15 PvIB reconnect in cyber security

ib
INFORMATIEBEVEILIGING MAGAZINE

Human Capital

- Interview Mark Ruijsendaal (HSD) over tekort aan securityspecialisten: ‘Stop met zoeken naar schaap met de vijf poten’
- Vrijwilligerswerk: Maak van je werk je hobby
- Twee nieuwe columnisten: Martijn Hoogesteger en Dimitri van Zantvliet

JAARGANG 22 - 2022 - EDITIE 2

HOE BESCHERMT U GEVOELIGE INFORMATIE?

ISO 27001 en ISO 27701 helpen u om gevoelige informatie op een gestructureerde manier te beschermen en privacy te waarborgen.

Wilt u uw kennis op het gebied van informatiebeveiliging of privacy vergroten? DNV biedt naast de training normkennis ISO 27001, nu ook de training normkennis ISO 27701 aan. Tijdens deze training leert u welke aanpassingen er nodig zijn om uw ISMS conform de ISO 27701 uit te breiden naar een PIMS. U kunt uw managementsysteem bij DNV in één keer tegen beide normen certificeren met één combinatie-audit. Met als resultaat: twee certificaten waarmee u laat zien dat de privacy en informatiebeveiliging in uw organisatie gewaarborgd is.

Kies DNV als uw partner in certificering en training. Bij DNV staat uw organisatie centraal. Tijdens onze trainingen vormen uw ambities en doelstellingen het middelpunt. Onze trainingen gaan verder dan alleen kennisoverdracht: leren door zelf te doen en zelf te ervaren. Training met impact.

Vind meer informatie over ISO 27001 en ISO 27701 op www.dnv.nl/informatiebeveiliging.

DNV

Mensen

Nicole van Deursen

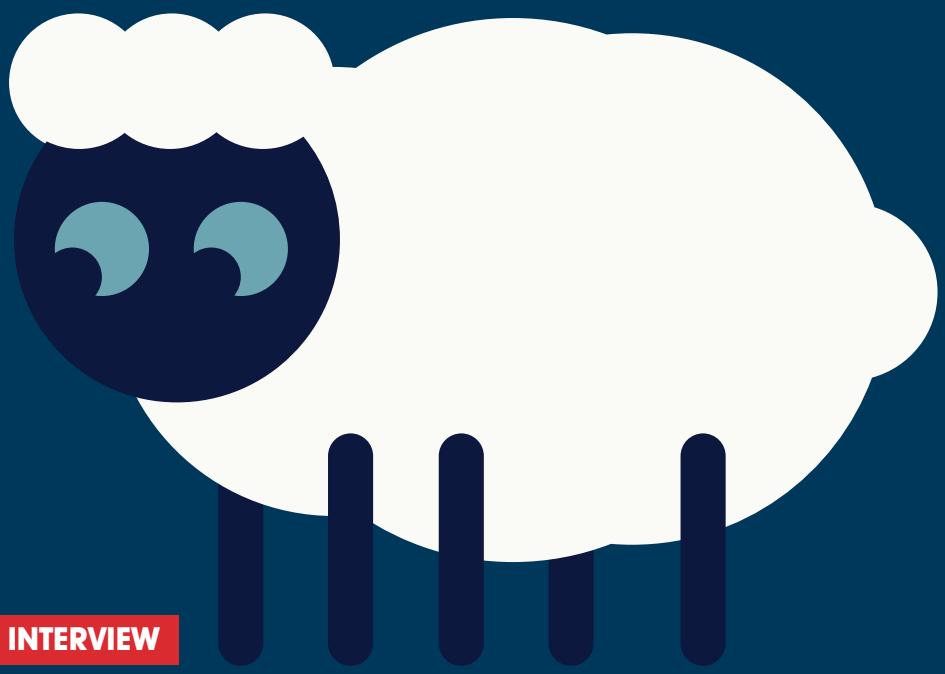
Informatiebeveiliging begint vaak met het identificeren van de 'kroonjuwelen' van de organisatie. Gek genoeg bedoelt men dan de informatie en systemen die het meest belangrijk zijn. Maar informatie en instellingen kun je kopiëren en de kopie kun je (als het goed is) weer terugzetten in systemen die op hun beurt vaak wel vervangbaar zijn. De echte kroonjuwelen van een organisatie zijn wij: mensen. Mensen die uniek zijn, met onze eigen specifieke inzichten en eigenaardigheden. Zonder ons valt alles stil en van ons kun je geen kloon in de kluis leggen als back-up. Dit themanummer gaat over ons. We gaan bijvoorbeeld in op hoe werkgevers naar ons zoeken. Verder kijken we naar de competenties die van ons worden verwacht. Bovendien zijn veel van ons zo gedreven dat we ons ook in onze vrije tijd vol passie inzetten voor een veiliger wereld. Daar hoef je geen superheld voor te zijn, ook kleinschalige initiatieven kunnen enorme impact hebben.

In deze uitgave vind je ook artikelen over bewustwording en gedragsverandering, dat blijft altijd een actueel mensen-thema. Onze vaste rubrieken en columns zijn er natuurlijk ook, uitgebreid met twee fantastische nieuwe columnisten: Dimitri en Martijn. Veel plezier met lezen en vergeet niet dat ook jij artikelen voor ons blad kunt schrijven!

Nicole

IN DIT NUMMER

Auteurs: Nicole van Deursen is redactielid van iB-Magazine. Nicole van Deursen is bereikbaar via nicolevandeursen@pvib.nl. Sandra Kagie is freelance tekstschrijver (Sanscript tekstproducties). Sandra is bereikbaar via info@sanscriptproducties.nl.



INTERVIEW

Tekort aan securityspecialisten

‘Stop met zoeken naar het schaap met de vijf poten’

Cybersecurity specialisten zijn en blijven lastig te vinden. Dat bedrijven en organisaties vacatures op dit vlak moeilijk ingevuld krijgen, heeft echter niet alleen te maken met een tekort aan talenten. Zelf kunnen en móeten bedrijven volgens Mark Ruijsendaal van het nationale veiligheids-cluster Security Delta (HSD) meer doen om mensen te interesseren voor het vakgebied en misschien nog wel belangrijker om de juiste mensen te behouden voor het vak van informatiebeveiliging. “Wanneer ik nu naar de sector als geheel kijk, zie ik vooral een onvolwassen onderwijs- en arbeidsmarkt. Een opgave voor ons allemaal om dit te veranderen”, roept hij op.

Met de term 'onvolwassenheid' doelt programmamanager Ruijsendaal bijvoorbeeld op 'het allegaartje aan eisen' dat hij tegenkomt in vacatureteksten van bedrijven en organisaties die op zoek zijn naar een cybersecurity specialist. "Ik zie irreële eisen en vacaturenamen die alle kanten op vliegen. Dat maakt het vakgebied onaantrekkelijk omdat geïnteresseerden op basis van dit allegaartje geen idee hebben over hun loopbaanpad en ontwikkelmogelijkheden", geeft hij aan.

Realistische vragen en eisen

Structuur en uniformiteit aanbrengen in vacatureteksten door gemeenschappelijk taalgebruik te hanteren, ziet hij dan ook als een belangrijke opgave voor de sector. "Maak hiervoor gebruik van de profielen die er zijn. Zo leg je gezamenlijk een heldere basis voor een ontwikkeling naar volwassenheid van de sector", luidt zijn hartenkreet. Waarbij hij bijvoorbeeld verwijst naar de functieprofielen en competenties zoals deze zijn opgesteld door het PvIB. Ook roept hij ons als beroepsvereniging op organisaties te helpen realistische vragen en eisen te stellen aan een potentiële kandidaat. "Nu zoekt iedereen het schaap met de vijf poten, zo niet acht poten. Een kandidaat moet dertien talen beheersen, drie systemen kennen, sinds zijn dertiende jaar bezig zijn met computers hacken en als persoon over een waslijst aan certificeringen beschikken. Kijk naar wat je vraagt en vraag je af of de eisen realistisch zijn om te vragen van één persoon."

Human Capital Agenda Security

Binnen Security Delta, waarbinnen zo'n 275 bedrijven, overheidsorganisaties en kennisinstellingen samenwerken om het verschil te maken in de veiligheid van onze digitaliserende samenleving, houdt Ruijsendaal zich als senior programmamanager onder meer bezig met de Human Capital Agenda Security (1). Een programma gericht op het aantrekken en ontwikkelen van talent en het oplossen van de mismatch tussen vraag en aanbod als het gaat om (cyber)security talent. En een programma dat Security Delta heeft opgesteld samen met een veertigtal partners voor een periode van vier jaar, 2019-2022.

Dat er na 2022 een nieuwe agenda komt, staat al vast. Het tekort aan security specialisten blijft immers een urgent vraagstuk. Hoe groot het tekort in Nederland echter is, vindt Ruijsendaal lastig aan te geven. Ook dit heeft volgens hem te maken met de 'onvolwassenheid van de sector'. "Het tekort wordt niet goed gemeten en in kaart gebracht", legt hij uit.

De vraag welke functies er nu precies vallen onder de noemer cybersecurity specialist, vindt hij bijvoorbeeld al lastig te beantwoorden. "Systeem- en applicatiebeheerders of een integraal risico manager, zijn dat cybersecurity specialisten?", vraagt hij zich af. Sowieso is het geen beroep dat door het Centraal Bureau voor de Statistiek standaard in kaart wordt gebracht. Reden voor Security Delta om met de Provincie Zuid-Holland een landelijke arbeidsmarktmonitor te maken en om vacatures te analyseren (2).

De talentpool vergroten

Eén van de doelen van Ruijsendaal en zijn collega's voor dit jaar is ervoor te zorgen dat er een nieuwe studie verschijnt met betrekking tot het aanbod en de mismatch op de cybersecurity arbeidsmarkt, zo kondigt hij aan. Een studie die als basis zal gaan dienen voor de nieuwe Human Capital Agenda Security 2023-2026. Daarbij noemt hij voor dit jaar de ontwikkeling van een programma om zij-instromers te interesseren voor het cybersecurity domein als een belangrijke doelstelling (zie cybersecuritywerkt.nl). De huidige aanwas voorziet namelijk niet in de bestaande en verwachte toekomstige vraag naar talent. Door de toenemende awareness voor cybersecurity in zijn algemeenheid zal de vraag naar professionals alleen maar verder toenemen, zo is zijn verwachting.

"Kijkend naar het MKB, denk ik dat de beer nog niet ontwaakt is", geeft Ruijsendaal aan. "Het grote volume in de vraag naar security talent moet in dit segment nog komen. Het gaat hier niet om staatsgeheime informatie die beschermd moet worden, maar toch kunnen succesvolle hacks ook hier grote (economische) impact hebben. Wanneer het ons samen niet lukt om aan de alsmaar toenemende vraag naar security talent te voldoen, zal onze veiligheid verder onder druk komen staan. Daarvan ben ik overtuigd."

Talent behouden

Behalve voor de noodzaak om te werken aan de instroom van nieuw talent, vraagt Ruijsendaal daarom ook nadrukkelijk aandacht voor het behoud van talent binnen het vakgebied. "Ik zie in de praktijk een uitstroom van security professionals in de tweede en derde fase van hun carrière", waarschuwt hij. Ook hier noemt hij het gebrek aan een helder carrière- en ontwikkelperspectief als een van de oorzaken. "Mensen zien geen ontwikkelmogelijkheden meer of voelen zich onvoldoende gewaardeerd en na een aantal jaren van bijvoorbeeld 24/7 ploegendiensten incident management of bij onderbezetting wreekt zich dat in uitval en uitstroom."

“Het grote volume in de vraag naar security talent binnen het MKB moet nog komen: de beer is nog niet ontwaakt.”

Automatisering van cybersecurity, denk aan de toepassing van Artificial Intelligence, ziet hij hier slechts als een deel van de oplossing. “Dit biedt kansen om het werk interessanter te maken”, legt hij uit. “Maar het risico van overbelasting blijft. Er blijft immers op basis van AI zoveel (analyse)werk te doen.”

“Cybersecurity heeft drie kanten: techniek, organisatie en mensen”, gaat hij verder. “Specialisten vanaf hbo-niveau worden vaak geacht op al deze vlakken te acteren. Met als gevolg dat ze ten prooi vallen aan roofbouw.”

‘Denk in teams’

Wat Ruijsendaal betreft moeten organisaties dan ook veel meer in cyberteams gaan denken waarin verschillende functies geclusterd zijn. Teams waarin een cybersecurityprofessional samenwerkt met bijvoorbeeld een risicoanalist, een applicatie-ontwikkelaar, een netwerkbeheerder, een beleidsmaker en een HR-adviseur. Zo creëer je breed draagvlak binnen je organisatie voor security door het onderwerp integraal te benaderen en onderdeel van je bedrijfscultuur te maken. Door de workload te verdelen wordt het werk bovendien behapbaar en daarmee duurzaam aantrekkelijker.

Een tip die Ruijsendaal organisaties vervolgens geeft, is om voor de samenstelling van dit soort integrale teams nadrukkelijk intern te kijken. “Vaak zijn er al medewerkers in alle geledingen die in cybersecurity geïnteresseerd zijn en over de nodigde competenties beschikken. Wanneer je dit verborgen talent vindt, hoef je extern niet meer op zoek en daarbij bied je deze medewerkers nieuw perspectief. Het mes snijdt zo aan twee kanten.”
Blijkt het opzetten van een cyberteam voor een (kleinere) organisatie een brug te ver dan is uitbesteden van je IT-security een optie. “Ook dit vraagt echter de nodige kennis en kunde vanuit het management, inkoop en HR”, stelt hij. “Zij moeten zorgen voor de juiste balans tussen zelf doen en uitbesteden. Waarbij wat Ruijsendaal betreft ontwikkeling van eigen talent, vanuit het oogpunt van draagvlak binnen een organisatie, de voorkeur heeft.

Rol overheid?

Tot slot vragen we de programmamanager van Security Delta of hij in de oplossing van het vraagstuk van het tekort aan securityspecialisten een rol ziet voor de overheid. Die ziet hij zonder meer, maar niet exclusief. Als grootste werkgever vindt hij dat de overheid in de eerste plaats ervaringen moet delen met de private sector. “Hoe zorgt de overheid voor integraal beleid door in alles wat ze doen aandacht te vragen voor cybersecurity, hoe houden zij talent vast en hoe zorgen zij voor ontwikkelperspectief voor hun mensen?”, somt hij op. “Ervaringen waar de private sector van kan leren.”

Vervolgens komt hij op het punt van opleidingen. Cybersecurity zou wat hem betreft veel meer verankerd moeten zijn in allerlei opleidingen. Niet alleen in IT-opleidingen, maar juist veel breder. Hij noemt het voorbeeld van het ROC Mondriaan in Den Haag dat met specifieke modules niet alleen binnen IT-opleidingen, maar juist ook binnen niet-technische studies, denk aan zorgopleidingen, aandacht besteed aan het onderwerp. Modules die ook beschikbaar zijn voor andere ROC’s. Dit alles om breder competenties te ontwikkelen. Iets waar wat Ruijsendaal betreft vanuit de overheid, ook op hbo- en wo-niveau, meer op gestuurd zou moeten worden in het kader van het maatschappelijk belang van opleidingen. Iets dat hij nu mist. “Onderwijs, bedrijfsleven en organisaties zoals HSD en PvIB moeten het samen met de overheid doen.”

