer per jaar hebben ze een meet-up, met bier en een BBQ, waar steeds minder mensen komen. Wel leuk dat de hele wereld ergens nog wel hun componentje gebruikt. En al die software draait in de cloud! Op de computer van een ander. In virtualisatiesoftware en containertechnologie die we niet kennen. Waarvan het intellectueel eigendom in handen is van grote ongrijpbare wereldwijd opererende concerns. En die draaien weer op hardware die ze niet zelf hebben gebouwd die afhankelijk is van stroom en internetverbindingen waarop niemand, aan onze kant van de keten, invloed heeft.

Softwareveiligheid

Een salade en de ingrediënten kun je controleren door de hele keten in beeld te hebben en de voedselveiligheid te garanderen. Dat vereist traceerbaarheid, transparantie, afspraken, certificeringen, keuringen, meldpunten en handhaving.

Ook in de software-industrie zijn er marktstandaarden met heel veel certificeringen en allerlei waarborgen in landen die we vertrouwen. Audits op CMMI, SOC2, ISAE3402, ISO 27001, Medical Device Regulation (MDR) en ga zo maar door. En gelukkig wordt er heel veel getest op alle niveaus. Daardoor is het maken van software wel een dure hobby geworden. Als je niet meer alles zelf kunt bouwen dan zul je onderdelen moeten inkopen. Maar dat drijft de prijs op, de keten wordt langer en het aantonen van aansprakelijkheid bij het falen van de software wordt steeds ingewikkelder. Allerlei servicelevel agreements, (open source) licentievormen en contractvoorwaarden maken het heel moeilijk om de kwaliteit en werking in de keten te garanderen. In aanbestedingen en tijdens onderhandelingen worden steeds grotere waarborgen gevraagd en verzekeren is al helemaal lastig.

Welke SaaS-leverancier durft er echt zijn handen nog voor in het vuur te steken?

...allemaal goed spul...

Referenties

(1) https://en.wikipedia.org/wiki/Standing_on_the_shoulders_of_giants

(2) https://www.rijksoverheid.nl/onderwerpen/voeding/voedselveiligheid-in-nederland

Auteur: mr. A.IJ. (Ard) Ruiter werkt als privacy- en beveiligingsfunctionaris/senior inspecteur bij de ILT Inlichtingen- en Opsporingsdienst (ILT-IOD). Hij schreef dit artikel op persoonlijke titel en is bereikbaar via LinkedIn.

Cyberrisicomanagement bij consumentisering en democratisering van IT

De doorlopende, digitale transformatie en het toegenomen thuis- of hybride werken leidt tot een vervaging tussen werk- en privémiddelen. Voorheen had de IT-afdeling de zeggenschap over de hard- en software om de bedrijfsveiligheid te garanderen. Nu worden privémiddelen ingezet voor bedrijfsdoelstellingen en worden USB-sticks van het bedrijf soms ook privé gebruikt. Welke middelen zijn er om dit toch cyber- en information secure in te zetten? Risicobewust management en inhoudelijke gesprekken met medewerkers kunnen goed inzicht geven in de risico's en de awareness verder vergroten.

De aanschaf van devices, de verwerking van informatie, het onderhoud en het goed beveiligen van informatie was ooit een exclusieve taak van de ICT-afdelingen van de onderneming. De deskundigen op die afdelingen bepaalden voor de organisatie met welke pc's en applicaties gewerkt kon worden. Nu lijkt het soms bijna omgekeerd: het personeel schaft als privépersoon IT-middelen aan en bepaalt zelf hoe ze bedrijfsinformatie inzien. Dit vereist een andere aandacht bij het managen van risico's en een Work From Anywhere (WFA)-strategie.

Trends bij digitaal gerelateerde veranderingen

Dat digitalisering meer is dan techniek, is wel bekend. Ook dat het niet meer iets is dat alleen de aandacht heeft van organisaties. Een decennium geleden bepaalde de organisatie welke middelen werden aangeschaft en hoe die worden gebruikt. Dat ligt al ver achter ons. De ongoing/doorlopende digitale transformatie (ODT/DDT) – de verdergaande intense verwevenheid en verknoping van informatietechnologieën (IT) in het dagelijks leven – heeft ook invloed op het gedrag. Het onderscheid tussen burger, werknemer en consument wordt steeds hypothetischer. In deze DDT vallen twee centrale trends waar te nemen: ten eerste het razendsnelle, revolutionaire tempo waarin nieuwe digitale technologieën worden geïnnoveerd en ook de toepasbaarheid én gebruiksvriendelijkheid waarmee ze op de markt worden gezet. Aan de andere kant nemen digitaal gerelateerde veranderingen op een groot aantal levensgebieden toe, die ook nieuwe zwakke punten blootleggen. De effecten doen zich voor in ons (privé)leven en bij de door ons gebruikte producten die steeds dieper in ons leven alsook in onze (bedrijfs)omgeving geïntegreerd zijn; tegelijkertijd zijn ze wereldwijd met elkaar verbonden. Medewerkers zien op 'hun' consumentenmarkt interessante technologieën die ze eerst voor privédoeleinden gebruiken en privé testen en vervolgens nemen ze deze mee naar hun werkplek om die 'handige' middelen ook te gebruiken voor de bedrijfsdoelstellingen. Deze 'Consumerization of IT' (CoIT) is het verschijnsel waarbij nieuwe informatietechnologie eerst in de consumentenmarkt wordt geadopteerd en daarna naar de zakelijke wereld migreert.

Iedereen digitaal inclusief

Tegelijkertijd kan een toegenomen democratisering van technologie worden gezien: mensen hebben makkelijk(er) toegang tot technische of zakelijke kennis zonder uitgebreide – en dure – trainingen. Bovendien zijn er al vele Massive Open Online Courses (MOOC) en andere gratis e-learnings om je kennis en vaardigheden te optimaliseren. Het is al vele jaren aan de gang, maar kreeg een ongekende versnelling door de coronamaatregelen als gevolg van de door COVID-19 veroorzaakte pandemie. Zelfs nu Work From Home (WFH) normaal is, ontstaat er een nieuwe vorm van werken op afstand: werken vanaf elke locatie, Work From Anywhere (WFA). Werknemers kunnen in theorie wonen en werken waar ze willen, meestal binnen een specifiek land, maar in sommige gevallen overal ter wereld met een betrouwbare internetverbinding. Bij de aanvang van de coronamaatregelen hebben de organisaties met een robuuste infrastructuur voor informatietechnologie onbewust/onbedoeld gezorgd voor democratisering van technologie om hun operaties soepel te laten verlopen en het hoofd boven water te houden. Dit zowel binnen de keten als voor hun werknemers. De DDT leidt ook tot een investering in digitale inclusie, zodat iedereen gelijkwaardige kansen heeft en volwaardig kan deelnemen aan het maatschappelijk leven. Vele lokale initiatieven worden opgezet om 'digitale zelfredzaamheid' te ontwikkelen en mensen digitaalvaardig(er) te maken (1). Eind 2021 ontstond de eerste Cyberbank: een soort voedselbank voor laptops en digitale ondersteuning. Daarmee kunnen minima met een stadspas, tegen betaling van statiegeld van 20 euro aanspraak maken op een laptop (2). Met de bestrijding van digibetisme wordt iedereen digitaal inclusief.

Consumentisering van IT (CoIT)

De term consumentisering van IT (CoIT) (3) is zeker niet nieuw, maar staat inmiddels voor een steeds breder fenomeen. Tien jaar geleden publiceerde het EU-agentschap voor cyberbeveiliging ENISA al over de risico's en mogelijkheden bij dit fenomeen (4). Echter, CoIT verovert steeds meer terrein. CoIT omvat het gebruik van technologieën in een dagelijkse, op consumenten gerichte context; deze nieuwe informatietechnologie wordt eerst in de consumentenmarkt geadopteerd vervolgens na succesvol gebruik

en inzichten van consumenten c.q. werknemers naar de zakelijke wereld gemigreerd.

Het gaat om:

- Gebruik van persoonlijk geselecteerde en gekochte client devices zoals: notebooks, laptops, smartphones en tablet-pc's. Het gebruiksgemak, de toegevoegde waarde en de eenvoud in contentuitwisseling maakt dat deze technologie onmiskenbaar verbonden is met ons persoonlijk leven; thuis en op het werk.
- Gebruik van online services, zoals: online data- & cloudopslag, webbased e-maildiensten (webmail), sociale media/netwerken of vertaaldiensten.
- Toenemende IT-deskundigheid van medewerkers, de aansturing van ICT/netwerk-applicaties en Software as a Service (SaaS) geschiedt door meer IT-bekwamere en -deskundigere werknemers, die devices aanschaffen, de zelfgekozen applicaties installeren en vervolgens verbinding maken met het bedrijfsnetwerk, al dan niet met kennisgeving aan de eigen organisatie.
- Medewerkers als IT-ontdekkers, zij ontdekken – in navolging van de traditioneel gespecialiseerde IT-afdelingen – nu zelf 'handige' toolings en nemen die mee naar kantoor, zoals digitale vergadermiddelen en 'vergaderuiltjes'. Een vergaderuil is een alles-in-één-apparaat: een intelligente full HD-camera, speakers en microfoons met een bereik van 360 graden die verbonden kan worden met apps om te videobellen, te chatten en om presentaties te geven. Installatie op kantoor geschiedt door henzelf, zodat van daaruit contact kan worden gelegd met de thuiswerkende collega's en natuurlijk ook vanuit het eigen huis met de eigen middelen. De waarneming: privédevices zetten het bedrijfs-ICT opzij.
- Hybride middelengebruik, 'handige' middelen verstrekt door het bedrijf, worden thuis ingezet. Een voor de hand liggend voorbeeld: de telefoon van het werk inzetten voor privédoeleinden. Acceptatie van de toelaatbaarheid binnen redelijke kaders. De mooie vakantiefoto's gedeeld met de grootouders via de mobiele telefoon van het werk of met behulp van die ene USB-stick, die eigenlijk van het werk is.