Referenties

(1) https://securitydelta.nl/media/com_hsd/report/231/document/HSD-Human-Capital-Agenda-Security-Webversie.pdf
(2) Securitytalent.nl https://securitytalent.nl/career/dashboard

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Het kopie ID is hoogbejaard

Gelukkig hoef ik niet zo heel vaak meer te vertellen dat een kopie van je paspoort of ander identiteitsdocument een kroonjuweel is dat je niet zomaar moet afstaan. Onlangs deelde de Autoriteit Persoonsgegevens nog een forse boete uit aan DPG Media. Zij vroegen aan iedereen die een inzage- of wijzigingsverzoek deed standaard om een kopie van het ID. Dat vond de toezichthouder te veel van het goede en legde een boete op van 525.000 euro.

Voor de AVG was het gemeengoed dat overal om het kopie ID gevraagd werd bij het uitoefenen van bovenstaande rechten. Maar ook toen had het kopietje eigenlijk al zijn langste tijd gehad. Veel hackers waarschuwden voor het gevaar van rondslingerende (veelal digitale) kopieën. Zo liet Jeroen van Beek al zo'n tien jaar geleden zien dat mensen kopietjes onveilig verzenden en onveilig opslaan – hij zocht simpelweg via filesharing netwerken naar termen als 'paspoort' en 'wachtwoord' en vond in een mum van tijd een schat aan informatie. In 2014 schreef Tokmetzis daar al eens een mooi artikel over voor De Correspondent.

De AP houdt aan die lijn vast en stelt in haar boetebesluit: 'Het is onevenredig om een kopie van een identiteitsbewijs te vereisen als de identiteit van de betrokkene op een andere manier kan worden geverifieerd. Bovendien vormt de verwerking van kopieën van identiteitsbewijzen een groot risico voor de veiligheid van persoonsgegevens.'

DPG-media bood personen de mogelijkheid om zich via een onlineaccount te verifiëren, maar dat vond de toezichthouder niet afdoende. Daarmee wordt een extra belemmering opgelegd aan personen om hun rechten uit te oefenen. Het besluit wijst in de richting van verificatie aan de hand van gegevens die de verwerkingsverantwoordelijke al heeft. Denk daarbij aan het albekende riedeltje van de doktersassistent die als je belt altijd vraagt naar geboortedatum en achternaam. Waarbij de AP nog wel aangeeft dat bij twijfel, in een uitzonderingsgeval gevraagd kan worden om een afgeschermde kopie waarbij ten minste het BSN onleesbaar is gemaakt.

Het zal de nodige kopzorgen gaan opleveren voor verantwoordelijken. Je wilt immers niet ten onrechte een grote hoeveelheid persoonsgegevens aan de verkeerde persoon geven – ook daar ligt het gevaar voor (identiteits)fraude op de loer. En een enkele geboortedatum en achternaam liggen ook niet in de rede. Ik kan alleen in mijn omgeving al zeker twintig mensen opnoemen die zonder enige moeite deze gegevens kunnen oplepelen. Laat staan dat iemand die kwaad wil, met een kleine zoektocht langs sociale media ('Gefeliciteerd met je 30ste verjaardag Rachel!') al snel de benodigde gegevens kan vinden. En ik denk dat hier precies de zwakte zit van het besluit van AP.

Als het gaat om persoonsgegevens, kun je niet experimenteren omdat de mogelijk negatieve gevolgen te groot zijn. En hoezeer ik het ook met AP eens ben – dat kopietje heeft echt zijn langste tijd gehad-, zal het nog best een klus zijn om de juiste balans te vinden omdat zogezegd aan beide kanten van het spectrum voor personen hetzelfde gevaar op de loer ligt.

Rachel

Auteurs: Rik van Dijk en Nicole van Deursen zijn onderzoekers bij het NCSC en zijn bereikbaar via research@ncsc.nl.

Tekort op de arbeidsmarkt: vele oplossingen voor een onduidelijk probleem

Je hoort vaak dat er een tekort is aan goede securityspecialisten. Zo meldt het (ISC)[2] in de 2021 Workforce Study dat er alleen al in Nederland 22.000 vacatures zijn. De oplossing wordt vaak gezocht in het opstellen van beroepsprofielen en het ontwikkelen van opleidingen en trainingen. Hoe helpen competentieprofielen om vacatures te vervullen? Moeten werkgevers en opleiders zich vastpinnen op die profielen? Is het verstandig dat werkgevers zoeken naar werknemers met een lijst certificaten op hun LinkedInprofiel? En waaraan precies hebben we eigenlijk een tekort?

De Cyber Security Skills Shortage is een onderwerp waar de afgelopen jaren over is gesproken en geschreven. Het overheersende idee is dat het ontbreekt aan bekwame specialisten die Nederland kunnen verdedigen tegen het snel toenemende aantal digitale aanvallen. Ook over de grens wordt het ontbreken van geschikte specialisten gezien als een groot probleem. Uit onderzoek van het International Information System Security Certification Consortium (ISC)² een bekend opleidingsinstituut dat onder andere de populaire CISSP training aanbiedt, ziet 63% van hun respondenten dat er een personeelstekort is (1).

Opleidingen

Onderwijsinstellingen spreken vaak met werkgevers over de inhoud van opleidingen en bieden zo wellicht aanknopingspunten om te reflecteren welke behoeftes er zijn op de arbeidsmarkt. Zo dacht ook ENISA die in november 2021 een rapport publiceerde over de kloof in de Europese Unie tussen de vraag naar revelante cybersecurityvaardigheden en het huidige aanbod van deze vaardigheden (2). Daarin laat ENISA zien dat de huidige studies ruimschoots technische vaardigheden aan studenten aanbieden. Gemiddeld gaat bijna 50% van de studiepunten naar technische vakken, gevolgd door een categorie overig, waar onder andere onderzoeksvaardigheden onder vallen. Op de derde plek staat de categorie organizational, risk management, business compliance met 12% van het aanbod. Daarmee zou je zeggen dat het huidige aanbod van studies en met een focus op technische vaardigheden, we hard op weg zijn het gat te dichten? Alleen wat ook weer ontbreekt in het rapport is een duidelijke omschrijving waar precies de vaardighedenkloof in de EU uit bestaat.
De jaarlijkse (ISC)² Workforce Study biedt meer houvast. Volgens dit onderzoek zijn de meest gevraagde kennisgebieden:

- Cloud Security (40%);
- Risk assessment, analysis and management (26%);
- Artificial intelligence/machine learning (25%);
- Governance, risk management and compliance (GRC) (24%);
- Threat intelligence analysis (22%).

Kijken we naar het aanbod van de cybersecuritystudies dan zien we hier dus een mismatch ontstaan. Het meest gevraagde kennisgebied, cloudsecurity, is pas sinds een aantal jaar sterk in opkomst. De kennisgebieden risicomanagement en governance raken sterk aan economische en bestuurskundige studies, niet aan technische opleidingen. Zelfs threat analysis bestaat voor grote delen uit niet-technisch gerelateerde onderwerpen, zoals internationale betrekkingen en militaire studies. De meest gevraagde kennisgebieden uit de (ISC)² studie en uit analyses van vacatures (3) genereren het beeld dat een cybersecurity expert dus een soort alleskunner moet zijn.

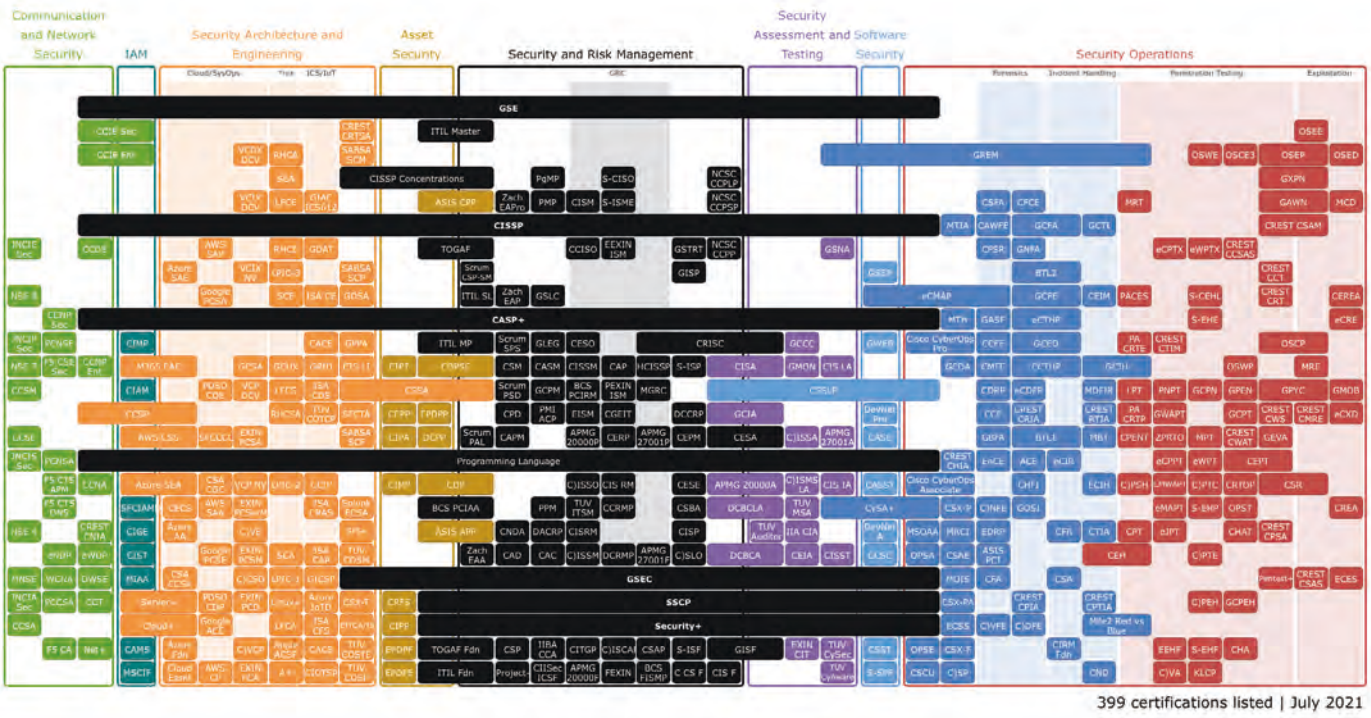
Certificeringen

Hoe moeten we dat soort diamanten dan vinden? Veel organisaties grijpen naar certificering als een proeve van bekwaamheid. Om een CISSP of CISM certificering te dragen moet je vijf jaar ervaring hebben. De certificeringen behandelen onderwerpen uiteenlopend van het Lapadula-Bell model (Don't Read Up!) tot aan Kernel Security. Alleen, het hoofdstuk Cloud Security, volgens (ISC)² het meest gevraagde kennisdeel door werkgevers, is net drie pagina's lang. Onderwerpen als Threat Intelligence Analysis of AI worden omschreven maar het hoe en wat blijft achterwege. Toch geldt CISSP vaak als harde eis om een baan in het vakgebied te vinden. De focus van werkgevers op CISSP is opmerkelijk: er zijn honderden mogelijke certificeringen, waardoor er voor iedereen wel mogelijkheden zijn om relevante kennis op te bouwen. Voor verzamelaars van certificaten hebben we het overzicht van Paul Jerimy bijgevoegd, hij heeft inmiddels 399 mogelijke certificeringen in kaart gebracht, zie afbeelding 1 op pagina 10.

Toch gaan er veel stemmen op voor certificeringen van professionals. Iedereen kan zich informatiebeveiligings- of cybersecurityprofessional noemen, dus een erkende vorm van bewijs kan wel helpen om charlatans in je organisatie te vermijden. In het Verenigd Koninkrijk is recentelijk een publieke consultatie gestart (4) over de behoefte aan helderheid van professionele standaarden en carrièrepaden, zoals we die kennen voor accounting of juridische beroepen. Met de antwoorden hopen ze meer inzicht te krijgen in de beroepsgroep.

Competentieprofielen

Certificeringen, opleidingen en competentieprofielen gaan hand in hand. Omdat er van alles en nog wat lijkt te vallen onder de noemer 'cybersecurity' kunnen we tientallen uiteenlopende profielen vinden. Alleen al het NICE framework van de US National Institute of Standards and Technology (NIST) telt 52 functies over 33 specialistische werkvelden (5). Het vakgebied is breed en een multidisciplinair samenspel van diverse beroepen. Dit zie je bijvoorbeeld ook terug in de mogelijke carrièrepaden, waar een IT-opleiding al lang geen vereiste meer is om aan de slag te gaan. Carrièrepaden zijn hierdoor



Afbeelding 1 - Een overzicht van certificeringen. Bron: https://pauljerimy.com/security-certification-roadmap/.

geen vaste routes en het van tevoren kiezen van de 'juiste' opleiding voor je carrière is een lastige opgave. We vragen ons af of we niet te veel proberen om allerlei taken en rollen in hokjes te stoppen? Of is het juist een teken van groeiende volwassenheid van het vak?

Het QIS framework van het PvIB (6) is een goede start voor organisaties om voor zichzelf in kaart te brengen wat ze echt nodig hebben. Het is echter niet helemaal toereikend voor een multidisciplinair team waarin je bijvoorbeeld ook incident response doet of OT-beveiliging. De profielen beschrijven bijvoorbeeld wel functies die plannen maken voor incident management, maar er staat geen profiel in voor de mensen die daadwerkelijk de incidenten onderzoeken en oplossen. Kaders beschreven door andere organisaties kunnen dat aanvullen, hoewel die soms weer naar heel veel detail doorslaan. De beschrijvingen verschillen sterk in aantal functies per werkveld en diepte waarin functies worden uitgeschreven. Het NICE framework is bijzonder uitgebreid en gedetailleerd en geeft ook carrièrepaden weer. Commerciële partijen zoals SANS bieden ook diensten aan om te helpen bij het beschrijven van gewenste teamrollen en (uiteraard) de bijbehorende (dure) GIAC certificeringen (7).

Vaardigheden versus inhoudelijke kennis

Recruiteren op wat mensen al inhoudelijk weten kan helpen om enkele plekken te vullen op korte termijn. Voor de lange termijn moeten werkgevers ook inzetten op het om- en bijscholen van mensen en het werven op vaardigheden in plaats van kennis. Dit is een aanpak van lange adem, maar wel op termijn een duurzame: je houdt de mensen enthousiaster, up-to-date en hopelijk langer in dienst. Dit heeft ook gevolgen voor hoe opleidingen in elkaar zitten: het ontwikkelen van analytisch denken, problemen oplossen en hoe je zelfmanagement doet, vraagt om specifieke lesmethoden. Reflecterend op de huidige staat van opleidingen en certificeringen zien we een enorme focus op (technische) kennisopbouw, waarbij we proberen te komen tot een soort holistische cybersecurity expert die zowel kan pentesten, de pentestresultaten duidelijk aan het management kan uitleggen, geopolitieke dreigingen kan duiden, verschillende risicomanagementmethoden kan toepassen en ook de organisatiestructuur goed neerlegt. Het is toch of je aan een Europees Recht expert vraagt de verdediging van je moordzaak op zich te nemen: hoogstwaarschijnlijk een slecht idee.

Naam	Werkveld	Aantal beschreven profielen	Bron
PvIB QIS	Informatiebeveiliging	6	(6)
Security Delta	Safety & Security	48	(10)
CSA Singapore	OT security	15	(9)
NICCS – CISA (NICE)	Cybersecurity	52	(11)
SANS GIAS certificeringen	Cybersecurity	43	(12)
EN16234-1:2019 e-Competence Framework (e-CF).	ICT	42 ICT profielen, waarvan 2 informatiebeveiliging	(13)

Tabel 1 - Overzicht van enkele bronnen voor competentieprofielen.

Bijkomend probleem is dat ons vak niet is losgezongen van de sectoren, domeinen en organisaties die digitale beveiliging nodig hebben. De noodzaak tot domeinkennis is misschien het meest evident in het Operational Technology (OT) Security gebied. Een onderzoek uitgevoerd door Secura in opdracht van het NCSC (9) toont aan organisaties met OT-netwerken het meest waarde hechten aan domeinkennis, bijvoorbeeld het begrijpen van de processen en risico's rondom sluizen in de watersectoren, de werking van chemische processen in de olie en chemie sector. Uit het onderzoek blijkt dat het begrijpen van operationele risico's en deze kunnen vertalen naar bedrijfsafwegingen waardevoller is dan pure technische kennis.

Ook een uitgebreid onderzoek van de Cyber Security Agency (CSA) van Singapore (10) naar OT-securityrollen laat zien dat technische kennis over bijvoorbeeld cryptografie en netwerk security wenselijk is. Echter, net zo belangrijk is dat de medewerker probleemoplossend kan denken, goed kan communiceren, buiten zijn of haar comfortzone moeten kunnen stappen en over analytisch vermogen beschikt. Kortgezegd blijkt uit zowel het Secura onderzoek als die van CSA dat een focus op puur technische verworvenheden niet leidt tot de meest geschikte expert.
Een focus op certificeringen en technische vaardigheden verhoogt daarnaast de drempel voor mogelijk nieuwe medewerkers uit andere vakgebieden. Hiermee krijgt gemotiveerd talent moeilijk voet aan de grond omdat ze een certificering missen, terwijl ze deze kennis on the job net zo goed opdoen. Het omgekeerde is ook waar. Zwaar overgekwalificeerde specialisten met meerdere certificeringen en een studie op zak, worden aan het werk gezet als generalisten. Iemand die malware analyse heeft gestudeerd, meerdere certificeringen over het onderwerp heeft gehaald, wordt hoogstwaarschijnlijk niet gemotiveerd om aan een bestuur zonder enige cybersecurity kennis te moeten pleiten voor een hoger securitybudget.

Hoe moet het verder?

Het gebrek aan duiding van het uiteenlopende probleem 'tekort aan cybersecurity mensen' heeft ook tot gevolg dat voorgestelde oplossingen veelsoortig zijn. De verschillende bronnen voor dit artikel geven een aantal richtingen. Bijvoorbeeld ENISA suggereert drie type algemene acties die een overheid kan nemen om de tekorten aan te pakken:

- Kennis en awareness verbeteren in de samenleving, zowel in basis onderwijs als in voortgezet onderwijs;
- Verbeteren van opleidingen in hoger onderwijs en studenten stimuleren om in cybersecurity te gaan werken;
- Organiseren van cybersecurity oefeningen en challenges om jong talent te laten oefenen.

Competentieprofielen kunnen hierbij een houvast geven, maar gebruik ze vooral ter inspiratie voor je eigen functiehuis binnen je specifieke domein.

(ISC)[2] stelde de vraag aan professionals, die zeggen:

- Leg de nadruk op ontwikkelen en behoud van de mensen die je al hebt;
- Neem initiatieven voor recruitment en aanmoedigen van toekomstige medewerkers;
- Investeer in AI/ML en overige automatisering van processen.

Wij dragen graag bij aan de hoeveelheid mogelijke oplossingen en voegen er nog drie toe voor organisaties:

- Organiseer je organisatie. Inventariseer concreet wat je nu echt nodig hebt en stapel niet verschillende behoeftes op. Werf dus niet voor één persoon die eigenlijk acht vacatures tegelijk moet kunnen vullen, maar wees redelijk en splits zware functies op. Zo creëer je ook plek voor MBO'ers. Competentieprofielen kunnen hierbij een houvast geven, maar gebruik ze vooral ter inspiratie voor je eigen functiehuis binnen je specifieke domein. Blijf ruimte houden voor mensen om hun eigen ontwikkelpad te volgen. Kijk ook eens over de grenzen van je eigen afdeling. Misschien zijn er mensen met talent die gemotiveerd zijn om voor een paar uur per week security taken op te pakken.
- Straal uit dat het leuk is! Werken in dit vak is belangrijk, uitdagend, dynamisch, spannend en maatschappelijk relevant. Vertel het dus door. Ga regelmatig in gesprek met studenten en docenten in MBO en hoger onderwijs om een realistische kijk in de keuken te geven. Denk daarbij ook aan andere opleidingen dan ICT. Communicatie, data science, rechten, accountancy, economie, psychologie en zelfs geschiedenis zijn allemaal richtingen die waardevol kunnen blijken bij het opstellen van beleid, risicoscenario's, awareness programma's, threat intelligence, of het analyseren van oorzaken van incidenten.
- Train je recruiters. Voor specialistische vacatures is het verstandig dat recruiters enigszins bekend zijn met terminologie en specifieke opleidingen. Een goed geschreven vacaturetekst nodigt uit te solliciteren. Zorg ook dat de eisen redelijk zijn. Zoek je een azure cloud security specialist? Vraag dan niet om een generieke certificering. Zoek je een junior? Vraag dan niet om een dure certificering die je pas mag voeren na vijf jaar werkervaring. Zoek je een senior? Dan is vijf jaar ervaring misschien echt nog niet genoeg.

Referenties

(1) https://www.isc2.org/Research/Workforce-Study
(2) https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education
(3 N. van Deursen. Wie is de meest gezochte informatiebeveiliger? iB-Magazine 4, 2018
(4) https://www.gov.uk/government/consultations/embedding-standards-and-pathways-across-the-cyber-profession-by-2025/embedding-standards-and-pathways-across-the-cyber-profession-by-2025#introduction
(5) https://niccs.cisa.gov/workforce-development/cyber-career-pathways
(6) https://www.pvib.nl/actueel/nieuws/whitepaper-beroepsprofielen-informatiebeveiliging
(7) https://www.giac.org/workforce-development/job-descriptions/
(8) https://www.ncsc.nl/onderzoek/onderzoeksresultaten/iacs-competenties
(9) https://www.csa.gov.sg/News/Publications/operational-technology-cybersecurity-competency-framework-(otccf)
(10) https://securitytalent.nl/career/career-navigator-in-safety-security
(11 https://niccs.cisa.gov/workforce-development/cyber-career-pathways?community=cybersecurity
(12) https://www.giac.org/certifications/
(13) https://ecfexplorer.itprofessionalism.org/

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

COLUMN DIMITRI

The Great Cyber Resignation

Nu we een paar jaar in de covidlockdown zitten, wordt het tijd om eens goed na te denken over de retentie van cybercollega's. Het was - en is een complexe periode met een verhoogde waarschijnlijkheid op stress, levensbedreigende situaties en financiële zorgen. Deze life changing experiences maken dat medewerkers anders in de wedstrijd kunnen komen te zitten of zelfs anders in het leven staan. De markt die toch al extreem schaars was, wordt nu dus ook nog eens zeer volatiel. Dit post-pandemisch paradigma is enerzijds een risico en anderzijds een kans!

The Great Resignation wordt in vakbladen een soort medewerkers revolutie genoemd. Veel persoonlijke omstandigheden zijn door corona veroorzaakt en worden soms gevoelsmatig versterkt door de reacties van overheden en werkgevers. Het kan natuurlijk ook samenvallen met de lastige financiële- of operationele situatie waarin een organisatie ineens verkeert en hierdoor gestapelde stress veroorzaken. Burn-out en depressie worden genoemd als de volgende pandemie omdat het ecosysteem van work-life balance verstoord is.
Cyberfatigue is een bekend fenomeen. Het asymmetrische gevecht tussen kat en muis maakt dat we soms de moed verliezen. In ons vakgebied hebben we ons daarnaast extra hard mogen inspannen om versneld naar de cloud te gaan, thuiswerken te faciliteren, mobiel werken te omarmen, extra awareness campagnes uit te rollen en de tsunami aan nieuwe aanvalsvormen te pareren. Werkgevers dienen hier rekenschap van te geven en deze inspanning te erkennen. Ik vrees echter dat het tegenovergestelde vaak het geval is.
Medewerkers die overwegen te vertrekken hebben een verhoogd risicoprofiel. In het algemeen kunnen ze slordiger worden. Boze werknemers kunnen gevoelige informatie meenemen naar de concurrent of zelfs ondermijnende activiteiten ondernemen door bewust wél op linkjes te klikken. Insider Threats zijn de komende jaren daarom echt een stuk reëler. Data Loss Prevention, XDR en Anomalie Detectie kunnen technische hulpmiddelen zijn om vreemd gedrag te pareren. Een continue dialoog tijdens een rondje wandelen om dit gedrag te voorkomen.
Recent gepubliceerd onderzoek van $(ISC)^2$ geeft aan dat er wereldwijd minstens 2,7 miljoen cybervacatures zijn. Medewerkers (van de concurrent) die overwegen te vertrekken kunnen door de pandemie openstaan om nu de overstap te maken. Ik denk persoonlijk dat sociaal maatschappelijk relevante organisaties daarom wellicht meer kans hebben cyberspecialisten aan zich te binden. Geld is immers niet zaligmakend gebleken. Maak die 'WHY' dan ook nadrukkelijk onderdeel van de werving.
Talent mag ook ontwikkeld worden. Een universitaire opleiding plus cissp, cism, cisa, etc. én tien jaar ervaring zijn als een speld in een hooiberg te vinden. Een arbeidsmarkt-toeslag helpt als instrument om met de commerciële arbeidsmarkt te kunnen concurreren maar nog meer kansen zie ik gelegen in jong talent. Ik bedoel jong qua cyberervaring. Kijk dus niet enkel naar de nog op te leiden generatie jongelingen maar ook naar de ervaren workforce die omgeschoold wil worden. Laat medewerkers zich ontwikkelen, laat ze spreken op podia en meeschrijven aan publicaties. "Maar wat als ik ze heb opgeleid en ze gaan weg?" Wat als je ze niet laat ontwikkelen en ze blijven?
Het vasthouden aan het beheersen van de Nederlandse taal helpt ook niet om de skills-gap te dichten. Cybertoptalent wil graag komen wonen en werken in ons land en we moeten echt af van het Algemeen Beschaafd Nederlands-dogma, zeker in IT- en cybersecurityfuncties.
Mocht die topper, uiteindelijk toch besluiten ergens anders het geluk te beproeven neem dan altijd goed afscheid en zorg voor een warme referentie. Onderhoud contact en neem na een tijdje contact op om te vragen of ze het naar hun zin hebben. Misschien willen ze, nieuwe ervaring en kennis rijker, binnenkort wel terugkomen!

Auteur: Sander Krijntjes is Sales Manager bij Cqure en is gespecialiseerd in het helpen van organisaties met recruitment van cybersecurityspecialisten. Hij is te bereiken via sander.krijntjes@cqure.nl of 06 12 89 87 53.

Recruitment awareness

Organisaties hebben genoeg uitdagingen op het gebied van cybersecurity. Naast het beschermen van gevoelige data en het continu verbeteren van de algehele informatiebeveiliging, ligt er ook een grote uitdaging op het gebied van het werven van zowel interne als externe cybersecurity en privacyprofessionals.

Mede door het grote aantal serieuze incidenten en het feit dat niet alleen de omvangrijke, gerenommeerde organisaties een target zijn tegenwoordig, komt informatiebeveiliging steeds hoger op de agenda te staan. Een logisch gevolg hiervan is dat er vaker en meer budget wordt vrijgemaakt voor het aannemen of inhuren van cybersecurity professionals. Hier blijkt dan ook weer een grote uitdaging te liggen.

Zoeken en vinden

Cqure zet zich al ruim dertien jaar in om bedrijven te helpen met onder andere de werving van permanente en tijdelijke cybersecurity professionals. Oprichter Dennis Nuijens geeft aan: "Wij gaan al een tijdje mee maar we hebben de huidige schaarste nog niet eerder meegemaakt. Dit komt doordat de 'bad guys' meer slachtoffers maken door automatisering en ontwikkeling, dan de groei van het aantal professionals die ze bestrijden aankan. Het 'spel' van recruitment in cybersecurity is hierdoor aan het veranderen en wij helpen onze opdrachtgevers om zich zodanig aan te passen dat ze hier hun voordeel mee kunnen doen."
De vraag is het laatste jaar enorm toegenomen en het aanbod is nagenoeg gelijk gebleven. Het zoeken en vooral vinden van de juiste mensen, die ook nog open staan voor een gesprek, is hierdoor een stuk lastiger geworden vergeleken met een aantal

jaren geleden. Daarbij komt ook nog eens dat de kandidaten veelal met meerdere partijen tegelijk in gesprek zijn. Geef ze eens ongelijk! De wereld ligt aan hun voeten….

Ik heb als recruiter goed overzicht van de markt, aangezien ik veel verschillende organisaties spreek (van start-up tot enterprise en alles daar tussenin) over hun wervingsproces. Wij merken dat sommige vacatures soms al maanden open staan. Het antwoord dat wij het meest horen als wij vragen waarom de vacature nog niet is ingevuld, is dat de potentiële nieuwe collega ergens anders heeft getekend. Of dat zij toch intern bij de huidige werkgever een stap hebben gemaakt en dus is ingegaan op een voorstel met betere arbeidsvoorwaarden van de huidige werkgever, die hem/haar niet kwijt wil.

Sollicitatieproces stroomlijnen

Goede 'recruitment awareness' kan erg goed helpen om toch de juiste cybersecurityspecialisten aan je te kunnen binden. Wees bewust van het proces en wat dit betekent voor een sollicitant en probeer het proces in te richten op de behoefte van de sollicitant. Bij Cqure zie ik het als mijn taak om deze awareness te creëren bij onze opdrachtgevers. Ik stel verschillende verbeteringen voor. Deze leveren soms best moeilijke managementbeslissingen op. Bij cybersecurityprojecten wordt er ook veel weerstand ondervonden, bijvoorbeeld door de extra kosten gecombineerd met de functionele beperkingen. Bij het creëren van recruitment awareness ondervind ik hetzelfde, maar toch merk ik dat onze opdrachtgevers die zich hierin kunnen aanpassen een duidelijk voordeel hebben en daardoor meer succes.

Wij adviseren onze opdrachtgevers om hun sollicitatieproces zoveel mogelijk te stroomlijnen. Er zijn voorbeelden van bedrijven die hierdoor het hele proces zelfs in twee dagen afronden, iets dat een enorm concurrentievoordeel biedt. Dit is voor veel organisaties niet haalbaar, maar als het proces lang duurt is de kans aanzienlijk dat de beoogde kandidaat ergens anders tekent. En dat is zonde van iedereen zijn tijd, geld en resources.

Het veranderen (of eigenlijk het verkorten) van het sollicitatieproces is niet zomaar gedaan. Vooral voor de meer seniorfuncties wordt er over het algemeen met veel verschillende stakeholders binnen de organisatie gesproken. Iedereen is druk, en regelmatig worden gesprekken gepland die ruim een week of zelfs twee weken later plaatsvinden. Dit is vaak funest.