Inmiddels hebben Tweede Kamerleden al het initiatief genomen voor een 'Wet werken waar je wilt'. Het doel van dit wetsvoorstel is om werknemers meer vrijheid te geven in de verdeling tussen werken op de werklocatie en thuiswerken, om zodoende het wettelijk kader mee te laten bewegen met de huidige tijd waarin flexibel werken is omarmd, aldus de initiatiefnemers (5).

Sociaal en sociaalpsychologisch vlak

Privé opgedane ervaringen met technologie, worden meegenomen naar het werk. Dat leidt ook tot veranderingen in het sociale en sociaalpsychologische terrein. 'In de hoofden' is er steeds meer een vervaging tussen privé en werk en daarmee ook tussen private en bedrijfseigendommen van IT-middelen. Als een entiteit die middelen overneemt kan dat enkel binnen de grenzen van het risicobewustzijn. Eigen persoonlijke devices inzetten voor bedrijfsactiviteiten gaat gepaard met nieuwe verantwoordelijkheden, waar sommige medewerkers niet op bedacht zijn of moeilijk mee om kunnen gaan. De werknemer is steeds flexibeler; overal kan gewerkt worden en ook in uren die afwijken van de traditionele 9-5 kantooruren. Iedereen is daarmee altijd connected met het bedrijf. Nadelig is dat er altijd contact kan worden gelegd tussen werkgever en werknemers alsook tussen werknemers onderling. De 'quality time' met familie en vrienden kan daaronder leiden. In België is inmiddels het recht op deconnectie ontstaan: het recht om buiten werktijd niet te reageren op e-mails, telefoontjes of berichtjes van je baas of klanten. Het deconnectierecht is bedoeld om burn-out en stress te voorkomen (6).

De markt levert veel gratis applicaties, die ook nog vaak gebruiksvriendelijker zijn dan de goed beveiligde middelen die het bedrijf leverde. 'Gratis bestaat niet', is een bekend adagium in de IT-securitybranche. Bij medewerkers kan de vraag rijzen 'waarom het bedrijf zo moeilijk doet', omdat het bedrijf minder gewillig is die devices over te nemen. Medewerkers doen privé-ervaringen op die kunnen bijdragen aan innovatieve ontwikkelingen binnen bedrijven. Door de toegenomen populariteit van technologie in het dagelijkse leven worden medewerkers steeds behendiger met software en hardware en diens toepassingen.

Consumentenmiddelen worden ingezet voor organisatiedoelen of overheidsinstanties, terwijl het maar de vraag is of deze organisatie/overheid een legitieme of wettelijke grondslag hebben om deze consumentenmiddelen in te zetten. Als privépersoon googelen is toegestaan, maar als diezelfde persoon als medewerker googelt is dat wellicht een inbreuk op iemands privacy (7).

Hoewel werknemers steeds comfortabeler zijn in het gebruik van technologie op het werk en minder training nodig hebben, zijn ze ook veeleisender. Medewerkers denken (on)gevraagd mee hoe bedrijfsmiddelen moeten worden ingezet. Als middelen niet voldoende productief zijn, kan het personeel de verleiding voelen om op zoek te gaan naar alternatieven buiten het zicht van de organisatie. Dit brengt natuurlijk grote beveiligings- en compliancerisico's met zich mee. Aan de andere kant kan ook worden waargenomen dat medewerkers steeds meer secure-aware worden. Ze vragen zich vaker zelf af of devices en applicaties wel goed zijn om in te zetten voor het bedrijf. Meer kennis van IT zorgt in veel gevallen ook voor soepelere en snellere adoptie van nieuwe software en

Afstandsbeheer van devices

Consumentisering van IT/Consumerization of IT (CoIT): verschijnsel waarbij nieuwe informatietechnologie eerst in de consumentenmarkt wordt geadopteerd en daarna naar de zakelijke wereld migreert. **Democratisering van IT:** mensen krijgen gemakkelijk toegang tot technische of zakelijke kennis door het gebruik van informatietechnologie zonder uitgebreide (en dure) trainingen. **Bring Your Own Device (BYOD):** gebruikers van een computernetwerk mogen hun eigen apparaten, zoals een privételefoon of laptop, gebruiken voor zakelijk gebruik. Vaak mag dit alleen onder bepaalde voorwaarden. **Choose Your Own Device (CYOD):** (vaak beperkte) selectie uit het totaal aantal beschikbare mobiele devices dat door de organisatie reeds is beoordeeld op veiligheid en risico'. De werknemers kiezen uit deze selectie welk device ze voor hun werk willen gebruiken. **Company Owned/Business Only (COBO):** een organisatie schaft de apparaten aan en blijft ook eigenaar van het apparaat; tevens zorgt de organisatie dat de apparaten secured zijn en mogelijk te allen tijde gecontroleerd kunnen worden door het bedrijf. Deze apparaten zijn uitsluitend zakelijk, waardoor werknemers geen toegang hebben tot apps voor entertainment of persoonlijk gebruik. **Company Owned/Personally Enabled (COPE):** impliceert een persoonlijk geactiveerd apparaatomgeving die eigendom is van het bedrijf. Medewerkers kunnen zelf een device kiezen dat aan hun eisen en voorkeuren voldoet. De organisatie vergoedt deze, maar stelt eisen aan de modellen en de technische prestaties, maar mag het privégebruik niet reguleren. **Endpoint protection platform (EPP):** een set softwaretools en technologieën die de beveiliging van endpoint apparaten mogelijk maakt. Het is een uniforme beveiligingsoplossing die antivirus, antispyware, inbraakdetectie en -preventie, een persoonlijke firewall en andere eindpuntbeschermingsoplossingen combineert. **Endpoint Detection and Response (EDR)/Endpoint Threat Detection and Response (ETDR):** geïntegreerde endpoint security-oplossing die real-time continue monitoring en verzameling van endpoint gegevens combineert met op regels gebaseerde geautomatiseerde respons- en analysemogelijkheden. **Endpoint threat detection and response (ETDR):** = EDR. **Enterprise Mobility Management (EMM), toestel + appbeheer:** een reeks beleidsregels en praktijken die door ondernemingen worden gebruikt om gevoelige bedrijfsgegevens te beveiligen op mobiele apparaten die eigendom zijn van het bedrijf en van werknemers. Dit gebeurt vanuit één centrale omgeving. Het is een uitgebreide, hardware onafhankelijke methode voor het op afstand beheren van apparaten, inclusief hun configuratie en de daarop gegenereerde bedrijfsinhoud, via MDM, MAM en EMM, is allesomvattend: het kan de toegang tot bedrijfsapps, interne websites en zelfs de bijbehorende gegevenssilo's beheren. Het gaat erom de toegang tot bedrijfs- en klantgegevens goed te regelen en ervoor te zorgen dat er beheersing (`control') is over waar data een gegevens naartoe gaan. **Managed BYOD (MBYOD):** BYOD waarbij de werkgever een selectie geeft van mogelijk aan te schaffen devices die de werkgever vervolgens vergoedt. **Mobile Application Management (MAM):** appbeheer voor het controleren van toegang tot intern ontwikkelde en commercieel beschikbare mobiele apps die worden gebruikt in zakelijke omgevingen. Organisaties kunnen een eigen, separate enterprise appstore inrichten. **Mobile Content/Information Management (MCM/MIM):** type software waarmee inhoud gemakkelijk en veilig kan worden gedeeld vanaf elk apparaat in een specifieke onderneming om ervoor te zorgen dat bedrijfsinformatie uniform is en veilig blijft. **Mobile Device Management (MDM), kortweg toestelbeheer:** geautomatiseerd uitrollen en centraal monitoren en beheren van mobiele apparaten. Mobiele apparaten in een organisatie moeten goed beheerd en beveiligd worden door bijvoorbeeld het instellen van een pincode of doordat gegevens op afstand kunnen worden gewist. **Mobile Endpoint Security (MES):** biedt uitgebreide en continue risicobeoordeling om gebruikers te beschermen tegen app-, apparaat-, netwerk- en phishinggebaseerde bedreigingen. **Multi Factor Authentication (MFA)/encompassing authentication/2 Factor Authentication (2FA):** een elektronische authenticatiemethode waarbij een gebruiker alleen toegang krijgt tot een website of applicatie nadat hij/zij met succes twee of meer bewijzen (of factoren) heeft gepresenteerd aan een authenticatiemechanisme: kennis (iets dat alleen de gebruiker weet), bezit (iets dat alleen de gebruiker heeft) en inherentie (iets wat alleen de gebruiker is). **Unified Endpoint Management (UEM): EMM + laptops + Internet of Things (IoT):** kan endpoints devices op afstand beheren en beveiligen; kan apparaten op verschillende platforms beheren – in ieder geval theoretisch – waardoor het eenvoudiger wordt om hardware af te sluiten en kritieke gegevens te beschermen. Het is een verdere ontwikkeling van EMM dat zich ook toepast op smartphones en tablets. Ook op andere met het internet verbonden apparaten. **Zero Trust Security Model (ZTSM)/ Zero Trust-Architecture (ZTA), Zero Trust-Netwerk Architecture, (ZTNA) perimeter-less security:** een benadering van het ontwerp en de implementatie van IT-systemen. Het belangrijkste concept achter het zerotrustbeveiligingsmodel is 'never trust, always verify', wat betekent dat apparaten standaard niet mogen worden vertrouwd.

Doorlopende digitale transformatie is investeren in digitale inclusie!

stelt medewerkers in staat mee te denken over technologische toepassingen voor de bedrijfsprocessen binnen de organisatie als geheel.

Omdat medewerkers digitaal vaardiger zijn, vinden zij ook meer `oplossingen' voor (vermeende) technische problemen. Medewerkers helpen elkaar, sturen onderling e-mails met oplossingsrichtingen, in plaats van dat ze contact opnemen met de ICT-helpdesk. Net zoals ze als privépersoon zelf oplossingen zoeken in een communityplatform.