Een mooi voorbeeld is dat een van onze opdrachtgevers haar proces volledig heeft veranderd na onze adviezen. Het gaat hier om een snel groeiende tech scale-up in Amsterdam met ongeveer 750 medewerkers, die op zoek waren naar een interne senior security specialist. Twee kandidaten hadden ieder zeven (!) gesprekken op één dag, waaronder met de CTO en Lead Development. Daarvoor hadden ze al gesproken met de key-stakeholder, de CISO. De dag na de gesprekken kreeg een van de kandidaten een aanbod en was het direct geregeld!

Het versnellen van het sollicitatieproces is makkelijker gezegd dan gedaan en zal niet binnen een week helemaal omgegooid kunnen worden. Maar het is absoluut de moeite waard om er eens kritisch naar te kijken.

Vijf tips om sollicitatieproces te versnellen

1. Creëer 'recruitment awareness' binnen de organisatie, vooral bij de belangrijkste stakeholders voor de desbetreffende functie zoals bijvoorbeeld de inhurende manager;
2. Plan meerdere gesprekken voor dezelfde kandidaat op één dag in;
3. Zet eventuele vervolggesprekken met potlood alvast in de agenda's kort na de uitnodiging voor een eerste gesprek;
4. Zorg dat er bij interesse na het laatste gesprek snel een aanbod wordt gedaan;
5. Zorg samen met het recruitment bureau ervoor dat duidelijk is wat de kandidaat een aantrekkelijk aanbod zou vinden en wat hij/zij daarbij belangrijk vindt.

Mijn advies is om na het lezen van dit artikel eens na te denken hoe het sollicitatieproces er nu uitziet in jouw organisatie. Het zou voor iedere organisatie mogelijk moeten zijn om een proces van begin tot eind binnen twee tot tien dagen te voltooien. Is dat nog niet het geval? Dan is het mijn advies om daaraan te werken.

Het werven van mensen binnen het domein van Cybersecurity & Privacy is aan het veranderen, zorg ervoor dat je interne organisatie mee veranderd om niet achterop te raken en achter het net te vissen!

Auteur: Bas Schiltmans is Chief Technology Officer (CTO) van KCM Group. Hij is van huis uit bedrijfskundige en heeft enkele decennia ervaring in vele functies binnen ICT-omgevingen. Bas Schiltmans is bereikbaar onder: welcome@kcmgroup.eu.

Medewerkersbewustzijn is meer dan een training

Veel organisaties steken een groot deel van hun inspanningen om veiliger te werken in zaken als techniek en formele organisatie. Belangrijk, maar al deze inspanningen zijn echter van beperkte waarde als medewerkers niet in staat zijn op een veilige manier om te gaan met (ICT-)hulpmiddelen die ze daarin ondersteunen.

Een veilige manier zou bijvoorbeeld kunnen zijn: vergaande technische anti-phishingmaatregelen met sluitende formele procedures hoe je moet handelen wanneer je zo'n phishing e-mail ontvangt. Als er toch een mail door het technisch net slipt en bij een medewerker terechtkomt die niet weet hoe hiermee om te gaan, is er een grote kans op een veiligheidsincident.
Er ligt dus een grote uitdaging voor organisaties om ervoor te zorgen dat medewerkers qua kennis en gedrag opgewassen zijn tegen de bedreigingen die op ze afkomen op het gebied van veilig werken met gegevens. Veel organisaties doen nog helemaal niets aan medewerkersbewustzijn, andere organisaties grijpen voor het initieel op peil brengen van het bewustzijn instinctief vaak naar trainingsmiddelen als e-learning. Een eenmalige training met een toets die bewijst dat mensen weten wat ze moeten doen. Soms worden deze trainingen en toetsen periodiek herhaald om de kennis beter te laten beklijven, maar dit gebeurt dan meestal niet heel vaak en met relatief lange tussenpozen.
Wanneer je het 10-20-70 model (1) toepast, wordt duidelijk dat alleen formeel leren niet de benodigde langetermijneffecten zal hebben om kennis en gedrag continu te verbeteren. Tenminste 70% van het leren vindt volgens dit model immers plaats buiten formele leeromgevingen. Slechts 10% in de formele leeromgeving, dus e-learning.

De vergeetcurve van Ebbinghaus (2) maakt ook duidelijk dat eenmalig trainen met eventuele periodieke herhaling met wat langere tussenpozen niet voldoende is om praktisch kennis en gedrag van medewerkers structureel te verbeteren. Mensen vergeten dingen die ze in dit soort formele training geleerd hebben heel erg snel. Een keer per kwartaal herhalen en toetsen is dus eigenlijk veel te weinig, als je dit beschouwt.
Wanneer dan ook nog de implicaties van de zaken die door neurowetenschapper Erik Schoppen zijn aangedragen in zijn publicatie in iB-Magazine uit 2019 (3), blijkt nog duidelijker dat alleen formeel trainen echt onvoldoende is. Uit zijn betoog volgt onder andere dat gedragsverandering continue aandacht en herhaling vereisen. Mensen reageren met het primaire deel van hun hersenen – het zgn. reptielenbrein – op veiligheidsdreigingen en vragen om informatie. Het aanpassen van dit primaire gedrag is bijzonder lastig. Wat we leren in het rationele deel van ons brein passen we maar moeilijk toe in situaties waarin het primaire deel klakkeloos reageert. Om gedrag te veranderen is continue aandacht en oefening nodig. Dit benadrukt hoe belangrijk het is om meer te doen dan een 'standaard' training. Idealiter zouden we ervoor moeten zorgen dat primaire reacties veranderen. Op zijn minst willen we een situatie creëren waarin herkenning optreedt van situaties waarin de primaire reacties tot verkeerde resultaten leiden. We willen dan een bewustwordingsmoment creëren bij de medewerker om de ratio aan te kunnen spreken. Dit is een intensief proces waarin het in elk geval heel belangrijk is om met zo groot mogelijke regelmaat het onderwerp onder de aandacht van de medewerker te brengen en zo mogelijk te oefenen. Al met al een onmogelijke opgave om de zogenaamde human firewall van je organisatie op peil te brengen en te houden met alleen af en toe eens trainen.

Bewustzijnsverbetering

Wat zou je als organisatie kunnen doen om bewustzijn, kennis en gedrag te vergroten op het gebied van veilig werken met gegevens? Relevante kennis beschikbaar stellen aan je medewerkers is belangrijk. E-learning is en blijft hierbij een heel belangrijk startpunt maar voor echte bewustzijnsverbetering is meer nodig.

Hierbij een aantal uitgangspunten:

- De kennis moet begrijpelijk zijn. Soms wordt de fout gemaakt strikt formele procedures en instructies uit bijvoorbeeld een ISMS zonder filter aan medewerkers van alle niveaus in de organisatie te geven. Dit is een veel te hoge drempel voor velen. Denk aan het vertalen van relevante zaken in jip-en-janneketaal zodat elke medewerker deze makkelijk tot zich kan nemen.

- De kennis moet hapklaar zijn. Wanneer kennis alleen te volgen is in de vorm van een langdurige e-learning of langdradig document, zal dit voor veel medewerkers een te hoge drempel zijn. Ze zullen deze kennis wellicht initieel nog wel tot zich nemen, maar in hun dagelijkse werkpraktijk kunnen ze er weinig mee, omdat ze de informatie vaak snel nodig hebben. Denk hier aan korte beschrijvingen, tips-and-tricks; liever niet langer dan een paar schermen om te lezen.

- De kennis moet zo compleet mogelijk en actueel zijn. Wanneer kennis niet compleet en actueel wordt gehouden zullen mensen snel interesse verliezen en het nut er niet meer van inzien.

- De kennis moet eenvoudig te vinden zijn. Een centrale plek; goede zoekmogelijkheden liggen voor de hand. Nog veel beter is het om de kennis te koppelen aan zaken die medewerkers in hun werk tegenkomen. Denk bijvoorbeeld aan het koppelen van instructieteksten en reminders binnen 'normale' werkinstructies, checklists of zelfs in het scherm van bepaalde applicaties waarmee mensen werken.

Zoals vanuit het 10-20-70 model blijkt, leert men het meeste tijdens het toepassen in het werk. Naast het beschikbaar stellen van kennis is het belangrijk ervoor te zorgen dat mensen snel en eenvoudig contact kunnen krijgen met ondersteuning wanneer zij zaken niet (tijdig) zelf kunnen vinden, zaken aantreffen die niet specifiek beschreven staan of twijfelen. Een open bedrijfscultuur waardoor mensen zich niet bezwaard voelen hulp in te schakelen en een laagdrempelige manier van contact vinden en maken is hierbij van groot belang. Zorg dus voor informatie over de beschikbare communicatiemogelijkheden op de plaatsen waar mensen deze nodig hebben. Een telefoonnummer verstopt op het intranet is niet voldoende!

Uiteraard is alleen kennis beschikbaar stellen niet voldoende. Mensen moeten getriggerd worden om de kennis te consumeren. Het liefst zo vaak mogelijk. Dit kan door kennis op te nemen op logische plaatsen in werkprocessen zoals hierboven beschreven, maar er is meer mogelijk:

- Regelmatige simulaties helpen om gedrag te conditioneren zodat mensen (zonder te veel gevaar) geconfronteerd worden met de gevolgen van hun acties. Phishingsimulaties en telefoongesprekken waarin social hacking wordt gesimuleerd zijn goede voorbeelden. Let op, met name de tweede genoemde optie kan een relatief dure vorm van bewustzijnsverhoging zijn.
- Games waarin bewustzijn wordt getest kunnen een goede en leuke manier zijn om mensen duidelijk te maken welke zaken ze nog niet goed genoeg weten of doen. Een competitief element kan sommige mensen enorm stimuleren om meer te willen weten of het beter te doen. Belangrijk is wel dat in deze games dan ook terugkoppeling is naar de eerder besproken kennis.
- Zeer regelmatig toetsen. Door bijvoorbeeld elke week op een gemakkelijke manier één vraag stellen. Als hierbij ook wordt uitgelegd wat het goede antwoord zou zijn geweest als iemand een fout antwoord kiest en een gemakkelijke verwijzing wordt gegeven naar bijbehorende kennis, wordt dit nog effectiever.

Een belangrijk aspect bij bovenstaande manieren om mensen te activeren is de tijd die het hen kost. Voor de meeste organisaties is veilig werken met gegevens belangrijk, maar zeker niet de core business. Men is in de praktijk vaak huiverig om hier veel aan te doen met het idee dat dit te veel 'productietijd' van medewerkers opslokt. Het is daarom heel belangrijk om weloverwogen keuzes te maken uit de verschillende manieren om mensen bij het onderwerp te blijven betrekken. Effect versus kosten en tijdsbeslag is daarbij dan een belangrijke factor. Het kostenplaatje zou voor veel – met name kleinere –organisaties sowieso een beperkende factor kunnen zijn om medewerkersbewustzijn zo veelomvattend op te pakken, ondanks het belang. Daarom moet zoveel mogelijk naar standaardisatie worden gezocht. Als elke organisatie het wiel opnieuw gaat uitvinden zal dit onvermijdelijk leiden tot suboptimale oplossingen en onnodige kosten. Zorg dus voor:

- Een bestaande bron van kennis uit de markt die ook actueel wordt gehouden. De meeste kennis die hier benodigd is, is voor vrijwel elke organisatie hetzelfde. Een kleiner deel is organisatie-specifiek. Deze kun je dan toevoegen. Dit scheelt uiteraard enorm in het opbouwen en onderhouden van alle benodigde kennis.

- Standaard technische hulpmiddelen om je te helpen met het continue triggeren van je medewerkers zonder dat dit telkens veel tijd kost om te organiseren.

- Een geïntegreerde set van hulpmiddelen zodat de gegevens die je hieruit wilt registreren om je organisatie te sturen en je acties aantoonbaar te maken voor stakeholders als directie, klanten, auditors en worst case de Autoriteit persoonsgegevens, centraal en met minimale moeite te produceren zijn. Naast het verbeteren van kennis en gedrag van je medewerkers is dit aantoonbaar doen immers bijna net zo belangrijk.

Door bovenstaande te implementeren is het mogelijk medewerkersbewustzijn over veilig werken met gegevens naar een hoger plan te tillen in je organisatie. Duidelijk is ook dat hiermee veel meer bereikt wordt dan met alleen die eerste training. En dat binnen rede voor tijdsbeslag van medewerkers en kosten.

Referenties

(1) https://702010institute.com/702010-model/
(2) https://en.wikipedia.org/wiki/Hermann_Ebbinghaus
(3) Artikel Keynote speech Erik Schoppen en interview in iB-Magazine 3 2019

Even voorstellen

Ik ben Migiel de Wit-Beets. Sinds deze zomer heb ik de voorzittersrol van de Commissie PR & Communicatie overgenomen van Henk Brandon. Daardoor ben ik actief betrokken bij het bestuur van het Platform voor Informatie Beveiliging. Tijd om mijzelf dus ook voor te stellen aan jullie!

Ik ben Migiel de Wit-Beets. Sinds deze zomer heb ik de voorzittersrol van de Commissie PR & Communicatie overgenomen van Henk Brandon. Daardoor ben ik actief betrokken bij het bestuur van het Platform voor Informatie Beveiliging. Tijd om mijzelf dus ook voor te stellen aan jullie!

De commissie PR & Communicatie heeft de afgelopen jaren veel zaken gerealiseerd. Aan mij en natuurlijk mijn mede commissieleden de schone taak om deze lijn verder voort te zetten. Samen willen wij ervoor zorgen dat ons Platform de bekendheid gaat krijgen die zij verdient en dat haar leden die informatie vinden die ze zoeken. Dit alles op basis van communicatie(middelen) die passend zijn bij de specifieke doelgroep. Immers, we hebben een grote diversiteit aan leden en daarmee dus ook een grote verscheidenheid aan behoeften.
In de laatste ALV van 2021 heb ik al een klein tipje van de sluier opgelicht waar wij dit jaar onze aandacht naar uit laten gaan. Voor degenen die daar niet aanwezig waren nog even een korte samenvatting.

Samen met de Commissie Jong PvIB gaan we de laatste fase van mailautomation inrichten zodat we beter in staat zijn om onze leden beter te betrekken binnen onze organisatie vanaf hun allereerste kennismaking.
We willen meer gebruik gaan maken van sociale media (vooral LinkedIn) om de naamsbekendheid van ons platform te vergroten. Daarnaast willen we een slag maken met de verdere digitalisering van PvIB met als doel dat we beter kunnen interacteren met onze omgeving en de verschillende doelgroepen.

Naast mijn rol als voorzitter ben ik bij Grant Thornton verantwoordelijk voor het team Cyberriskservices, waar wij een diversiteit aan organisaties (groot en klein) ondersteunen op het gebied van cyberweerbaarheid. Het is geweldig om te zien hoe wij in staat zijn zowel de koekjesfabriek op de hoek als de multinational die actief is in tien landen te ondersteunen met vraagstukken die eigenlijk best dicht bij elkaar liggen. Organisaties helpen bij het cyberweerbaar worden en blijven is waar wij iedere dag met plezier aan werken en waar wij energie van krijgen.

Ik zie uit naar 2022. In mijn optiek een jaar waarin we onze vrijheid stukje bij beetje terug zullen krijgen en waar digitale veiligheid nog meer aan de orde van de dag zal zijn dan in 2020 en 2021. Onze kennis en kunde van ons vakgebied zullen opnieuw op de proef worden gesteld in kaders van veiligheid en weerbaarheid. Let's rock together!

O ja, mocht je denken, ik wil ook wel een steentje bijdragen aan het Platform, schroom dan niet om contact met ons op te nemen via: secretariaat@pvib.nl

Groet, Migiel de Wit-Beets

Auteur: Nicole van Deursen is redactielid van iB-Magazine. Nicole is bereikbaar via nicolevandeursen@pvib.nl..

Maak van je werk je hobby

We hebben het allemaal hartstikke druk en toch vinden heel veel mensen de tijd om ook als vrijwilliger bezig te zijn met informatiebeveiliging. Dat is om meerdere redenen een goed idee. Het kan bijvoorbeeld een manier zijn om ons vak naar een hoger niveau te brengen, om je eigen vaardigheden te oefenen of om jouw maatschappelijke betrokkenheid in actie om te zetten. Na twee jaar thuiswerken is vrijwilligerswerk ook nog eens een mooie gelegenheid om nieuwe mensen te ontmoeten.

Droom je ook wel eens om van je werk je hobby te maken? We zetten een aantal mogelijkheden op een rij.

1. Platform voor Informatiebeveiliging
Bij onze eigen vereniging zijn diverse commissies waar je actief in kunt zijn. Je kunt helpen bij het organiseren van evenement, helemaal dit jaar met een jubileum. Of schrijf bijvoorbeeld eens een artikel voor het magazine. Voordeel van PvIB vrijwilligerswerk is dat je er PE-punten mee verdient!

2. Gemeente
Gemeentes zetten vrijwilligers in om in wijken te helpen bij digitale veiligheid. In Den Haag staat dat bekend als Digitaal veilig in de wijk, in Utrecht heet het Stadsmakers Digitale Veiligheid en in Breda zijn er Digitale Buurtambassadeurs. Misschien heeft jouw gemeente dit ook georganiseerd, of staan ze ervoor open dat je zo'n initiatief opstart.

3. Politie
Veel eenheden bij de politie hebben mogelijkheden voor politievrijwilligers met kennis van cybercrime. Je krijgt een screening, je wordt beëdigd en je volgt een opleiding. In de toekomst zullen er meer plekken beschikbaar komen, dus als je dit interessant vindt kun je de website van de politie in de gaten houden.

4. Open source projecten
Er zijn heel veel online communities die zich richten op het ontwikkelen en delen van open source tools en informatie voor cybersecurity. Je kunt er zelf een bijdrage leveren en vooral ook veel van leren. Enkele voorbeelden zijn OWASP ZAP, de COVID-19 Cyber Threat Coalition, ClamAVC. Je hoeft niet per se te kunnen programmeren. Je kunt ook helpen met documentatie of marketing.

5. Dutch Institute Vulnerability Disclosure
Een team van vrijwilligers ondersteunt het DIVD bij het vinden en rapporteren van kwetsbaarheden. Dit gebeurt op een professionele wijze, volgens een gedragscode en onder toezicht van Nederlands meest bekende en gewaardeerde gezichten. Zie ook het artikel elders in dit blad.

6. Seniorweb
Senioren hebben het soms lastig met internet, smartphones, en computers. Met computervragen kunnen ze terecht bij Seniorweb. Vrijwilligers helpen ze verder met uitleg en hulp.

7. Bits of Freedom
Wil je je inzetten voor vrijheid en privacy op het internet? Kijk dan eens naar de vele thema's bij Bits of Freedom, een beweging die opkomt voor internetvrijheid.

8. Spiegelbeeld – VHTO
Ben je een vrouw en wil je meisjes enthousiast maken voor het werken in de IT? Word dan rolmodel bij VHTO en geef voorlichting of les tijdens diverse activiteiten.

9. Hack in the Class
Vind je het leuk om mee te helpen met het ontwikkelen van lesmateriaal voor kinderen? Of misschien naar scholen te gaan en workshops te geven? Dan is deze organisatie misschien wat voor jou.

10. Cyberworkplace
Cyberworkplace biedt gratis cybersecuritytraining en coaching aan jonge mensen. Training wordt gegeven door vrijwilligers in Rotterdam, maar er is interesse om ook op andere plaatsen actief te worden.

11. Hacklab
Deze werkplaats in Leeuwarden staat open voor digitale hangjongeren, gamers, schoolverlaters, jongeren met een autismespectrumstoornis en jongeren die uitdaging in hun huidige opleiding missen. De leerlingen worden met verschillende individuele en groepschallenges uitgedaagd op het gebied van hacken, programmeren, lockpicking, pentesting etc.

12. CoderDojo
Deze internationale organisatie zet zich over de hele wereld in om kinderen gratis te leren programmeren. Er zijn inmiddels 1900 Dojos in 93 landen, allemaal gerund door vrijwilligers.

13. Bellingcat
Als je interesse hebt in het speuren in openbare bronnen kijk dan eens bij Bellingcat. Op hun website kondigen zij aan dat ze in 2022 een vrijwilligersplatform zullen lanceren waar je kunt bijdragen aan verschillende open source onderzoeksprojecten.

En dan zijn er nog mogelijkheden om in de tijd van de werkgever een extra steentje bij te dragen:

14. Hack Right
Hack Right is een alternatief voor een straf voor jongeren die worden aangehouden voor cybercrime. Vaak overzien zij de gevolgen van hun daden niet. Met Hack Right worden jongeren weer op het rechte pad geholpen en leren ze hun talent in te zetten op een positieve manier. Meerdere grote Nederlandse organisaties werken mee om de jongeren te coachen en werkervaring op te laten doen. Het gaat dus niet echt om vrijwilligerswerk in je vrije tijd, maar om vrijwillige medewerking als organisatie.

15. Non-profit organisaties gericht op kennisontwikkeling en kennisdeling
Naast de vakvereniging zijn er ook diverse samenwerkingen die zich richten op het ontwikkelen en delen van kennis, best practices, workshops, seminars enzovoorts. Enkele voorbeelden waarvoor je je kunt inzetten zijn CIP-overheid, Secure software alliance, Open web application security-project (OWASP) en Forum of Incident and Response Teams (FIRST).

16. Cyberreservist bij Defensie
Het is geen vrijwilligerswerk, maar iets dat je naast je vaste baan kunt doen: cyberreservist bij Defensie. Je moet wel aan strenge eisen voldoen en een training volgen. Daarna kun je worden ingezet bij oefeningen, onderzoeken, operaties of een militaire missie.

Auteur: Chris van 't Hof is directeur bij DIVD en is bereikbaar via chris@divd.nl.

DIVD: het Rode Kruis van het internet

Vrijdagavond 2 juli 2021 startte REvil een wereldwijde ransomware-aanval via kwetsbaarheden in KaseyaVSA. Dit is software waarmee Managed Service Providers de IT van hun klanten op afstand kunnen beheren. Door deze kwetsbaarheid, een Authentication Bypass, konden de criminelen dus in een keer alle klanten van deze MSPs besmetten met ransomware. Het moment was niet toevallig gekozen: in de VS waren veel werknemers al naar huis om met bier en barbecue het weekend van de 4th of July in te luiden.

Niet bij het bedrijf Kaseya zelf, want daar gingen alle alarmbellen af. Onmiddellijk namen ze contact op met DIVD-onderzoeker Wietse Boonstra. Hij had namelijk diezelfde kwetsbaarheid al ontdekt op 2 april en nog zeven andere waar inmiddels ook een CVE-nummer voor was aangevraagd. DIVD-CSIRT Manager Frank Breedijk hielp hem een goede Proof of Concept te schrijven en DIVD-voorzitter Victor Gevers wendde zijn contacten aan om met Kaseya een Coordinated Vulnerability Disclosure traject in gang te zetten. Onderzoeker Lennaert Oudshoorn haakte aan om het internet te scannen op wie gebruik maakt van KaseyaVSA. Anders dan bij veel andere ontvangers van een CVD-verzoek, reageerde Kaseya destijds direct zeer coöperatief. De eerste zeven CVE waren al gefixed en patches werden verstuurd naar de MSPs. De laatste, de Authentication Bypass, was na twee maanden nog niet gefixed en Kaseya was dus net te laat.

Groot voordeel was dat DIVD al sinds april de hele IPv4 range van het internet scande op de aanwezigheid van KaseyaVSA. We kwamen op een totaal van 2.200 MSPs, elke met vele tientallen of honderden klanten in beheer, dus rond de miljoen potentiële slachtoffers. Er was ook al een early warning uitgegaan via CSIRT DSP richting MSPs dat er iets ernstigs aan de hand was met de software van Kaseya en er een disclosure aan zat te komen.

Nul potentiele slachtoffers

Met de contactenlijst van alle MSPs ging DIVD die vrijdagavond direct aan de slag om steeds weer alle IP-adressen te scannen op aanwezigheid van KaseyaVSA en meldingen uit te sturen naar de MSPs met de duidelijke boodschap: zet KaseyaVSA nu uit. Binnen Nederland waren er rond de honderd. Die werden niet alleen door DIVD gewaarschuwd, maar ook via onze Trusted Information Sharing Partners.

Intussen werden we ons ervan bewust dat we, door REvil te dwarsbomen ook zelf een target zouden kunnen zijn. Onze CISO Fleur van Leusden stelde direct de logfiles veilig, verhoogde de dijkbewaking en deed een treat analysis van de actor. En inderdaad, die zaterdag werd Wietses mailserver gebruteforced vanuit de Oekraiene, zonder al te veel schade. Op de DIVD-omgeving zagen we geen verdacht verkeer.

Zondag 4 juli zagen we eerst nog drie kwetsbare servers in Nederland online staan. De eigenaren daarvan werden gebeld en om 13.00 stond Nederland op nul potentiële slachtoffers van de ransomware aanval.

Rode Kruis van het internet

KaseyaVSA is een van de negentien onderzoeken die DIVD in 2021 heeft verricht. Daar publiceren we pas over als het onderzoek is afgerond. Echter, door de ransomware aanval en omdat het hier zero-days betrof die we zelf hadden ontdekt, kwam ons werk wel breed in de internationale media. Voorzitter Victor Gevers, CSIRT-manager Frank Breedijk en onderzoeker Wietse Boonstra waren in de week volgend op de aanval bijna dagelijks in het nieuws, in de VS o.a. bij CBS, Wall Street Journal en Bloomsberg en in Nederland bij RTL-nieuws, NOS Journaal en Nieuwsuur.

In de media zagen we een terugkerend patroon. Na uitleg over de aanval, verwonderden de journalisten zich vooral over het feit dat het wereldwijd scannen en melden van dergelijke kwetsbaarheden afhangt van een klein groepje Nederlandse vrijwilligers. Waarom doet de overheid of het bedrijfsleven dat niet?

Dat gebeurt ook wel, echter heeft elk van deze partijen zo hun eigen doelgroep en mandaat. DIVD werkt precies andersom. We zijn ook geen CERT of SOC voor een specifieke doelgroep, maar gaan uit van een kwetsbaarheid en scannen daar de hele wereld op. Zitten daar IP-adressen bij die volgens ons door anderen bediend worden, bijvoorbeeld hun CERT of Internet Service Provider, melden we ook via die partijen.

We blijven scannen en melden om potentiële slachtoffers te helpen, ongeacht wie of waar ze zijn, ongevraagd en gratis. DIVD is daarmee een soort Rode Kruis van het internet.

Het belang van ons werk werd ook erkend door de Onderzoeksraad voor de veiligheid in hun rapport 'Kwetsbaar door software' van (16 december 2021). DIVD wordt daarin 47 keer genoemd, met een beschrijving van onze onderzoeken en als een van de hoofdconclusies: 'Alle door de Onderzoeksraad onderzochte voorvallen laten zien dat (vrijwillige) beveiligings- onderzoekers een cruciale rol spelen in de incidentbestrijding.'

Wel een Engelse naam

Dat terwijl DIVD nog geen drie jaar bestaat. Het begon met het werk van Victor Gevers, alias @0xDUDE. Ik schreef al eerder over hem in mijn vorige boek Helpende Hackers (2015), waarvan ook diverse stukken zijn verschenen in dit tijdschrift. Hij was toen al 16 jaar bezig met het hele internet te scannen op kwetsbaarheden en die ongevraagd te melden bij degenen die het kunnen oplossen. Na 9.000 uur vrijwilligerswerk had hij toen 4.000 responsible disclosures op zijn naam staan. 2016 was het jaar waarin hij met zijn missie naar buiten trad, door het hele jaar rond, alle 366 dagen, 15 uur per dag lekken te vinden en te melden. Daarna is hij

Gaandeweg haakten steeds meer organisaties aan als zogeheten Trusted Information Sharing Partners.

geloof ik gestopt met het tellen van zijn disclosures.
Victor verscheen daarop vaker in de media en op evenementen en ik zag steeds meer hackers die zich wilden aansluiten bij zijn missie. In het voorjaar van 2019 besloten Astrid Oosenbrug, Victor en ik een stichting op te richten om zijn werk in onder te brengen. We vroegen vier cyberzwaargewichten om onze Raad van Toezicht te worden: Lodewijk van Zwieten, Petra Oldengarm, Herbert Bos en Ronald Prins - namen die in dit tijdschrift geen toelichting nodig hebben.
Hoe moeten we dan gaan heten? Er mag geen 'cyber' in onze naam voorkomen, want dat zou menig lezer van dit tijdschrift alleen maar oproepen ons te trollen. Liefst iets met 'vulnerability' en 'disclosure'. Moeten we dan het woordje 'responsible' of 'coordinated' ervoor zetten? Nee, dat wordt weer zo'n eindeloze discussie. Ik herinnerde me ineens dat ik de domeinnaam divd.nl nog had, om ooit nog eens de Democratische Inlichtingen- en Veiligheidsdienst op te zetten, een soort wiki voor dreigingsinformatie. Dat was bedoeld als grap en als naam van een serieus onderzoeksinstituut kon dit natuurlijk niet.
Het moet ook wel een Engelse naam zijn, want het internet houdt zich niet aan landsgrenzen. Maar met een vier letterige .nl URL lijkt het wel alsof je al lang bestaat, want de meesten daarvan zijn allang vergeven. Puzzelend met de vier letters kwam ik tot Dutch Institute for Vulnerability Disclosure. We doen onderzoek, onthullen kwetsbaarheden en doen het op z'n Nederlands: open, eerlijk en gratis. Daar kon iedereen zich wel in vinden.
Op 26 september gingen Astrid, Victor en ik naar de notaris om stichting Dutch Institute for Vulnerability Disclosure te registreren en op 1 oktober hebben we tijdens de OneConference DIVD gelanceerd. Daar sloot ook Frank Breedijk zich bij ons aan. Hij had namelijk net een Security Meldpunt opgericht om ook kwetsbaarheden bij organisaties te melden. We vonden het logisch dit initiatief meteen te incorporeren in onze nieuwe stichting. Dat was maar goed ook, want rond de jaarwisseling barstte de Citrix crisis los en was dit voor Frank het startsein voor zijn meldpunt.

Meedoen

CVE-2019-19781 werd op 17 december 2019 bekend gemaakt door Citrix zelf, echter zonder patch. Victor scande het hele internet en vond 128.777 kwetsbare servers online. Dat was toen nog te veel voor onze kleine organisatie om te melden. Matthijs Koot scande op de Nederlandse IP range en vond er 600. Dat was wel te doen. Toen 11 januari 2020 ook een exploit beschikbaar werd, activeerde Frank het Security Meldpunt, zocht de url's bij de IP-adressen en stuurde waarschuwingsmails naar info@, security@ en abuse@. Bij herhaalde scans zagen we de aantallen dalen en stuurde Frank herinneringsmails naar degene die nog kwetsbaar waren. De laatste tien hebben we gebeld.
Citrix was de kickstart voor DIVD en er volgden vele onderzoeken, die allemaal zijn terug te vinden op divd.nl. Het DIVD-meldpunt werd omgedoopt tot CSIRT, omdat alles op de site in het Engels is en we ook steeds meer buiten Nederland gingen melden. DIVD heeft inmiddels ook een eigen scan infrastructuur, dat ook ons eigen Autonomous System runt: AS 50559, IPv4 range 194.5.73.0 - 194.5.73.255. Daarmee weten degenen die gescand worden dat wij het zijn en houden we zelf als stichting controle over de scanresultaten.