Sommige apps voor mobiele apparaten verzamelen data over individuele gebruikers (bijvoorbeeld persoons- en locatiegegevens) en sturen deze op de achtergrond naar derden (bijvoorbeeld externe servers, ontwikkelaars of adverteerders) en zelfs soms zonder de gebruiker te informeren. Bedrijfsgeheimen en andere bedrijfsgevoelige informatie kan zo buiten de onderneming wegvloeien.

100% security vrijwel onmogelijk

Een afdoend niveau van informatiebeveiliging en privacybescherming is uiteraard noodzakelijk, maar tegelijkertijd niet altijd vanzelfsprekend en veel organisaties zijn zich hiervan bewust. Natuurlijk kan men reguleren dat updates en patches ten alle tijde zo spoedig mogelijk moeten worden doorgevoerd. Het is vrijwel onmogelijk te controleren welke devices en applicaties de medewerkers precies gebruiken. Ook komt het voor dat door het bedrijf voorgeschreven IT-middelen niet altijd worden gebruikt. Voor `the tone at the top' is het - vanwege de voorbeeldfunctie - van belang dat veilige IT-applicaties worden gebruikt zodat de rest van de organisatie dat ook vanzelfsprekend vindt dat voorbeeld te volgen. Populaire berichtenapps, tablets en smartphones hebben toch best vaak de voorkeur boven de sterk beveiligde middelen omdat ze gemakkelijker, sneller en gebruiksvriendelijker zijn.

Tips en risicoanalyse

Er is een aantal beheersmaatregelen te bedenken om de integrale informatiebeveiligingssystematieken toe te passen. Bijgevoegd kader geeft een overzicht van al die mogelijkheden. Het Digital Trust Center (DTC), onderdeel van het ministerie van Economische Zaken en Klimaat (EZK), heeft de ambitie om het Nederlandse bedrijfsleven weerbaarder te maken tegen de toenemende cyberdreigingen. Op zijn site (8) geeft het DTC advies en tips voor het veilig gebruik van privé-devices voor bedrijfsactiviteiten, waaronder:

- Inventariseer het gebruik van mobiele apparaten in je bedrijf.
- Stel beleid op.
- Sla bedrijfsgegevens centraal op.
- Licht je medewerkers voor over de voordelen én risico's bij het gebruik van privé-middelen.
- Laat werknemers een wachtwoord instellen op hun toestel.
- Verplicht beveiligingssoftware en gebruik beveiligde verbindingen.
- Zet een apart netwerk op voor mobiele apparaten.
- Wijs werknemers op de risico's van inloggen op openbare wifi-netwerken.
- Creëer een zwarte lijst van niet-toegestane apps, of een white list met toegestane apps.
- Zorg dat je de mogelijkheid hebt om op afstand zakelijke data van het toestel te verwijderen.
- Zorg voor een incident response plan.

Voor bedrijfsprocessen is het belangrijk data te classificeren volgens de lijnen van beschikbaarheid, integriteit en vertrouwelijkheid. Afhankelijk van de classificatie-uitkoms kan een risicoanalyse worden uitgevoerd om de belangrijkste risico's te bepalen. Dat kan inzicht geven in wat en in hoeverre beveiligd moet worden. Daarbij wordt gekeken naar de kans op optreden van een dreiging, het te verdedigen belang, de mogelijke impact hiervan op de bedrijfsvoering en gebruiksvriendelijkheid. Vanwege de grote verscheidenheid aan organisaties, persoonlijke voorkeuren, devices, specifieke risico's en maatregelen is dit maatwerk. Met het beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes. Dit maakt dat de noodzaak voor een Work From Anywhere (WFA)-strategie in een stroomversnelling komt.

Mensen en digitale machines verplaatsen zich en houden verbinding tot applicaties al dan niet in de cloud. Dit vraagt om goede endpoint-beveiliging en wellicht toegang op basis van zero trust. Aan de andere kant is aandacht voor de thuisomgeving nodig: een goede wifi-accespoint. Voorts moet nagedacht worden hoe de ICT-afdelingen op afstand de updates en patches kunnen doorvoeren. Bij een WFA-strategie gaat het er om dat de werknemers devices, applicaties en data hebben om hun werkzaamheden beter en efficiënter te kunnen doen en cyber- en datasecurity behoort daar een vanzelfsprekend deel vanuit te maken.

Toch een overeenkomst?

In de huidige gedigitaliseerde samenleving kunnen er eindeloze ketenschakels zijn van dienstverleners en onderaannemers. Dan is het nog wel van belang om duidelijk in beeld te hebben hoe je de privacypositie van partijen bepaalt: wie de (gezamenlijke) verwerkingsverantwoordelijke(n) is of zijn, en wie de verwerker(s). Helder moet zijn met welk doel de devices en applicaties zijn aangeschaft. Is daarbij goed gekeken naar de algemene en bijzondere voorwaarden? Er is immers een dienst/product waar de koper geen of beperkte invloed op heeft. Zijn de rollen van verwerkingsverantwoordelijke en verwerker daarbij helder? Dan kunnen immers ook privacyregulaties als de AVG/ GDPR van toepassing zijn. Dan is de kans groot dat alle betrokken partijen, met de beste bedoelingen en vele (sub-)verwerkersovereenkomsten verder, toch non-compliant zijn (9).

De DDT leidt tot consumentisering en democratisering van IT en uiteindelijk tot digitale inclusie. De 'rollen' van burger, werknemer, werkgever en consument vervagen wanneer het gaat over het gebruik van IT-middelen. Hoe het ook zij, er blijft altijd één punt van aandacht: een voldoende awareness voor cyber- en informationsecurity.

Referenties

(1) onderzoek.amsterdam.nl/publicatie/de-positie-van-amsterdamse-minima-in-het-gebruik-van-digitale-middelen-en-media

(2) amsterdam.nl/bestuur-en-organisatie/college/wethouder/touria-meliani/persberichten/amsterdam-krijgt-cyberbank-laptops/

(3) De duidelijkste vertaling van 'consumerization' is 'consumentisering'. Met dank aan het verkregen advies van Wouter van Wingerden MA van de Taaladviesdienst van Genootschap Onze Taal www.onzetaal.nl/taalloket.; doetietsmettaal.nl

(4) enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes/COIT_Risk_Mitigation_Strategies

(5) zoek.officielebekendmakingen.nl/kst-35714-3.html

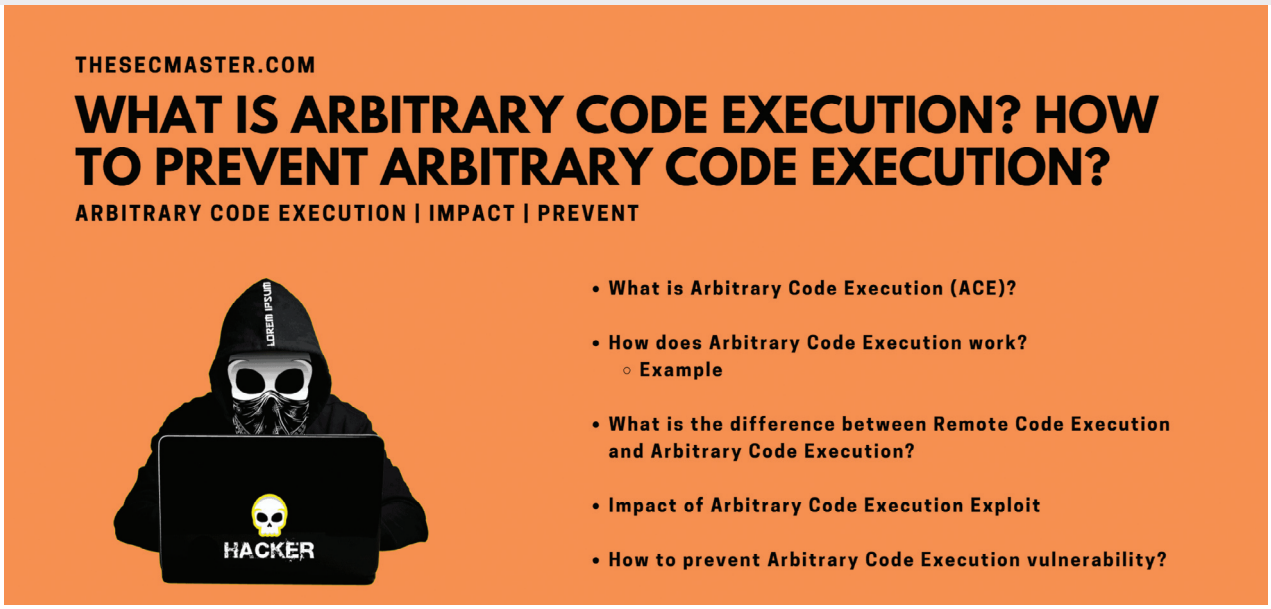
(6) fedweb.belgium.be/sites/default/files/Ozb-Circ%20702.pdf

(7) politieenwetenschap.nl/publicatie/politiekunde/2021/black-box-online-monitoring-bij-gemeenten-onderzocht-363/

(8) digitaltrustcenter.nl/informatie-advies/bring-your-own-device-byod

(9) Laan, V.I., Vaal, E.F. 'Hebben we een verwerkersovereenkomst nodig? Over het bepalen van de privacypositie van partijen', Tijdschrift voor Internetrecht, nr. 3 – juni 2021

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



BLOG

Smartphonetips voor vloggers en security professionals

Met deze vijf tips maak je betere video's en vlogs met je smartphone – en je kunt ze ook in je werk als security professional gebruiken.