Gaandeweg haakten steeds meer organisaties aan als zogeheten Trusted Information Sharing Partners. DIVD CSIRT stuurt in eerste instantie meldingen van gevonden kwetsbaarheden direct aan de gevonden potentiële slachtoffers maar vervolgens nogmaals via deze TISPs. Enkele zijn: NBIP voor providers, ZCERT voor de zorgsector, Surfcert voor het hoger onderwijs, IBD voor gemeenten, DTC voor het ondernemend Nederland, FERM voor de Rotterdamse haven, Connect2Trust voor CISO's onderling, Cyberveilig Nederland voor security bedrijven en NCSC voor Rijk en Vitaal. Hier komt in 2022 een aparte stichting voor, onder dezelfde naam die Frank Breedijk ooit gebruikte voor zijn meldactiviteiten: het Nederlandse Security Meldpunt.
Zoals in de vorige iB-magazine te lezen was, zijn we in 2022 gestart met een subsidie van DTC voor betaalde deeltijdfuncties. Dat zijn vooral managementtaken om de vrijwilligers te ondersteunen: administratieve ondersteuning vanuit LunaVia, Lennaert Oudshoorn als Head of CSIRT, Victor Gevers als Head of Research en ik als directeur DIVD. Hier komen nog hoofden bij voor de afdelingen HRM, Operations en Communication. Dit jaar gaat ook de DIVD Academy van start om jongeren het hackersvak bij te brengen en komt er een internationale tak CSIRT.global om DIVD chapters op te richten in verschillende landen.
Kortom, het wordt een mooi jaar voor DIVD. En als je mee wilt doen, weet je ons te vinden.

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

COLUMN MARTIJN

Oproep

Vroeger, toen de wereld nog plat was en de bureaus nog niet verstelbaar, studeerde ik cybersecurity. Oké, dat is maar zes jaar geleden, maar in de cybersecurity telt dat zomaar als een era. Alles verandert snel, en niet alleen omdat IT een enorme veranderende kracht in de wereld is. Voor criminelen is er immers ook veel te halen in de cyberwereld en de wapenwedloop verdubbelt nog weer de snelheid van verandering. Niet alleen de digitale wereld verandert, ook mijn blik erop.

Sorry, aan de helft van al mijn docenten destijds. Toen ik studeerde vond ik alle technische vakken uitermate veel leuker dan het 'socio-economische' van cybersecurity. Leren hoe alles technisch werkt (en het vervolgens kapothacken uiteraard) dát was wat mij op dat moment trok. Ik begon, to nobody's surprise, dan ook als ethical hacker. De impact van kwetsbaarheden duidelijk maken was mijn missie. Snel daarop volgden jaren van Incident Response. De échte dreiging, de échte impact zag ik. Ik kreeg te zien waar het toch elke keer misging en kon er direct wat aan helpen doen.

Langzaam veranderde hier wat voor mij. Elke keer weer was het belangrijkste toch het uitzetten van de juiste acties, het prioriteren van de juiste recovery strategie. Soms trok ik mijn colbertje uit en kroop achter de laptop om een lastig IT-probleem op te lossen of een stuk van het digitaal forensisch onderzoek te doen. Dat was alleen niet wat op dat moment het belangrijkste was, #beginvanheteinde.

Tijdens en na zo'n incident evalueren we natuurlijk ook even. Hoe kon dit gebeuren? Wat moeten ze nu doen? Langzaam begon hier een gedachte te ontstaan. Als je je wilt beschermen tegen de huidige dreigingen, wat moet je dan doen?

Ik ging in gesprek. Vanuit de praktijk, vanuit mijn technische achtergrond. Wat vond ik dat er allemaal moest gebeuren? Altijd weer basisdingen. MFA. Ja, ook voor de belangrijke mensen die uitzonderingen willen. Ja, ook op je gekke back-up VPN. Ja, ook voor je clouddienst. Ja, ja en ja. Nee, geen uitzonderingen. Updates. Ja, overal. Ja, vaker dan eens in de maand ja. Uitzonderingen? Die segmenteer je helemaal weg. En zo gaat het lijstje maar door.

Drommels, wat ik nu deed lijkt toch wel heel erg veel op wat ik vroeger zo doodsaai vond in een collegebank: maatregelen bepalen aan de hand van… risico's? Nee, dat deed ik niet. Aan de hand van dreigingen, precies op basis van welke acties ze ondernemen. Misschien is dat wel een enorme shortcut, geen vertaling naar risico's. Maar even serieus, als je de basis niet op orde hebt, hoef je er echt nog niet zo diep in te duiken.

En als je al wel wat verder bent en risicomanagement goed wil aanpakken, is het in mijn ogen essentieel dat je die dreiging goed snapt. Verplaats je in hun schoenen. Waar zijn ze op uit? Wat is hun werkwijze? Met wie werken ze samen? Wat voor soort alcohol drinken ze eigenlijk wanneer ze toasten op hun volgende overwinning?
Dit is wat ik je oproep om te doen. Of je nou risico's in kaart aan het brengen bent, of een maatregel implementeert. Verplaats je in jouw aanvaller. Snap hun aanvallen. Begrijp waarom je maatregel hen tegenhoudt. Vertel dit verhaal erbij, waar je dit ook maar aan het doen bent. Met dit verhaal is alles zo veel sterker wanneer je zegt: nee, geen uitzonderingen.

Martijn Hoogesteger is vanaf dit nummer columnist van iB-Magazine. Hij heeft, zoals hij zelf zegt, een missie om cybersecurity 'plat te slaan': "Het is niet zo moeilijk, en dat ga ik je in elke column weer vertellen."

Auteur: Robert Metsemakers schrijft op persoonlijke titel en is als ervaren IT-auditor en informatiebeveiligings-expert beschikbaar voor security-advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

BLOG

Aan het roer van je eigen loopbaan

Het motto 'je zit aan het stuur van je eigen carrière', klinkt mij te gemakkelijk. Alsof je alleen hoeft te gaan zitten en de motor te starten. Om daarna je loopbaan simpel, via doseren van het gas, precies in de door jou gewenste snelheid in de beoogde richting te sturen. In de praktijk is het zoals in een zeilboot. Met het roer achter je. Je bent afhankelijk van de wind(richting) en moet steeds goed op je omgeving letten.

Je hebt inderdaad het roer in handen, maar op een boot zit dat achter je. Wat je meemaakte en leerde in je (arbeids)verleden moet je een plaats geven, er enige afstand van nemen en deze zaken in de hand houden, via de aan het roerblad verbonden helmstok. Bijzonder is dat je de helmstok juist de andere kant op moet bewegen dan waar je heen wilt met de boot. Zoals van veel stress in je baan, naar minder in je volgende. Van slecht verdienend met leuke collega's, naar goed verdienend met saaie collega's. Heen en weer, bij elke wissel in je carrière, tot je goed 'op koers' ligt. Maar als je te lang dezelfde koers aanhoudt, ga je van rustig naar te saai of van afwisselend naar te druk.

Wind mee

Verder moet je op een zeilboot 'de wind mee hebben'. Zonder wind is er geen beweging en zonder beweging is sturen op een boot onmogelijk. Het is noodzakelijk om vol-

doende wind in de zeilen te hebben. Tegen de wind in zeilen is onmogelijk. Door te laveren in grote bewegingen van links naar rechts kom je wel iets vooruit, maar helaas in een veel langere doorlooptijd. En als je dan ten langen leste arriveert, is de door jou te vervoeren lading katoenbalen of specerijen al aan een andere schipper gegund. En het romantische visrestaurant in dat leuke haventje is al dicht.
Om de actuele windrichting te weten, moet je continu je omgeving 'peilen'. Op een groter schip geeft het gedrag van andere bemanningsleden signalen af dat er storm op komst is, of juist een totale windstilte. Inspecteert men opvallend vaak de 'reddingsboten' op Linkedin? Dragen collega's reddingsvesten, zelfs in de eetzaal? Draaien veel gesprekken uit op: "Weet je waar ze óók mensen zoeken?", dan is er echt wel iets op komst. Je kunt ook omhoogkijken, naar het daarvoor bedoelde windvaantje. In een organisatie kijk je dan naar de managers, soms op het allerhoogste niveau. Zij hebben immers de meeste informatie. Is daar geen beweging te bespeuren en lijken ze muurvast op hun (pluchen) stoel te zitten, dan geldt dat vermoedelijk ook in de managementlaag en de werkvloer daaronder. En ook een zeer bewegelijk windvaantje - dus een groot verloop in hoge managers, die allemaal slechts kort blijven - moet je niet veronachtzamen, als je loopbaan je lief is.

Stormen en orkanen

Bij een vaartocht komt er altijd water in de boot. Noem het stress, tegenslag, pech of tegenvallers, het hoort erbij en is onvermijdelijk. Tot een bepaald niveau is dit te keren door te hozen, dus met een emmer het ongewenste water naar buiten te scheppen. Er zijn echter situaties waarin hozen niet helpt: als het water even hard of zelfs harder weer naar binnen stroomt, ben je aan het dweilen met de kraan open. Wanneer je meer tijd aan hozen besteedt dan aan het zeilen waarvoor je eigenlijk op die boot was gaan zitten, moet je jezelf afvragen of het niet eens tijd wordt het schip te verlaten...
Verlaat je dan het zinkend schip met de eerste ratten, die alles kaalvreten, onderpissen en de beste spullen meeslepen naar hun eigen hol of naar het volgende schip waar voor hen meer te halen is? Of blijf je loyaal 'in touw', heel eervol maar uiteindelijk wel funest, en ga je dan als laatste man met je geliefde schip ten onder? De keuze van het juiste moment is misschien wel de belangrijkste om te maken in je loopbaan. Soms moet je dit zelfs vaker doen in één loopbaan. Bijvoorbeeld als door klimaatverandering het aantal stormen en orkanen in jouw branche sterk toeneemt.

Scherpe blik

Het is dus zaak ontwikkelingen aan boord en daarbuiten goed in het oog te houden. Piraten, kapers, zeerovers, boekaniers en vrijbuiters worden vaak als karikatuur afgebeeld. Een flamboyante hoed (buitgemaakt op vrouwelijke slachtoffers op geënterde schepen), een papegaai op de schouder (er was veel zee-criminaliteit in het Caribisch gebied), een houten been (door neerstortende masten en gieken), een haak in plaats van een hand (na een kruitexplosie bij de kanonnen) en natuurlijk het bekende ooglapje. Verloren dan zoveel piraten een oog tijdens hun toen nog pre-ARBO - werkzaamheden? Neen, de reden is anders. De kanonnen op een piratenschip stonden onderdeks in twee rijen opgesteld. Heel soms werden alle kanonnen aan één kant tegelijk afgevuurd: het beschoten schip kreeg dan 'de volle lading' te verstouwen en dan raak je altijd wel iets. Mikken en dus goed zicht waren echter altijd nodig. Elektriciteit was er niet en vuur vermeed men vanwege het genoemde kruit op die houten schepen zoveel mogelijk. Het was onderdeks dus donker, terwijl op het dek zonlicht was. Soms veel zonlicht, zoals in dat Caribisch gebied. Als je als piraat (of K, Z, B, V) tijdens een zeegevecht de trap afdaalde naar de schietafdeling, zag je dus enige tijd niets omdat je ogen eerst moesten wennen aan het verschil in licht. Daarom dekten piraten terwijl ze bovendeks waren voortdurend één oog af. Dat oog bleef dus gewend aan donkere omgevingen. De trap aflopend klapte men fluks het ooglapje omhoog. Natuurlijk niet met de haakhand! Zo kon je meteen in het donker kijken, het doelwit zien en daarop mikken met dat ene uitwijk-oog. Dat zo niet het niet-functionerende, maar juist het beste oog voor de nieuwe situatie was. Zodat het door je omgeving waargenomen zwakke punt in je oude functie juist een sterk punt in de nieuwe job blijkt te zijn. Mooi man.

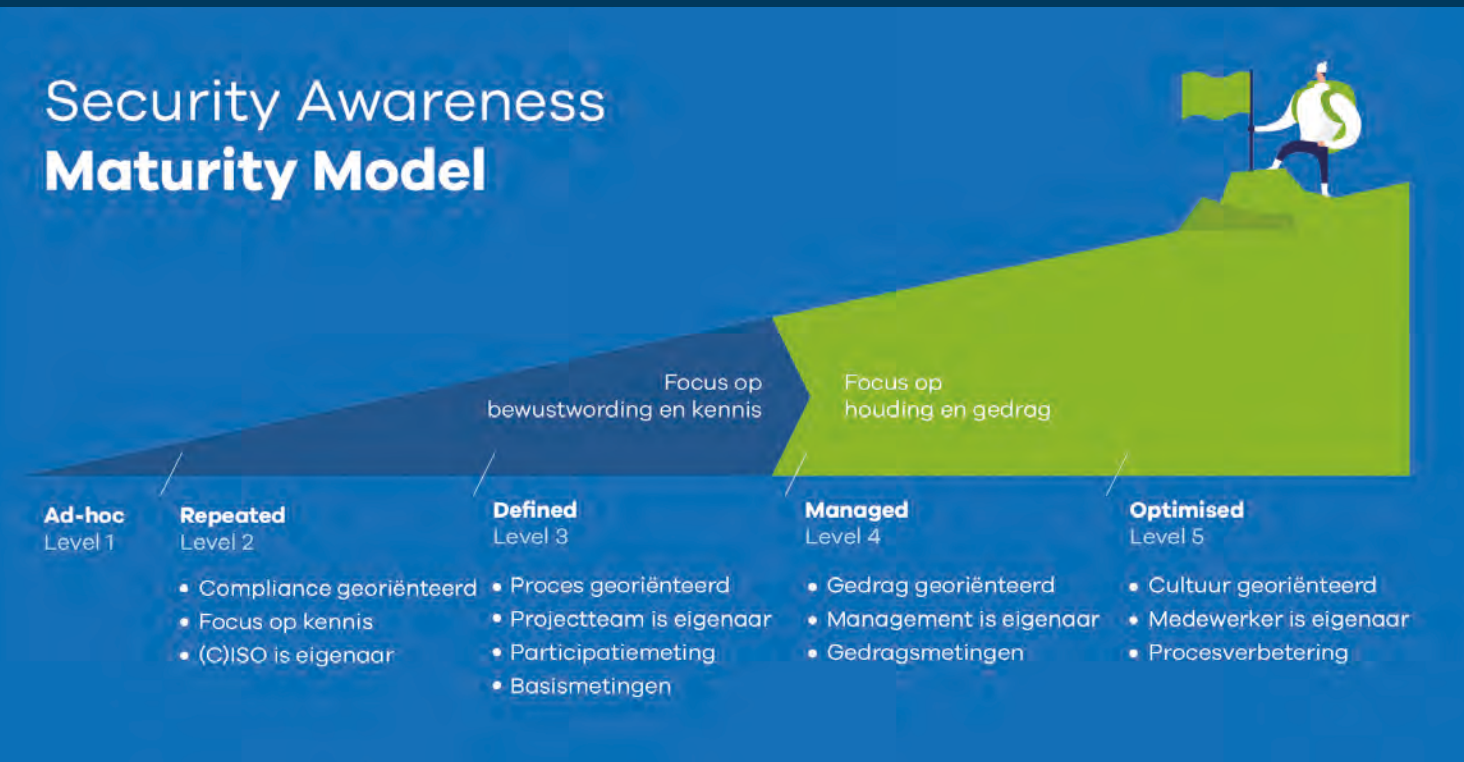
Als laatste tip: houd wat in reserve en geef beide ogen goed de kost. Scherp je blik boven- én benedendeks, op je eigen boot, maar ook op andere schepen en elders in de havens. Zo houd je jouw doel in zicht en de wind in de zeilen van je (security)carrière en raak je niet 'aan lagerwal'.