1. Vliegtuigstand
2. Horizontaal filmen
3. Schone lens
4. Externe voeding
5. Statief en/of tape

Ad 1 Vliegtuigstand

Met een smartphone kun je bellen, whatsappen, sms-berichten ontvangen en geluidssignalen horen als je op een van je accounts mail ontvangt. Het is stiller en daarmee beter om deze mogelijkheden voor en tijdens het filmen allemaal in een keer uit te zetten met de 'vliegtuigstand' van je telefoon. Information security is inderdaad een verantwoordelijkheid van elke medewerker. Toch is het goed op een aparte afdeling een aantal deskundige experts zich uitsluitend op security te laten richten. Is de afdeling security groot genoeg, dan kun je de SOC-medewerkers, software patchers, risk self assessmentbegeleiders, threat intelligence analisten en threat hunters ieder geconcentreerd hun eigen specialisme goed laten doen.

Ad 2 Horizontaal filmen

Houd tijdens het filmen je smartphone horizontaal, zodat de afdrukknop rechts zit. De cameralens links zit dan bovenaan. Je kunt weliswaar ondersteboven filmen en daarna het beeld in je video-editing pakket omdraaien, maar dit kost tijd en gaat soms ook ten koste van de beeldkwaliteit. Zoals je foto in Windows Explorer een kwartslag draaien en opslaan: dan past de nieuwe foto ineens in minder bytes. Als je met de smartphone rechtop filmt, krijg je zwarte strepen links en rechts, als een soort zuilen. Voor TikTok is dat goed genoeg, maar niet voor breedbeeld-tv. Als je rapporteert over threats, noem dan niet alleen de risico's

voor security, maar in de volle breedte. Leg ook uit wat de risico's zijn voor andere afdelingen, met name buiten IT. In een presentatie over een bepaalde threat gaf ik zelf ooit aan: RCE. Ik ging er vanuit dat iedereen in de security meeting dit begreep als 'Remote Code Execution'. De aanwezige IT-directeur wist het echter duidelijk niet. Hij vroeg: "Dus thuiswerken. Dat willen we toch graag?" (Ja hij wel, dacht ik, met zijn stomme iPad). "Nee," zei ik, "RCE is dat de externe aanvallers willekeurige code kunnen uitvoeren op je machines." "Maar wat kunnen ze dan doen?" wilde de eindverantwoordelijke voor het IT-budget weten. "Alles," zei ik, naar waarheid. Dit bevreemdde hem, zoals hij terstond liet merken: "Hoezo alles?" Hierbij keek hij grijnzend rond de tafel. "Alles wat ze willen, ze kunnen op afstand willekeurig doen wat ze willen met die code," lichtte ik toe en begon te twijfelen aan mijn aanname, dat iedere IT-medewerker wist dat computers met software werken en zo nu eenmaal alles kunnen. Moest ik dat ook nog erbij zeggen? Ik keek rond en zag collega security professionals me zwijgend zachtjes toeknikken, hun schouders licht ophalen, de ogen ten hemel slaan en diep, zeer diep ademhalen. De beste man was me voor, deed nu in de volle zaal alsof ik het niet begrijpende vierjarige kind was en zei, lang-zaam ar-ti-cu-le-rend: "Maar dan moeten ze toch wel heel toevallig net die ene juiste code raden om iets te kunnen doen, wat is nou de kans daarop?" Voor mij was die kans op iets kwaadaardigs 100%, omdat het deskundige misdadige aanvallers betrof, die er bovendien hun werk van maakten. Dat zei ik hardop en toen was gelukkig de security meeting afgelopen, althans de IT-directeur moest plots ergens anders heen.

Ad 3 Schone lens

Toegegeven, de gevoeligheid en afmetingen van de sensor in de camera zijn óók belangrijk voor de beeldkwaliteit. Maar maak de lens van je smartphone voor het filmen altijd schoon, dan ziet de opname er beter uit en zelf kom je bij degene die je bijvoorbeeld gaat interviewen, goed voorbereid en professioneel over. Als je buiten filmt en het regent, absorbeert keukenrol of wc-papier de waterdruppels op de lens beter dan een lensdoekje. Een paraplu lijkt handig, maar de smartphone met twee handen vasthouden is voor een rustig, stabiel beeld een beter idee. In security rapportages zie ik een schone lens als objectief en onpartijdig rapporteren. Over security dreigingen, interne fouten en vergissingen, gekozen oplossingen tegen die fouten, en over de gemaakte fouten in die oplossingen. Hoe neutraler en minder vertekend je rapportage, des te langer je eigen houdbaarheid als security analist. Het helpt om vastleggingstaken te rouleren en iemand anders een keer de analyse te laten schrijven. Wanneer er grote verschillen zijn in aantal ervaringsjaren tussen medewerkers, lijkt het beter het werk niet geheel over te dragen maar om 'de andere specialist' te laten meelezen of redigeren, als tweede paar ogen.

Ad 4 externe voeding

Beknoptheid in afgemonteerde video's is zeer belangrijk. Maar je wil wel de totale geplande ruwe opname kunnen maken met je smartphone. En bij het monteren denk je achteraf vaak: had ik maar wat extra materiaal 'geschoten'. Daarmee kun je namelijk de knip rond een verspreking mooi maskeren of heb je een duidelijke overgang naar het volgende onderwerp. Of toelichtend beeld bij een bepaalde vakterm (zoals: RCE). Neem dus een opgeladen (!) powerbank mee om, zolang je zelf wil, alles stroomintensief te kunnen filmen met je smartphone.
Als security manager is het belangrijk om voldoende tijd en budget voor je afdeling en personeel te krijgen. Ook duurzaam stakeholdermanagement (zoals het handig omgaan met je IT-directeur, zie punt 2) is noodzakelijk om je securitytent draaiend te houden.

Ad 5 Statief en/of tape

Met een camerastatief is je beeld stabieler en komt de gefilmde persoon zekerder en standvastiger over. Ook de cameraman zelf lijkt door statiefgebruik minder op een trillende zenuwpees. Een simpele selfiestick is als éénpoot al nuttig. Met (duct)tape kun je zonder een statief mee te zeulen, toch de smartphone overal plaatsen en dus ook midden op de velg van een autowiel plakken en langzaam rijdend indrukwekkende beelden schieten. Of de camera tegen de achterkant in de koelkast, waar dan de vlogger iets uitpakt: zwart, licht, gezicht, hand, bier, zwart, gesprekstafel met twee personen en twee blikken bier. Inleidende sfeerbeelden.

Ook als security afdeling is zichtbare, stevige externe support essentieel voor je imago en uitstraling. En niet alleen FTE en geld, maar ook voldoende aandacht en waardering (denk: 'serieus nemen') vanuit topmanagement zodat je tijdig betrokken wordt bij nieuwe projecten, waar je je als security professional dan als 'trusted advisor' van begin tot eind aan kunt hechten.

Digitaal zoomen: niet doen

Tot slot: digitaal zoomen op je smartphone is een slecht idee voor de beeldkwaliteit. Een onderwerp of persoon haal je dichterbij met je benen en niet met je vingers op het scherm.
Ook in securityland is het beter (af en toe) fysiek bij iemand langs te gaan voor een kop koffie, thee of maté dan jullie contact geheel digitaal te houden met alleen Whatsapp, e-mail of Zoom.

Toi toi toi.

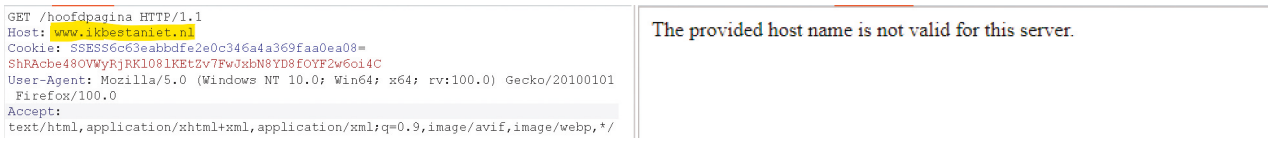
Auteurs: Maarten Hartsuijker is PViB-redactielid en beschermt en hackt al 20 jaar met veel plezier websites, apps, netwerken en applicaties. Maarten is te bereiken via m.hartsuijker@classity.nl.

Host header injection

SQL injection, OS Command Injection, XML Entity Injection. Wie al even meedraait in de wereld van webapplicatiebeveiliging heeft er ongetwijfeld weleens over gehoord. Het zijn allemaal aanvalsvormen die via het versturen van onverwachte verzoeken naar een webserver ertoe kunnen leiden dat aanvallers toegang tot het systeem krijgen. Vaak door ingewikkelde karakterreeksen op te sturen die het programma andere (of extra) opdrachten laat uitvoeren.

Een injectionfout – waar je mogelijk nog niet eerder van hebt gehoord – is de 'host header injection'. De host header is een onderdeel van het HTTP protocol (1). Webservers waarop meerdere websites aanwezig zijn gebruiken de host header om te bepalen in welke directory de webapplicatie zich bevindt. Een webserver waarop drie websites aanwezig zijn beschikt daarbij vaak over vier configuraties: de standaardconfiguratie (+1) en een configuratie per website (+3).

Figuur 1 - Host: www.classity.nl verwijst naar website.



Figuur 2 - De webserver vangt een niet bestaande host header netjes af.

Hierboven zijn twee identieke verzoeken aan dezelfde webserver te zien, waarin enkel de host header is gewijzigd. In figuur 1 wordt een op de server aanwezige website getoond nadat deze met een correcte host header is opgevraagd. Figuur 2 toont in dit voorbeeld geen website, aangezien de host header verwijst naar een site die niet expliciet op de server is ingesteld. Maar vaak wordt er ook wel voor gekozen om bij het aanroepen van een niet bestaande website te verwijzen naar de standaarddirectory. En deze standaarddirectory bevat in dat geval vaak de hoofdwebsite van de server. Ogenschijnlijk kan de keuze om gebruikers de hoofdwebsite te tonen op het moment dat ze een niet bestaande site aanroepen weinig kwaad. Men ziet op dat moment immers over het algemeen een website die toch al online is. Daar waar het gaat om het tonen van de site is dit ook zeker het geval. Maar de impact wordt anders op het moment dat de applicatie de host header in de applicatielogica verwerkt.

Waar gebruikt de applicatie de host header voor?

Voor webapplicaties die meerdere keren geïnstalleerd worden (dev/test/prod) kan het handig zijn om de links binnen de site dynamisch op te bouwen. Je wil immers voorkomen dat klanten op de website www.website.nl hyperlinks tegenkomen die verwijzen naar test.website.nl of dev.website.nl. Dit is het eenvoudigst op te lossen door elke link op relatieve wijze op te bouwen. Binnen de website zelf kan dit over het algemeen het beste door het domein weg te laten en te verwijzen naar /pagina1, /pagina2 etc. Maar soms ontkom je er niet aan om een volledige URL te gebruiken. Wanneer de applicatie bijvoorbeeld een mail verstuurt, moet het domein wel in de link zitten. De host naam van de URL wordt daarvoor vaak uit de host header gehaald. Oftewel: https://$HOSTHEADER/ga-naar-deze-pagina.

Wachtwoordreset

Op het moment dat een website op basis van elke host header de hoofdwebsite toont én deze host header gebruikt om bijvoorbeeld een wachtwoordlink mee op te maken, ontstaat er een risicovolle situatie. Een aanvaller die met een valse host header wachtwoordresets initieert voor bestaande gebruikers zal er dan immers voor zorgen dat de resetmails naar een kwaadaardig domein kunnen verwijzen. Zodra een gebruiker op de link klikt is de aanvaller in het bezit van de geheime resetcode en kan hij met gebruikersrechten inloggen in de applicatie. En indien een aanvaller een domein registreert die op het echte domein lijkt wordt de kans op succes natuurlijk nog veel groter dan in het onderstaande voorbeeld.

Figuur 3 – Wachtwoordreset.

Caching

Het manipuleren van links die via de mail worden verzonden is niet het enige risico van host header injection. Zodra een applicatie deze header ook binnen de applicatie zelf gebruikt én de werking van de publieke pagina's van de applicatie versnelt met een cachingmechanisme, ontstaat voor aanvallers ook een mogelijkheid om HTML en/of Javascript in de cache te injecteren. Als de applicatie een pagina in de cache opslaat waarin de host header is verwerkt, dan kan de aanvaller de cache vervuilen met pagina's die de CSS of Javascript inladen vanaf zijn eigen kwaadaardige site (https://$HOSTHEADER/js/main.js). De eerstvolgende bezoeker ontvangt via de door de cache aangeboden pagina vervolgens javascriptcode die afkomstig is vanaf https://kwaadaardig.classity.nl/js/main.js.

Zelf proberen

Ben je benieuwd of dit ook jouw website treft? Verwijs je webbrowser tijdens het surfen eens naar een proxy. Programma's zoals OWASP Zap (2) zijn vrij te gebruiken. Je kunt de verzoeken die je browser naar de webserver verstuurt in het programma onderscheppen, terugzoeken en (nadat je de host header hebt aangepast) opnieuw versturen. Krijg je op dat moment een mailtje binnen met de aangepast URL? Dan weet je dat de configuratie van jouw website (of webapplicatie) een aanpassing nodig heeft.

Referenties

(1) https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Host

(2) https://www.zaproxy.org/

Auteur: Chris de Vries is redacteur van iB-Magazine en werkt als consultant onder de naam De Vries Impuls Management. Hij is bereikbaar via impuls@euronet.nl.

Zware onvoldoende voor overheid

Algemene Rekenkamer: na aandacht nu toetsing van Rijksalgoritmes

De overheid zet algoritmes in met als doel onder andere automatisering, effectiviteit en voorspelling. Daarom heeft de Algemene Rekenkamer aandacht voor de automatiseringsbesluiten van onze Rijksoverheid. Zij ziet het als haar taak om overzicht, kwaliteitscontrole en ethische vraagstukken te beoordelen zodat verantwoord complexe, geautomatiseerde toepassingen op basis van algoritmes ontwikkeld kunnen worden (1,2). Dit mondde uit in een toetsingskader en een recente beoordeling (3,4).

Even terug naar 26 januari 2021 toen de Rekenkamer haar eerste onderzoek: *Aandacht voor algoritmes* (1,2) publiceerde. Daar formuleerde zij een belangrijke voorwaarde: 'De Rekenkamer schrijft dat vragen van bezorgde burgers over de toepassing van algoritmes meer aandacht verdienen' (1).

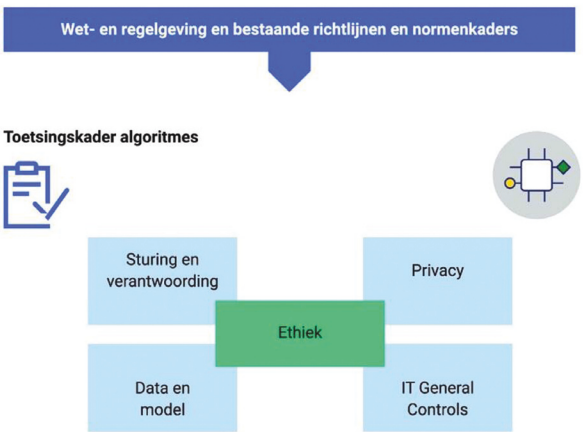
Op 18 mei 2022 publiceerde de Rekenkamer haar tweede onderzoek: *Algoritmes getoetst* (3) met als conclusie dat van negen algoritmes er drie zijn die voldoen aan alle basisvereisten en zes algoritmes uiteenlopende risico's vertoonden zoals: gebrekkige controle op prestaties of effecten, vooringenomenheid (bias), datalek of ongeautoriseerde toegang (4).

Onderzochte algoritmes en de selectiecriteria

Bij het onderzoek naar de algoritmes heeft de Rekenkamer een selectie gemaakt gebaseerd op volgende criteria:

- De impact op burgers of bedrijven.
- Risicogericht (waar is de kans het grootst op niet juiste inzet?).
- Verschillende domeinen (bv. sociaal - en veiligheidsdomein).
- Het in gebruik zijn van het algoritme.
- De soort van algoritme (van beslisbomen tot zelflerende toepassingen).

Doordat risicogericht gezocht is, zijn niet alle door de Rijksoverheid gebruikte algoritmes meegenomen. Daarom benadrukt de Algemene Rekenkamer dat de uitkomsten van het onderzoek niet de basis kunnen vormen voor algemene conclusies over processen, organisaties of de gehele Rijksoverheid.



Opmerking bij tabel 1:
1. Rwt: rechtspersonen met wettelijke taak.
2. Zbo: zelfstandige bestuursorganen.

In het onderzoek wordt aangegeven dat de onderzochte algoritmes in twee groepen zijn te verdelen: technisch eenvoudig tegenover technisch complex. Het tweede onderscheid zit in de functie van het algoritme: automatische besluitvorming versus ondersteunende. De automatische besluitvorming vindt men terug bij: RVO (Rijksdienst voor Ondernemend Nederland), Toeslagen, CBR (Centraal Bureau voor de uitgifte van Rijvaardigheidsbewijzen) en SVB (Sociale Verzekeringsbank). De ondersteunende algoritmen zijn de overige algoritmes van tabel 2, waarbij het RvIG (Rijksdienst voor Identiteitsgegevens) en de politie gebruik maken van de technisch complexe algoritmes.

Dit toetsingskader zoals ook in tabel 1 weergegeven, zij het in tabel 1 zonder het ethisch perspectief, ziet er als volgt uit:

Min	Organisatie	Status	Omschrijving algoritme
BZK	Rijksdienst voor Identiteitsgegevens (RvIG)	Agentschap	Ondersteunt bij de beoordeling van de kwaliteit van foto's voor identiteitsbewijzen
EZK	Rijksdienst voor Ondernemend Nederland (RVO)	Agentschap	Risicomodel dat gebruikt wordt bij de beoordeling van aanvragen voor de Tegemoetkoming Vaste Lasten (TVL)
FIN	Toeslagen	Onderdeel ministerie	Ondersteunt bij de beoordeling van aanvragen voor huurtoeslag in het Toeslagenverstrekkingensysteem (TVS)
IenW	Centraal Bureau Rijvaardigheids-bewijzen (CBR)	rwt/zbo	Ondersteunt bij de beoordeling van de medische rijgeschiktheid van mensen
JenV	Politie	rwt	Criminaliteits Anticipatie Systeem (CAS) voorspelt waar en wanneer het risico op incidenten hoog is
JenV	Directoraat-generaal (DG) Migratie	Onderdeel ministerie	Zoekt intelligent in vreemdelingen-persoonsgegevens of iemand al eerder in Nederland is geregistreerd
JenV	Centraal Justitieel Incassobureau (CJIB)	Agentschap	Koppelt gegevens voor verkeersboetes aan op kenteken geconstateerde verkeersovertredingen
SZW	Inlichtingenbureau (IB)	rwt	Levert signalen aan gemeenten voor rechtmatigheidscontrole op bijstands-uitkeringen
SZW	Sociale Verzekerings-bank (SVB)	rwt/zbo	Ondersteunt bij de beoordeling van AOW-aanvragen

Tabel 1 - Overzicht van geselecteerde algoritmes. Bron: Algoritmes getoetst, pagina 10 [3].

Op pagina 13, hoofdstuk 2.2.2 Inzet van algoritmes getoetst uit het rapport Algoritmes onderzocht (3) wordt het ethisch perspectief als volgt omschreven:

1. Respect voor de menselijke autonomie.
2. Voorkomen van schade.
3. Fairness (een eerlijk algoritme).
4. Verklaarbaarheid en transparantie.

Zoals figuur 1 aangeeft is het ethisch perspectief gekoppeld aan alle andere perspectieven.