Behouden vaart!

Auteur: Wilbert Pijnenburg CISA CISSP is commercial director bij Infosequre en sinds 1996 werkzaam in de informatiebeveiliging. Sinds 2007 heeft hij een volledige focus op security awareness. In de afgelopen 15 jaar heeft Wilbert tientallen nationale en internationale organisaties geholpen bij de inrichting van hun awareness programma's. Wilbert is bereikbaar via wilbert.pijnenburg@infosequre.com.

Security Awareness Volwassenheidsmodel

Verleg de focus van bewustwording en kennis naar houding en gedrag



Afbeelding 1 - Infosequre-security-awareness-CMM model.

Iedere security expert weet dat goede informatiebeveiliging een combinatie is van mens, organisatie en techniek. Bewustwording en training van medewerkers is een standaard onderdeel van ieder beveiligingsprogramma. Een security framework zonder awareness bestaat niet. De laatste jaren hoor je steeds vaker dat security awareness gaat om gedragsverandering in plaats van bewustwording. Gedragsverandering en het creëren van een duurzame beveiligingscultuur is de Big Hairy Audacious Goal (1), maar dat betekent niet dat iedere organisatie meteen aan gedragsverandering moet of kan werken.

Het ontwikkelen van een beveiligingscultuur is een lange reis en iedere reis begint bij de eerste stap. Iedere beginnende karateka wil ooit in zijn leven de zwarte band halen, maar weet ook dat het begint met de gele band. En zo is het met security awareness ook. Je hoeft het einddoel niet onmiddellijk te bereiken, je kunt er stapsgewijs naartoe groeien. Om je te helpen bij het ontwikkelen van je bewustwordingsprogramma, je inzicht te geven in je huidige situatie en je een vooruitzicht te geven op je potentiële volgende stap, ontwikkelden we een security awareness volwassenheidsmodel.

Level 1: Ad-hoc level: "We moeten iets doen aan security"

In dit level is er nog niet echt sprake van een bewustwordingsprogramma. Het volwassenheidsniveau van de organisatie is dusdanig laag dat informatiebeveiliging vooral bestaat uit technische maatregelen met hier en daar wat procedures. Onder het motto 'we moeten iets doen', wordt er ad-hoc over security gecommuniceerd, meestal als reactie op een incident in de markt. Het initiatief ligt volledig bij de security verantwoordelijke of IT-manager. Het management is niet betrokken.

Level 2: Repeated – creëren van bewustwording en kennis

Er wordt met enige regelmaat aandacht besteed aan security awareness. We spreken voor het eerst over een bewustwordingsprogramma. De insteek is veelal 'compliance' georiënteerd, bijvoorbeeld omdat een toezichthouder zegt dat er iets aan security awareness moet worden gedaan of het in een security framework staat beschreven. De security verantwoordelijke of IT-manager is zowel eigenaar, bedenker als uitvoerder van het programma. De focus ligt volledig op het creëren van bewustwording en het bijbrengen van kennis. Er is weinig budget voor de uitvoering aanwezig. Management is niet betrokken en management commitment is onduidelijk. Er wordt weinig tot niets gemeten. Misschien wordt er een ad-hoc phishingtest uitgevoerd. De incidenten registratie is technisch van aard en er wordt geen root-cause naar menselijk gedrag uitgevoerd. Zit jouw organisatie in dit niveau? Je bent niet de enige. In Nederland zit 60% tot 70% van de organisaties ergens tussen niveau 2 en 3. Met de volgende stappen breng je jouw security awareness programma naar een hoger niveau.

Level 3: Defined – security awareness als proces

Het is niet voor niets dat dit level 'defined' heet. Het is het eerste niveau waar je kunt spreken van enige volwassenheid en waar security awareness als proces is ingericht. De focus ligt nog steeds voornamelijk op het creëren van bewustwording en kennis, maar de activiteiten worden nu gepland en geregeld uitgevoerd. Als onderdeel van de procesinrichting is een on-boarding programma opgenomen. Nieuwe medewerkers worden bij aanname geïnformeerd over de geldende richtlijnen. Langzamerhand verschuift de individuele aanpak van een security verantwoordelijke naar een meer multidisciplinair team. Om de activiteiten uit te kunnen

voeren is een basisbudget aanwezig. Management commitment is beperkt en nog niet echt betrokken bij de uitvoer. Het team is volledig verantwoordelijk en voert alles zelf uit. De onderwerpen worden op basis van eigen inzicht gekozen. De incidentenregistratie is technisch van aard en wordt niet op basis van de menselijke factor in kaart gebracht. Er vinden voor het eerst metingen plaats, maar deze zijn vaak participatie georiënteerd. Zo af en toe wordt een praktijktest uitgevoerd.

Level 4: Managed – focus naar houding en gedrag

In dit level vindt de omslag plaats. Bij level 3 maakten we nog een belangrijke stap om security awareness als proces in te richten. De focus lag op bewustwording en kennis. In dit level maken we de overstap naar de focus op houding en gedrag.

Op managementniveau zijn er fundamentele wijzigingen. De verantwoordelijkheid voor security awareness is verschoven van het uitvoerende team naar het management. Management commitment is duidelijk aanwezig en betrokken. Het management spoort medewerkers aan deel te nemen aan de awareness programma's, besteedt aandacht aan informatiebeveiliging in het werkoverleg en vertoont voorbeeldgedrag. Door het toegenomen managementsupport is er meer budget beschikbaar en medewerkers mogen tijd besteden aan de diverse activiteiten. Het multidisciplinaire projectteam heeft een faciliterende en ondersteunende rol gekregen.

Er worden SMART gedragsdoelstellingen gedefinieerd om aan gedragsverandering te kunnen werken. De incidentenregistratie is niet meer puur technisch van aard. Incidenten veroorzaakt door menselijk gedrag worden herkenbaar gelabeld en er vindt een root-cause analyse plaats op de incidenten. Op veel voorkomende en terugkerende incidenten vindt 'problem management' plaats en er worden acties bedacht om terugkerende incidenten in de toekomst te voorkomen. De onderwerpen van het programma worden bepaald op basis van de incidentenanalyse, risico's en gerenommeerde marktrapporten. Om de effectiviteit te bepalen worden regelmatig metingen uitgevoerd die het gedrag beoordelen.

Level 5: Optimised – the holy grail

Zie dit level als de holy grail van security awareness. De ideale wereld waar veel over gesproken en geschreven wordt, maar waar maar weinig bedrijven aan voldoen. Het is ook de reden waarom dit model is uitgewerkt. Je hoeft niet meteen te voldoen aan alle eigenschappen die bij dit hoogste level horen. Dit level is de stip aan de horizon. Bepaal je huidige niveau, kijk naar de volgende stap en bepaal je groeipotentieel. In de ideale wereld draait het niet om het opleggen van gedrag maar is veilig werken een second nature van de medewerker. Hier bereiken we een securitycultuur. Management is natuurlijk van de partij, maar de medewerker staat centraal. Zij worden betrokken bij de analyse. Samen bepalen zij waar de behoefte ligt. Net als bij level 4 worden er SMART gedragsdoelstellingen gedefinieerd, maar om de medewerker optimaal te ondersteunen wordt er ook gekeken naar de omgeving. Kunnen we obstakels weghalen en hoe kunnen we veilig werken ondersteunen? Security policies en IT-middelen worden beoordeeld op werkbaarheid en de fysieke omgeving wordt aangepast als dit veilig werken vereenvoudigt. Tooling wordt toegevoegd om veilig werken makkelijker te maken. Gedrag en effectiviteit worden met regelmaat gemeten. Op basis van de incidenten en risico's die herleidbaar zijn naar menselijk gedrag, marktrapporten en de metingen, worden regulier verbeteringen aangebracht en aanpassingen doorgevoerd.

Op naar de volgende stap

Het succes van een security awareness programma wordt voor een groot deel bepaald door de inrichting van het proces. Daarna moeten de verschillende initiatieven van dusdanige kwaliteit zijn dat ze invloed hebben op het gedrag van de medewerker. Het volwassenheidsmodel gaat vooral in op het proces. Het geeft inzicht in je huidige situatie en toont de volgende stap. Het behoedt je voor onrealistische doelen. Door dit inzicht wordt het voor iedere organisatie mogelijk om aan security awareness te werken. Of je nu een bank of de bakker om de hoek bent. Wat is jouw volgende stap?

Referentie

(1) Jim Collins & Jerry Porras. Built to last: Successful Habits of Visionary Companies, Random House, 2005.

COLUMN LEX

Olympische cyberspelen

De Olympische winterspelen van 2022 in Beijing moeten nog aanvangen wanneer ik dit schrijf, maar zijn afgelopen wanneer jullie dit lezen. Meer en meer hebben de spelen ook een kritieke cyber-dimensie. Je kunt spreken van Olympische cyberevents.

Het grootste cyberevent is een veilige uitvoering. Hierbij is er maar één deelnemer, het gastland. En de opdracht is alle bedreigingen tot verstoring van de spelen blokkeren. Een hoop kan voorkomen worden door de cyber-infrastructuur van de spelen aan te pakken als een hoog betrouwbaar grootschalig IT-project. En daarnaast natuurlijk ook deze infrastructuur goed te monitoren en intelligence te verzamelen. Dit voer je uit op die infrastructuur, via social media en natuurlijk ook op traditionele, non-cyber manieren. Dit is wel toe te vertrouwen aan het gastland deze keer.
Daarnaast is er dezer dagen een pandemie te beteugelen. Nu heeft gastland China dit al goed onder controle, dus alle deelnemers en bezoekers kunnen hier al primair als bedreiging gezien worden. Hoe houd je dat in de klauwen? Met een app. In dit geval met de schattige titel 'My 2022'. Als je de beschrijving in de appstore doorleest, staat er geen woord over de monitoring van gezondheidsinformatie door deze app, in de privacysectie staat wel een notificatie. Het is verplicht voor atleten en bezoekers om deze app 14 dagen voor vertrek al te gebruiken. Om bij de openingsceremonie te zijn, had je het monitoren op 20 januari moeten beginnen. Zal het de organisatie lukken om covid binnen de perken te houden? Vast wel. En deze app zal daar een grote rol in spelen.

Al met al, voor dit event lijkt China goud al binnen te hebben.

Dan zijn er nog wat bedreigingen die wat unieker gerelateerd zijn aan de locatie. Als de spelen gebruikt worden om ook aandacht te geven aan vermeende misstanden in het land, kan men daar niet traditioneel hard op ingrijpen, door de aanwezige internationale media. Wat kan dan wel gedaan worden? De intelligence gebruiken die toch al verzameld wordt. Maar je kunt een stap verder gaan en alle personen met de 'My 2022' app te monitoren. Security researcher Citizen Lab vond een zwarte lijst met ruim tweeduizend woorden die hiervoor ingezet kon worden. Ik ben benieuwd hoeveel gebruik hiervan achteraf aangetoond kan worden.
Het andere Olympische cyberevent is ongewenste intelligence inzameling en monitoring tegengaan. Hier speelt ieder deelnemend land aan mee. Nederland raadde atleten af om hun eigen mobieltje of laptop mee te nemen, maar daarvoor in de plaats een 'burner' te gebruiken. En ook om alleen maar een apart, tijdelijk e-mailadres te gebruiken. Om dan maar niet te spreken van het niet gebruiken van sociale media. Dat kun je atleten toch niet ontzeggen? Bij de euforie van een medaille winnen hoort het delen van dit moment op sociale media. Ik verwacht dat dit even groots zal gebeuren als op andere recente spelen is gebeurd.
Australië had een andere aanpak gekozen, die lijkt op de Nederlandse aanpak tijdens de winterspelen in Sotsji in 2014. Ze bouwden een eigen netwerk waar de ploeg mee communiceerde middels een VPN.
Met wat discipline én medewerking van het gastland kan dit werken. Het is wel simpel om hier de stekker eruit te trekken — met kans op een imagorel, dus ik verwacht wel wat terughoudendheid.
Wie zal dit event winnen? De tijd zal het leren. En vergeet niet, dit event is niet over wanneer de spelen ten einde komen. Alles wat persistent is wordt mee teruggenomen naar huis en bij huldigingen van atleten zijn dan laterale besmettingen van huldigende bobo's mogelijk. Het kan een tijd duren voordat hier de winnaars en verliezers duidelijk zijn.

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

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.

Onderzoeksrapporten pleiten voor sterk nationale, centrale cyberweerbaarheidsdienst

Er moet meer worden gedaan om te voorkomen dat de maatschappij wordt ontwricht door cyberaanvallen. Essentieel is dat er een sluitend nationaal stelsel zal moeten opgericht dat organisaties helpt om de digitale veiligheid op systematische en doelmatige wijze te beheersen. Ze moeten samen een effectieve aanpak bedenken om Nederland weerbaarder te maken. Fabrikanten van IT-middelen en IoT-apparaten zullen (meer) gedwongen moeten worden om dat te realiseren en afnemers moeten ze daartoe kunnen dwingen. Dat is de strekking van een reeks van aanbevelingen die vele gezaghebbende instituten (AR, WRR, CSR, RvS, IvhO en OvV) hebben gegeven naar aanleiding van verrichte onderzoeken naar digitale incidenten.

Digitalisering is allang niet meer een geïsoleerd of op zichzelf staand proces dat gestart is om 'papieren' middelen om te zetten in techniek. Digitalisering is bovendien al veel meer dan het gebruik en de werking van IT. De gigantische ontwikkelingen en de diverse informatiesystemen, telecommunicatie(middelen), digitale informatie, data, informatie- en computersystemen hebben ook een steeds verdergaande en toenemende invloed op de economie, op de samenleving en op de menselijke gedragingen. Nee, het is zelfs veel sterker dan dat: veel beter kan worden gesproken over een doorgaande digitale transitie; de verdergaande intense verwevenheid en verknoping van IT in steeds meer aspecten van het dagelijks leven en de economische processen die vervolgens op hun beurt in steeds meer netwerken opgenomen zijn met allerlei verbindingen en afhankelijkheden.

Digitalisering biedt oplossingen voor maatschappelijke problemen, maar brengt ook risico's met zich mee. Strategische punten bij de verdere ontwikkeling van digitalisering zijn de informatiebeveiliging, de interoperabiliteit van data/gegevens en binnen organisaties de rollen en verantwoordelijkheden van de verschillende stakeholders: professionele medewerkers en management. Voldoende goed gekwalificeerd personeel zal beschikbaar en het 'IT-budget' zal toereikend moeten zijn voor – ook – die andere aandachtsgebieden. Voor informatiebeveiliging zal bijzonder aandacht moeten zijn binnen de organisatiestructuur om recht te doen aan de toegenomen digitale dreigingen en de noodzaak om hier een goed gefundeerde besturing voor in te richten. Daar komen ook nog de afhankelijkheden bij in een 'digitale monocultuur': een kwetsbaarheid in één product raakt vele andere informatietechnologieën, dat een groot deel van de publieke sector en het bedrijfsleven kan raken.