Om een van de bevindingen naar voren te halen gaan wij kort in op het privacyperspectief en dan met name over de verplichting om in sommige gevallen een Data Protection Impact Assessment (DPIA) oftewel een gegevensbescherming-effectbeoordeling uit te voeren. Uit de toetsing blijkt dat zeven van de negen uitvoeringsinstanties c.q. de onderzochte algoritmes of de processen waar zij deel van uitmaken een DPIA hebben gerealiseerd. Twee dus niet en dat zijn de Rijksdienst voor Identiteitsgegevens (RvIG) en de politie. Door geen DPIA uit te (laten) voeren kunnen deze instanties niet gestructureerd volgens vastgestelde methodiek beoordelen of risico's afgedekt zijn. Ook het niet proportioneel gebruik of verzamelen van gegevens (dataminimalisatie) is bij acht van de negen organisaties met maatregelen beschreven, met uitzondering van de politie, die bijvoorbeeld gegevens over de nationaliteit verzameld, maar die niet gebruikt in de algoritmeberekeningen. De Rekenkamer ziet ook bevestigd dat de problemen met IT-beheer bij de Rijksoverheid (Algemene Rekenkamer, 2020) ook bestaan bij zes van de onderzochte algoritmes en spijtig genoeg – cursivering en toevoeging auteur – op veel vlakken.

Toetsingskader algoritmes versie 1.0

De Algemene Rekenkamer stelt aan geïnteresseerden de Toetsingskader algoritmes versie 1.0 (5) beschikbaar dat bestaat uit drie tabbladen, respectievelijk: Over het toetsingskader, Toetsingskader algoritmes en Ethische principes.

Het eerste tabblad is een uiterst leesbaar overzicht van de uitgangspunten, hoe de gebruiker/geïnteresseerde (overheid/bedrijfsleven) aan de slag gaat en een verdieping aangaat ten aanzien van het ethisch perspectief. Het is helder, verfrissend en dus prettig om op een dergelijke wijze verleid te worden dit kader te gaan gebruiken. Dat geldt niet alleen voor (overheids)organisaties, maar ook voor andere bedrijfsorganisaties.

Het tweede tabblad is het werkblad. Ook hier is helderheid nagestreefd en de (toelichtende/onderzoeksvraag) teksten lezen vlot. Prettig is de vermelding van bronnen. Het gebruik van dit toetsingskader wijst zich haast als vanzelf.

Het derde tabblad over de ethische principes koppelt elk ethisch principe en de daarbij behorende subonderdelen aan het toetsingskader, respectievelijk het gerelateerd risico en de bronnen van deze principes. Goed geordend, een goede leidraad voor de gebruiker die zich ook wil verdiepen in de achtergronden.

Het enige waar de gebruiker even attent op moet zijn is dat op het eerste tabblad de afbeeldingen Over het toetsingskader en Aan de slag met ethiek iets naar onderen toe uitgetrokken moeten worden om de volledige tekst te lezen. Tip voor het derde tabblad: vergroot de eerste rijhoogte naar waarde 220 en trek dan de afbeelding De ethische principes (links bovenaan bij veld A1) iets uit, dan ziet men ook het ethische principe 4. Kleine euveltjes waar een ervaren Excel-gebruiker al snel de weg weet te vinden.

Zie ook het rapport Algoritmes getoetst, pagina's 46 t/m 51 voor de onderzoeksvragen (3).

Het onderzoek naar algoritmes

'We hebben in ons onderzoek gezien dat drie van de negen algoritmes aan het toetsingskader voldoen. Dit laat zien dat je algoritmes op een eerlijke, verstandige manier kunt gebruiken. We hebben ook gezien dat zes van de negen onderzochte algoritmes niet helemaal voldoen aan de voorwaarden in ons toetsingskader. Er zijn nog veel dingen die beter kunnen' (3). De

Rekenkamer formuleert als eerste conclusie dat als de overheid een andere organisatie vraagt om een algoritme te maken (uitbesteding) een gebrek aan goede afspraken ertoe kan leiden dat zij zelf niet meer in de gaten kan houden of het algoritme veilig gebruikt wordt.

De tweede conclusie is dat het IT-beheer beter moet. Toegang en autorisaties moeten de gegevens van de burger en het bedrijfsleven veilig stellen, maar dergelijke afspraken ontbreken te vaak, zie tabel 1 van het toetsingskader. En dan de derde conclusie: de vooringenomenheid. De meeste van de onderzochte organisaties controleren de fouten in algoritmes niet en kunnen dus niet weten of de uitkomsten van die algoritmes voor iedereen hetzelfde zijn.

Deze constateringen leiden tot de vraag of er sprake is van een incidentele waarneming of van een structureel probleem. Door middel van dit artikel geef ik mijn visie op die vraag/constatering. Samengevat geeft het toetsingskader van de Algemene Rekenkamer het volgende beeld van de negen algoritmes bij de negen onderzochte uitvoeringsorganisaties:

		Toetsingskader van de 9 onderzochte algoritmes								
Rijksdiensten		CBR	CJIB	IB	RVO	Toeslagen	SVB	DGM (JenV)	RvIG	Politie
Perspectieven										
Sturing en verantwoording	Taken en verantwoordelijkheden	Δ	Δ	Δ	Δ	∇	∇	∇	∇	∇
	Risico afwegingen	Δ	Δ	Δ	Δ	Δ	∇	∇	∇	∇
	Governance bij uitbesteding	Δ	Δ	O	O	O	O	∇	∇	O
	Monitoring	Δ	Δ	Δ	Δ	Δ	Δ	∇	∇	∇
Data en Model	Bias model	O	O	O	Δ	O	O	∇	∇	∇
	Bias data	O	O	O	Δ	O	O	O	Δ	∇
Privacy	DPIA	Δ	Δ	Δ	Δ	Δ	Δ	Δ	∇	∇
	Dataminimalisatie	Δ	Δ	Δ	Δ	Δ	Δ	Δ	Δ	∇
	Privacybeleid	Δ	Δ	Δ	∇	∇	Δ	O	∇	∇
IT beheer (**IT General Controls - ITGC**)	Toegangsbeheer	Δ	Δ	Δ	∇	∇	∇	∇	∇	∇
	Wijzigingen-beheer	Δ	Δ	Δ	∇	∇	∇	∇	∇	∇
	Backup en recovery	Δ	Δ	Δ	∇	∇	∇	∇	∇	∇
Algoritme voldoet wel/niet aan het toetsingskader		√	√	√	X	X	X	X	X	X

∇	Het resterende risico met betrekking tot dit element is midden tot hoog
Δ	Het resterende risico met betrekking tot dit element is laag
O	Element uit toetsingskader niet van toepassing op algoritme

Tabel 2 - Bewerkt toetsingskaderoverzicht van 9 algoritmes [3].

Het betreffen hier zowel complexe als eenvoudige algoritmes. Deels zijn deze automatisch besluitvormend (toekenning toeslagen, voldoen aan steunvoorwaarden, medische rijgeschiktheid), deels ondersteunend (verkeersboetes verzenden). In de tabel ontbreekt de weergave van het perspectief 'ethiek', maar dat vormt de verbindende factor tussen de overige vier perspectieven.

Reacties en aanbevelingen

Het rapport zelf leidt tot uiteenlopende reacties. De staatssecretaris voor digitalisering grijpt direct in en wil vóór het zomerreces de tekortkomingen (laten) oppakken (3, pagina 36 & 37). Ambitieus! – cursivering en toevoeging auteur. De politie en de Dienst Migratie lijken daarvan af te wijken (3, pagina 38). De politie is het niet eens met het door de Rekenkamer gehanteerde toetsingsmodel en zij acht haar algoritme niet vallend onder de AVG, maar onder de Wet politiegegevens, bron: Tweakersnet d.d. 18.05.2022: 'Rekenkamer: 6 van 9 onderzochte overheidsalgoritmen voldoen niet aan basiseisen' (3, pagina 38 en referentie 6).

Een zorgelijke waarneming als alleen het CBR, het Centraal Justitieel Incassobureau (CJIB) en het Inlichtingenbureau (IB) weten te voldoen aan alle basisvereisten, terwijl de politie dat ten aanzien van geen enkel perspectief weet te realiseren.

'Daarnaast vinden wij de reacties van zowel DG Migratie als de politie zorgelijk. Het lijkt ons goed als de verantwoordelijke vakminister deze organisaties vraagt de door ons gesignaleerde risico's aan te pakken, 'omdat deze wel degelijk burgers kunnen raken' – cursivering auteur – (3, pagina 38).

Het geheel overziende slaagt twee derde van de uitvoeringsinstanties niet, getuige het toetsingskader (4) én... dat begint en staat met IT-beheer en de vooringenomenheid! De aanbevelingen van de Rekenkamer richten zich daar dan ook op:

1. Maak afspraken en monitor de nakoming daarvan bij uitbesteding of inkoop.
2. Bescherm algoritmes en data door goed functionerende IT-beheersmaatregelen.
3. Controleer voortdurend (ontwerp/uitvoering) op het effect van vooringenomenheid.
4. Heb aandacht bij publieke taken uitvoeringsalgoritmes voor het toezicht op instellingen op afstand van het Rijk.

De eerste twee aanbevelingen dateren van januari 2021, het eerste rapport van de Algemene Rekenkamer Aandacht voor algoritmes (2), de laatste twee zijn nieuw.

Welke koers voor de toekomst?

Wat kan het voorgaande ons leren c.q. aan inzichten verschaffen? Allereerst dat security-by-design en aansluitend daarop privacy-by-design niet alleen begrippen zijn die in het bedrijfsleven best moeilijk realiseerbaar zijn, maar blijkbaar ook bij de overheid dan wel haar uitvoeringsorganisaties. Dat

Andere actuele bronnen

De 'Inspectie Justitie en Veiligheid is bezorgd om commerciële hacksoftware politie' (7). De Inspectie spreekt haar bezorgdheid uit ten aanzien van de privacy van verdachten door het hacken van hun systemen met commerciële software, waarbij niet gegarandeerd kon worden dat alleen de politie bij de gegevens kunnen. Geen verandering ten opzichte van vorig jaar luidde haar conclusie.

Dit nieuwtje is afkomstig van Tweakersnet d.d. 31-05-2022 en het betrof de 23 zaken waar de commerciële software is ingezet gedurende 2021 Net als de Algemene Rekenkamer noemt de Inspectie deze software een black box. Dus ook vanuit 'eigen huis' eenzelfde oordeel.

In een interessant websiteartikel van mr. Arnoud Engelfriet (Ius mentis d.d. 25-05-2022 getiteld: Meerdere algoritmen van de overheid voldoen niet aan de basiseisen (8)) vraagt hij aandacht voor de verschillende soorten foutrisico's waarbij hij kansen ziet voor de private sector om de overheid te assisteren bij het tot stand brengen van de procedurele transparantie (ibid. (8) in de op één na laatste paragraaf).

Dit standpunt deel ik.

Problemen zijn er om kansen uit te putten.

bovendien ook daar het IT-beheer op een hoger plan moet komen.

In mijn beleving leeft authenticatie en autorisatie volop in het bedrijfsleven. Ontwerpoverwegingen besteden dan ook veel aandacht aan het toegangsbeheer. Bij de overheid mag hier wel een schepje bovenop, zie het toetsingskader. Het bedrijfsleven draagt verantwoordelijkheden tegenover haar klanten, leveranciers en de keten(s), dat ze met de haar beschikbaar gestelde of ter beschikking gekomen data zorgvuldig omgaat (economische en privacybelangen). De overheid draagt die verantwoordelijkheden op een veel grotere schaal (de burger en het bedrijfsleven in de meest ruime zin). Dat omvat de essentiële burgerdata die letterlijk/figuurlijk het wel of niet bestaan van de burger raakt (inclusief diens rechten en/of verplichtingen, eveneens een vitaal belang).

Zoals je het ook kan benaderen: problemen zijn er om kansen uit te putten. Overheid, bedrijfsleven en de burger zouden moeten onderzoeken hoe samenwerking en betrokkenheid bevorderd kunnen worden, om uiteindelijk ICT, AI en algoritmes te verbeteren/transparanter te maken zodat acceptatie (vertrouwen) kan toenemen. Nu blijkt te vaak dat vertrouwen in de algoritmes van de overheid afneemt en daarmee de acceptatie.

Referenties

(1) https://www.rekenkamer.nl/publicaties/rapporten/2021/01/26/aandacht-voor-algoritmes

(2) https://www.rekenkamer.nl/binaries/rekenkamer/documenten/-rapporten/2021/01/26/aandacht-voor-algoritmes/Aandacht+voor+algoritmes.pdf

(3) https://www.rekenkamer.nl/binaries/rekenkamer/documenten/-rapporten/2022/05/18/algoritmes-getoetst/108+AR+rapport+Algoritmes+II+DEF+220516.pdf

(4) https://www.rekenkamer.nl/actueel/nieuws/2022/05/18/diverse-algoritmes-rijk-voldoen-niet-aan-basisvereisten

(5) https://www.rekenkamer.nl/binaries/rekenkamer/documenten/-publicaties/2021/01/28/download-het-toetsingskader/Toetsingskader+algoritmes+v1.0.xlsx

(6) https://tweakers.net/nieuws/196914/rekenkamer-6-van-9-onderzochte-overheidsalgoritmen-voldoen-niet-aan-basiseisen.html

(7) https://tweakers.net/nieuws/197410/inspectie-justitie-en-veiligheid-is-bezorgd-om-commerciele-hacksoftware-politie.html?utm_source=nieuwsbrief&utm_-medium=email&utm_campaign=twk_nieuwsbrief

Dimitri van Zantvliet is CISO bij de Nederlandse Spoorwegen en columnist van iB-Magazine.

COLUMN DIMITRI

Birds of a feather, shift left together!

De vijftiende verjaardag van PvIB, van harte gefeliciteerd! Het is een eer voor mij om via dit mooie platform bij te mogen dragen aan het verspreiden van zoveel jaren cyberlove. Ik schrijf deze column trouwens op 25 mei, de vierde verjaardag van GDPR (General Data Protection Regulation). Met een hoop bombarie kwam de wet onze organisaties binnen. Stevige boetes zouden uitgedeeld gaan worden als de regels overtreden zouden worden. Waar organisaties nog geen privacy officers in dienst hadden werden wij bij cyber aangekeken. Ook ik behaalde diverse certificaten via de IAPP en heb destijds een hoop bijgeleerd over persoonsgegevens.

Dat uitdelen van boetes duurde echter nog wel even, want de meeste lokale Autoriteiten Persoonsgegevens hadden niet eens adequate middelen om al die meldingen te verwerken. De Belgische Gegevensbeschermingsautoriteit zat zelfs lange tijd zonder bestuur. Tandeloze tijgers werden ze genoemd en ook onze eigen AP kreeg het er in de pers van langs. Opmerkelijk, want de AP, eerst de registratiekamer genoemd en later omgedoopt tot College Bescherming Persoonsgegevens, bestaat al sinds de eind jaren tachtig. Veel langer dan het PvIB!

Enfin, de versnelling is deels gekomen en de fikse boetes ook: 746 miljoen euro voor Amazon, 225 miljoen euro voor WhatsApp, 90 miljoen voor euro voor Google Ierland, 60 miljoen euro voor Facebook en op nummer vijf Google LLC voor 50 miljoen euro. Iemand nog een cookie bij de koffie?

Op cybersecuritygebied hebben we een vergelijkbare wet die in dezelfde periode het levenslicht zag. De NIS Directive is de Europese netwerk- en informatiebeveiligingrichtlijn, de NIB-Richtlijn. Deze is in Nederland geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni). De Wbni schrijft een zorgplicht en een meldplicht voor aangaande cybersecurity. Men moet passende maatregelen treffen om de zaak goed te beveiligen en als het onverhoopt toch misgaat moet men hiervan melding doen. Als organisaties er met de pet naar gooien dan kan de toezichthouder een bestuurlijke boete van 5 miljoen euro opleggen. Kán…

Boetes zijn dus nog niet opgelegd onder de NIS maar ook in ons cybervakgebied is dat aan het verschuiven. De nieuwe NIS 2 Directive die op 13 mei 2022 door de EC en het Parlement is geratificeerd gaat voor veel meer organisaties gelden die enig belang hebben voor de vitaliteit van een economie. De boetes voor vitale organisaties zijn in deze nieuwe wet maximaal 10 miljoen euro of 2% van de wereldwijde jaarlijkse omzet. Dat percentage van de omzet is gebaseerd op de gemiddelde ransomwarebedragen die de afgelopen jaren worden gevraagd. De voorlopige melding van een incident moet overigens al binnen 24 uur gedaan worden. We zien de sectorale toezichthouders stevig opschalen op cyberkennis en -kunde gebied om invulling te kunnen geven aan toezicht op deze wetgeving. Het NCSC krijgt daarnaast via een spoedwet mandaat om breder threat intel uit te wisselen.

Naast de NIS 2 Directive is er de Cybersecurity Act en is de RED en Cyberresilience Act in de maak. De privacy- en securitywetgeving lijken dus na al die jaren dichter tot elkaar te komen en er komt misschien wel een moment – misschien duurt het geen vijftien jaar – dat een organisatie door meerdere toezichthouders tegelijkertijd beboet gaat worden na een stevige databreach.

Dit stelt vitale en belangrijke organisaties voor een volgende keuze: betaal ik miljoenen in bitcoins als ik geransomwared ben, betaal ik miljoenen aan boetes aan de toezichthouder(s) als ik de boel niet op orde had of investeer ik die bedragen om by design en by default de cybersecurity en dataprivacy op orde te brengen en te houden? Schuiven we nu samen voor eens en voor altijd op naar links in de application development cycles met cyber en privacy?

Time Fines will tell!

Achter Het Nieuws

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.

NIS 2 Directive: zijn we er in Nederland klaar voor?

In mei 2022 is er politieke overeenstemming bereikt over de tekst van de tweede versie van de Europese Network and Information Security Directive (NIS Directive). De concepttekst was in december 2020 gepubliceerd en de verwachting is dat dit najaar de definitieve tekst zal worden gedeeld.

Er zijn diverse verschillen met de eerste NIS Directive uit 2016. Zo zullen er meer sectoren worden aangemerkt als essentiële of belangrijke diensten. Maar ook kunnen Europese lidstaten ervoor kiezen om middelgrote en kleinere bedrijven met een hoog veiligheidsrisicoprofiel te identificeren. Dus kleine bedrijven met minder dan 50 medewerkers en een lagere omzet dan 10 miljoen euro kunnen ook onder de nieuwe wet gaan vallen. Voor al die organisaties worden de security-eisen aangescherpt door het verplichten van risicobeheersing, security van toeleveringsketens en leveranciersrelaties, een lijst van minimale basisbeveiligingelementen die toegepast moeten worden en verplichte rapportage van incidenten. Bovendien wordt de positie van toezichthouders versterkt en moeten alle spelers in het cybersecuritylandschap meer gaan samenwerken.

Zodra de NIS 2 definitief is, zal de Directive binnen 20 dagen ingaan, en krijgen lidstaten nog 21 maanden om de Directive om te zetten in nationale wetgeving. Zijn we hier in Nederland wel klaar voor? Hebben organisaties risicomanagement al voldoende ingebakken? Gaan we met de NIS2 niet een cultuur creëren van compliance-vinkjes zetten? Kunnen/willen de stakeholders in Nederland wel goed samenwerken?

Vinkjesmaatschappij - Maarten Hartsuijker

'Prima, die extra aandacht voor informatiebeveiliging', zou een eerste gedachte kunnen zijn bij het lezen van dit nieuws. Maar tegelijk zijn we ook wel een beetje een 'vinkjesmaatschappij' aan het worden. Terwijl ik deze reactie schrijf lees ik net in de krant over een Nederlander die


Chris de Vries


Fook Hwa Tan


Maarten Hartsuijker

zijn reis naar de VS moet annuleren. Hij had op zijn online visumaanvraag per ongeluk een verkeerd vinkje gezet. En een afspraak om een ambassademedewerker om die fout te laten corrigeren kan niet eerder dan in de zomer van 2023 plaatsvinden.
Een vergelijkbare impact van de vinkjesmaatschappij kan ook makkelijk in de informatiebeveiligingshoek ontstaan. Want hoewel sommige organisaties zeker een push kunnen gebruiken om zichzelf, ketenpartners en hun klanten beter te beschermen, wordt het voldoen aan regelgeving al snel het hoogste doel. Een doel dat ik (je kunt je tijd maar één keer besteden) niet zelden ten koste zie gaan van waardevolle inhoudelijke beveiligingswerkzaamheden.
Ik hoop van harte dat dit goede initiatief leidt tot meer aandacht voor veilige IT, zonder vanuit de toezichthouders meteen door te slaan in vinkjes- en rapportagedwang. En dat bedrijven die hieraan moeten voldoen actief op zoek gaan naar *beveiliging* in plaats van naar *NIS2-compliancy*.

Gaat nieuwe wetgeving de wereld redden? - Fook Hwa Tan

Veel mensen zullen zich afvragen of aanscherping van de wetgeving cybersecurity op Europees niveau daadwerkelijk zoden aan de dijk zet in deze chaotische tijd van oorlog en pandemie. We hebben gezien hoe belangrijk kleine organisaties kunnen zijn in de hele keten als hun processen tijdelijk of langdurig onderbroken worden. Tekorten op alle vlakken, in alle industrieën zijn ontstaan en onze maatschappij is ontregeld in deze turbulente tijden. Gelukkig nog niet allemaal door cyberaanvallen, maar we zien dit wel langzaam en gestaag toenemen.
Daarom is het belangrijk dat er een visie is op wat beveiliging is. Organisaties zoeken naar richtlijnen en handvatten om informatiebeveiliging te regelen in hun eigen organisatie. Wetgeving kan hier een handje bij helpen. NIS2 is herzien en geeft nu betere handvatten en eist van meerdere sectoren om hieraan te voldoen. Het betekent niet dat als alle sectoren hieraan voldoen onze maatschappij helemaal veilig is, maar het is zeker een stap in de goede richting om informatiebeveiliging in organisaties volwassener te krijgen.
Zoals eerder aangegeven zijn er meer sectoren toegevoegd, die aan deze wetgeving moeten voldoen. De vitale sectoren moesten al eerder aandacht besteden aan hun informatiebeveiliging. Nu moeten andere essentiële sectoren dat ook. Het is steeds minder vrijblijvend, omdat de handhaving geregeld is en gaat worden door bestaande en nieuwe toezichthouders.
Wat deze nieuwe wet ook doet is een lijst met basismaatregelen voorschrijven, waarbij risicomanagement centraal staat bij de keuze van maatregelen. Dat betekent, dat sectoren kunnen nagaan wat als basiscyberhygiëne wordt beschouwd in informatiebeveiliging. Let wel, op basis van de eigen risicoanalyse komt pas echt in beeld welke maatregelen genomen dienen te worden. Beveiliging kan niet alleen geregeld worden door een generieke lijst aan maatregelen.
Kortom, de nieuwe wet betekent niet dat we er zijn met betrekking tot informatiebeveiliging, maar dat we wel worden aangespoord om net weer een extra stap te nemen om de maatschappij iets veiliger te maken!

Zijn wij er met regels opleggen? - Chris de Vries

Ik ben blij met de vervolgstappen gezet door NIS 2 Directive. Oog hebben voor de risico's hoort niet alleen thuis bij de overheid, de vitale sectoren en de groot- c.q. de middenbedrijven met een hoog risicoprofiel. Ook voor de kleinbedrijven geldt dat.
De gedachte is goed, zoals in het verleden de ISO-certificatie (International Organization for Standardization) goed was. Hoe is dát destijds verlopen? Niet altijd op slimme wijze. Toen werd bij sommige organisaties enkel gewerkt aan het beschrijven van bestaande werkwijzen en die tot standaard te verheffen.
In principe kon de standaard dan luiden: 'We doen ons best, fouten worden gemaakt, maar dat is goed, mits wij het maar vastleggen.' Dit is natuurlijk een simplistisch gedachtenspel, de ISO werd een echte norm dankzij de begeleiding van vele, kostbare specialisten. En daar zit hem de kneep. Een nieuwe norm en regel, op hoog directiefniveau genomen, gaat uit van de omvang van de geldbeurzen alsook de beschikbare kennis op dat niveau.
Zo ook bij NIS 2 Directief voor hoog risicoprofiel bedrijven met minder dan 50 werknemers en een omzet niveau beneden de 10 miljoen euro. Dan (boven de 20 werknemers) spreken wij over middenbedrijven, die te groot zijn voor 'het servet en te klein voor het tafellaken'. Om maar niet te spreken over de kleinbedrijven (minder dan 20 werknemers), die zelfs te klein zijn voor het servet.
Het probleem: kunnen deze bedrijven de kennis inhuren tegen redelijke prijs en bezitten zij binnen de eigen geledingen voldoende kennis? Vaak zal het antwoord ontkennend zijn, los of zij zich van hun verantwoordelijkheid en de door hun gelopen risico's (ook in de keten) bewust zijn. Hier ontstaat voor de overheid een plicht om die midden- en kleinbedrijven te helpen om aan de (nieuwe) spelregels te voldoen tegen gematigde kosten, zo niet door kosteloze ondersteuning (denk aan begeleidende adviseurs, standaarden, modellen). Anders ontstaat er weer een nieuwe generatie van kansloze ondernemingen, omdat zij worden uitgesloten van deelname aan het dan exclusieve, maatschappelijke grootbedrijfsleven.

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

COLUMN MARTIJN

De magie van allowlisting

Hoe weet ik dat een bericht echt van jou komt? Het is een vraag waar we al bijna drieduizend jaar mee bezig zijn. Heel vroeger werd er een bolletje gemaakt van klei met speciale symbolen die aangaven waar het bericht vandaan kwam. Een 'bulla'. Was de gebakken klei gebroken, dan wist je dat er iemand de integriteit van de zending misschien had aangetast.

De klei met symbolen kwam daarna op papier, wat we nu nog steeds kennen als een zegel. In die tijd slecht na te maken, dus prima voor authenticatie en zelfs voor een integriteitscheck. Later gebruikten we onze handtekening als authenticatie; ook niet altijd even makkelijk na te maken. Vroeger prima manieren om zeker te weten dat het echt je overleden oom uit Zimbabwe was die je een erfenis had nagelaten. Maar toen vond iemand e-mail uit.

In mijn vorige column omschreef ik drie manieren hoe criminelen binnenkomen: technische kwetsbaarheden, slechte wachtwoorden en phishing. Ik ging in op de eerste twee, die relatief makkelijk opgelost kunnen worden. Die laatste blijkt toch altijd weer een lastige. Of niet?
Eigenlijk lopen we weer tegen hetzelfde probleem aan als met de bolletjes klei, wassen zegels en complexe pentekeningen. Hoe weet ik dat een e-mail echt van jou komt? Uiteraard hebben we hier een overmaat aan technische hulpmiddelen voor.

Als je je domeinnaam correct instelt voor e-mail, stel je ook je SPF, DMARC en DKIM in. Niet veel werk, maar het zorgt ervoor dat een ontvanger kan checken of je e-mail wel verstuurd is vanaf een server die jij hebt goedgekeurd. Deed iedereen dat maar. (Check het! www.internet.nl)
Als je wat verder wil gaan, kun je je wassen zegel ook digitaal krijgen. Met PGP of S/MIME zet je een persoonlijke cryptografische zegel op je mail, en iedereen weet zeker dat het van jou afkomt. Deed iedereen dat maar.

De realiteit is dat je er niet vanuit kun gaan dat mensen zo'n techniek gebruiken, dus vertrouwen we nog steeds alles wat binnenkomt, of het nou een officiële zegel heeft of niet. Er staat een document klaar voor me om te downloaden? Prima! Klik. Dat was het voordeel van die bolletjes klei en wassen zegels, die we een paar honderd jaar gebruikten. De snelheid waarmee IT verandert wacht helaas niet op een awareness-cursus die vier eeuwen duurt.

Maar, ik heb een gouden oplossing. Allowlisting. Het is hoe we de wapenwedloop van input filteren op het web ook ooit wonnen. Vanaf volgende maand maken we een lijst van domeinnamen die we vertrouwen en als je van die domeinen een mailtje krijgt, zetten we er een groen bolletje bij. Hoe maak je die lijst? Kijk maar waar je bedrijf het afgelopen jaar mee heeft gemaild bijvoorbeeld. Komt er een nieuwe domeinnaam bij? Check even (automatisch natuurlijk) of hij heel erg lijkt op iets wat al op je lijst staat (typosquatting), of de domeinnaam pas net bestaat (verdacht), en misschien zelfs of er een website bij die domeinnaam hoort (bij phishing bestaat er soms geen). Ziet het er fout uit? Rood bolletje, iemand even extra laten checken voordat we deze op de allowlist zetten. Opgelost! Extra voordeel, je bent ook niet afhankelijk van anderen die niet snappen hoe PGP werkt.

Natuurlijk zitten er wat haken en ogen aan en bij een e-mailadres-hack, beschermt dit je niet. Maar we zouden er een goede deuk mee kunnen maken! Zoals bij elke vorm van criminaliteit: als wij het lastiger maken is het verdienmodel van de crimineel op den duur kapot.

15 PvIB reconnect in cyber security

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
Nicole van Deursen

REDACTIE
Tom Bakker
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
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, Raalte

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 2022 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

TSTC

ICT en Security Trainingen

ADVANCE YOUR CAREER WITH SECURITY IN 2022

CSA - Certified SOC Analyst
GSEC - Giac Security Essentials
GPEN - Giac Penetration Tester
EDRP - Disaster Recovery Professional
EHF - Ethical Hacking Foundation
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v11
CPENT - Certified Penetration Testing Professional

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 weer klassikaal of Live Online te volgen