Op nationaal niveau zijn de afgelopen jaren enkele belangrijke onderzoeken gedaan en is er gerapporteerd over het thema digitale veiligheid. Adviezen zijn gegeven over hoe 'verstoring van de digitale infrastructuur' dan wel een 'digitale ontwrichting' en 'cyberrampen' voorkomen kunnen worden alsook hoe 'cyberincidenten' zo spoedig mogelijk bestreden dan wel beheersbaar kunnen worden gemaakt.
De aanbevelingen uit al die rapporten geven vaak een eenduidige tendens aan: het Nederlandse digitale poldermodel is niet goed toegesneden, er dreigen digitale ontwrichtingen, de instanties reageren te traag én zowel aanbiedende fabrikanten, consumenten c.q. burgers, ondernemingen die gebruik maken van IoT-apparaten en andere IT-middelen kunnen en moeten veel meer doen aan cybersecure en cybersafe handelen. Nederlandse overheidsorganisaties en bedrijven zijn zeer kwetsbaar voor cyberaanvallen en er bestaat geen nationale structuur waarlangs alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd.

Dit artikel voorziet in een zeer beknopt overzicht van die rapporten.

AR: al meer dan tien jaar onderzoek

De Algemene Rekenkamer (AR) doet al meer dan tien jaar onderzoek naar informatiebeveiliging en heeft deze recent weer geanalyseerd. 'Hieruit blijkt herhaaldelijk dat de gestelde ambities op het gebied van digitalisering niet goed in balans zijn met de mensen, middelen en organisatie', zo valt op rekenkamer.nl/onderwerpen/ICT-en-digitalisering te lezen. De AR vraagt regelmatig aandacht voor het eenduidig beleggen van taken en een adequate invulling van verantwoordelijkheden, bijvoorbeeld rondom cybersecurity, informatiebeveiliging, het e-ID stelsel en het stelsel van basisregistraties. Zo wordt ook gevraagd om een (meer) coördinerende rol voor de verantwoordelijke bewindspersoon in het kabinet. 'Dat kan een uitbreiding van bevoegdheden van de minister inhouden, zoals bij informatiebeveiliging, waar resultaten achterblijven', zo schrijft de AR (1).

WRR: voorbereiden op digitale ontwrichting

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) startte in 2018 een adviestraject over hoe Nederland kan omgaan met een mogelijke cyberramp. De overheid en aanbieders van vitale processen hebben beperkt zicht op de partijen van wie zij afhankelijk zijn. Op het terrein van cybersecurity krijgt de voorbereiding op ontwrichting echter weinig aandacht. Dit maakt het lastig om de ernst van incidenten te kunnen vaststellen en het hoofd te bieden aan een digitale ontwrichting. Bij de bestrijding hiervan ontbeert de overheid bovendien een duidelijk omschreven bevoegdheid om in te grijpen. In het rapport Voorbereiden op digitale ontwrichting (2) pleit de WRR voor een betere voorbereiding op een digitale ontwrichting door o.a. adequate bevoegdheden om escalatie te voorkomen en inspanningen op het terrein van cyberverzekeringen te verrichten.

Van 'digitale maatschappelijke ontwrichting', of kortweg 'digitale ontwrichting' is volgens de WRR sprake als - door de groeiende verwevenheid van de digitale wereld met de fysieke en de sociale wereld - verstoringen van het maatschappelijke leven steeds vaker samenhangen met een ernstige verstoring of uitval van digitale processen. Van digitale ontwrichting is sprake wanneer het normale leven ernstig is verstoord.
De WRR stelt dat incidenten – door onderlinge afhankelijkheden en door de complexiteit en diversiteit van netwerk- en informatiesystemen – sneller grootschalige en grensoverschrijdende effecten

bezitten. Volgens de WRR moeten zowel de overheid als het bedrijfsleven samenwerken ten einde voorbereid te zijn op incidenten in de digitale ruimte.

De WRR deed een aantal aanbevelingen, waaronder de volgende:

- besteed bij het beleid voor vitale infrastructuur meer aandacht aan de ketens en netwerken die vitale processen ondersteunen;
- onderzoek bovendien of digitalisering het nodig maakt de prioritering van die processen aan te passen; en
- benut nationale en internationale incidentdata beter, om lessen te trekken met het oog op toekomstige verstoringen.

CSR: integrale aanpak cyberweerbaarheid

Ook de Cyber Security Raad (CSR) liet in april 2021 op een vergelijkbare wijze van zich horen. In het rapport Integrale aanpak cyberweerbaarheid (3) stelde de CSR dat digitale veiligheid op het hoogst bestuurlijke niveau moet worden belegd. Op dit moment is de cyberweerbaarheidsketen in Nederland niet op alle punten even sterk. Hierdoor ontstaan er lacunes en gebreken waardoor de cyberweerbaarheid van Nederland op diverse onderdelen zwakheden vertoont. De CSR adviseert voor de langere termijn te verkennen hoe het besturingsmodel zo kan worden ingericht dat overheden, inclusief de decentrale overheden, bedrijfsleven en wetenschap gezamenlijk kunnen werken aan één nationale cyberweerbaarheidsstrategie. "Wij gaan hier echt stevig werk van maken. Niet omdat het kan, maar omdat het moet", zei de demissionair minister van JenV bij de inontvangstneming.

RvS: precisie, standaardisatie en centralisatie

In mei 2021 bracht de Raad van State (RvS) een publicatie uit waarin het zijn visie ontvouwt op het gebied van digitalisering. Natuurlijk adviseert de RvS dat de wetgever waarborgen moet bieden voor de bescherming van de rechten van burgers en bedrijven bij algoritmische besluitvorming. Algoritmische besluitvorming is complex en vaak lastig uit te leggen. De bestuursrechter moet burgers rechtsbescherming bieden bij algoritmische besluitvorming. Er is een verscheidenheid in situaties en van complicaties waarmee men bij de uitvoering geconfronteerd zal worden. De RvS geeft na deze beschouwing aan op welke wijze dat beter kan: 'Dat wordt dan op de klassieke manier opgelost: door de bepalingen vaag te formuleren en in de toelichting alle mogelijkheden open te laten. Juristen en beleidsmakers gaan er doorgaans vanuit dat een gedigitaliseerde uitvoering de ruimte voor flexibiliteit, variëteit en oneindige mogelijkheden biedt. Het is echter precies omgekeerd: gedigitaliseerde uitvoering vraagt om precisie, standaardisatie en centralisatie, want alleen zo heeft men de voordelen van digitalisering' (4).

IvhO: meer sturing op cyberveiligheid

Naar aanleiding van de cyberaanval op de Universiteit Maastricht besteedde ook de Inspectie van het Onderwijs (IvhO) aandacht aan het thema cyberveiligheid in haar rapport met het heldere adagium 'Binnen zonder kloppen' (5). Onderwijsinstellingen zijn voor een groot deel zelf verantwoordelijk en daardoor onvoldoende beschermd. De IvhO vindt dat de overheid meer verantwoordelijkheid en regie moet nemen. 'Want de kennis en kunde blijkt in het veld zeker aanwezig, maar de sturing ontbreekt', aldus de IvhO. 'Het verhogen van de digitale weerbaarheid van de onderwijssector is niettemin noodzakelijk', maar 'ook moet het duidelijk zijn welke verantwoordelijkheden individuele instellingen zelf kunnen invullen, waar ze in gezamenlijkheid kunnen optreden om de kennis en expertise van alle ketenpartners optimaal te benutten en waar aanvullende coördinatie of ondersteuning vanuit de overheid nodig is', schrijft de demissionaire minister van OCW (6).

OvV: 'Kwetsbaar door software': fundamenteel ingrijpen

Het meest recente rapport over dit thema komt van de Onderzoeksraad voor Veiligheid (OvV). De OvV is duidelijk en zeer helder. De Nederlandse aanpak van digitale veiligheid moet snel en fundamenteel veranderen om te voorkomen dat de maatschappij ontwricht raakt door cyberaanvallen. Tot deze stevige conclusie kwam de OvV in het rapport Kwetsbaar door software (7). De OvV onderzocht beveiligingslekken die ontstonden bij duizenden organisaties door kwetsbaarheden in de software van Citrix. De OvV-voorzitter stelde duidelijk: 'Uit dit voorval blijkt dat Nederlandse overheidsorganisaties en bedrijven zeer kwetsbaar zijn voor cyberaanvallen en dat er geen nationale structuur is waarbinnen alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd.' De OvV merkt in het bijbehorend persbericht op dat aanvallers 'tot op de dag van vandaag' illegale toegang hebben 'tot systemen en data in bedrijven en organisaties die zij op elk moment kunnen activeren met disruptieve effecten op bedrijfsprocessen, dienstverlening, privacy en veiligheid.'

De OvV ziet 'opvallende overeenkomsten' tussen de onderzochte voorvallen. Organisaties, mensen die afhankelijk zijn van organisaties en ketenpartners waren digitaal onveilig omdat zij kwetsbare software gebruikten. De OvV geeft ook aan dat 'incidentbestrijding nog geen sluitende, vanzelfsprekende, systematische ingebouwde reflex is.'

Vanwege de doorgaande digitale transitie verkrijgen we steeds meer mogelijkheden, maar daarmee creëren we ook een steeds grotere afhankelijkheid van de digitale systemen. Fabrikanten, overheden en organisaties zullen samen tot een effectieve aanpak moeten komen om Nederland weerbaarder te maken tegen cybercriminaliteit; dus voorbereiden van een organisatie om

repressief te kunnen reageren. 'Fabrikanten overstelpen softwaregebruikers nu met patches en updates om gebreken in hun software te verhelpen zonder met structurele oplossingen te komen'. 'Er zijn geen instrumenten die afnemers van software onafhankelijk inzicht bieden in de veiligheid van de software. Ook schiet de eigen kennis en positie van afnemers vaak tekort om zelf eisen te stellen aan fabrikanten en veiligere software af te dwingen, of zien zij daar het belang niet van in', aldus de OvV. Dit vraagt van fabrikanten dat zij de veiligheid van hun software voortdurend en fundamenteel verbeteren. Door samen te werken kunnen afnemers hun positie richting softwarefabrikanten versterken en hun schaarse expertise beter benutten.

Dat vergt dat er één bewindspersoon en één centrale dienst komt die hierop toeziet, zo nodig kan ingrijpen en verantwoording aflegt. Ook beveelt de OvV aan dat grotere bedrijven en organisaties wettelijk worden verplicht om verantwoording af te leggen over de wijze waarop zij hun digitale veiligheid beheersen.

Korte beschouwingen

De inhoud van deze rapporten komen grosso modo overeen, al dan niet soms anders geformuleerd.

– De publieke sector en het bedrijfsleven zijn onvoldoende voorbereid om mogelijke, digitale ontwrichtingen te voorkomen en te bestrijden. De digitale polder functioneert onvoldoende of te traag door de vele lagen om de toenemende bedreiging goed het hoofd te kunnen bieden;

– De onderzoeken geven aan dat de kennis en kunde aanwezig is, maar overheden en het bedrijfsleven moeten hun krachten bundelen, meer regie, meer centralisatie, meer (en aanvullende) coördinatie tot stand brengen;

– De wens is om te komen tot één nationale cyberweerbaarheidsstrategie;

– Er wordt steeds meer geadviseerd een nationale 'instanz- und behördenübergreifende' structuur te laten ontstaan waarbij een effectieve vorm van regie met betrekking tot samenwerking vorm moet krijgen. Deze centrale dienst zal de informatiedeling sneller moeten verspreiden zodat alle belanghebbende organisaties tijdiger geworden gewaarschuwd om zodoende snel mitigerende maatregelen te nemen;

– Een aardige gedachte is om grotere bedrijven en organisaties wettelijk te verplichten om verantwoording af te leggen over de wijze waarop zij hun digitale veiligheid beheersen; dit naar analogie van de verplichte accountabilityverplichtingen uit de AVG/GDPR;

– Fabrikanten zullen de veiligheid van hun software voortdurend en fundamenteel moeten verbeteren. Dit zijn eigenlijk de alom bekende vereisten van 'privacy/security by design' en verbeteringen die worden doorgevoerd na toepassing van die ontwikkelprincipes! Inkopende organisaties kunnen dat uiteraard zelf afdwingen. In het bestek van aanbestedingsprocedures en bij andere inkoopprocedures kunnen eisen worden gesteld alvorens die IT-middelen daadwerkelijk aan te schaffen. Wellicht dat als IT-middelen door een virus getroffen worden, zouden achteraf de leveranciers aansprakelijk kunnen worden gesteld. Dan is het leed echter al geschied. Een zorgplicht voor fabrikanten – voor levering van veilige hard- en software aan burgers, bedrijven en overheid – kan leiden tot een vooraf beschermen alsook tijdig en snel leveren van eventuele updates en patches.

De zwakste schakel

De rapporten en de aanbevelingen zijn er. Nu is het te bezien hoe de CEO's en de bestuurders dit gaan oppakken hoe deze aanbevelingen georganiseerd worden. De sterke schakel is dat er voldoende kennis en kunde aanwezig is om Nederland voldoende cyberveilig te houden en nog cyberveiliger te krijgen. Fabrikanten kunnen meer doen om cybersecure en cybersafe producten te ontwikkelen. 'De zwakste schakel in de cyberketen is de mens. Maar dat is niet per se de gebruiker. Het kan ook de ontwerper van de beveiliging van het informatiesysteem zijn' (8). Het op peil houden van de cyberawareness voor burgers c.q. consumenten c.q. werknemers is van groot belang. Er zal maar dat ene mailtje met malware binnenkomen; hopelijk wordt dat niet geopend.
De soft controls goed realiseren blijft altijd het lastigst en probeer de boodschap positief over te brengen. En, o ja, denk niet aan de smaak van citroen.

Referenties

(1) AR (2019), https://www.rekenkamer.nl/onderwerpen/ict-en-digitalisering

(2) WRR (2019), Voorbereiden op digitale ontwrichting (rapport nr. 101, 2019) Den Haag; wrr.nl/adviesprojecten/digitale-ontwrichting

(3) CSR (2021), Integrale aanpak cyberweerbaarheid, Advies 2021, nr. 2, Den Haag; cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

(4) RvS (2021), Digitalisering - wetgeving en bestuursrechtspraak, Den Haag, p. 116-117; raadvanstate.nl/publicaties/studies-onderzoeken/

(5) IvhO (2021), Binnen zonder kloppen - digitale weerbaarheid in het hoger onderwijs, Utrecht

(6) Kamerstukken II, 2021/22, 31 288, 31 524 en 26 643, nr. 922

(7) OvV (2021), Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix, Den Haag; onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software-lessen-naar-aanleiding-van

(8) Kok, T. de (2021), De zwakste schakel in de cyberketen kan ook de ontwerper zijn! agconnect.nl/blog/de-zwakste-schakel-de-cyberketen

Lexicon

Informatiebeveiliging is het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit en ook het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen (1).
Cybersecurity alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of te herstellen als die toch is ontstaan. Voorbeelden van schade zijn dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen.
Datasecurity gaat over de bescherming gedurende de gehele lifecycle van digitale informatie tegen bedoelde of onbedoelde aanpassing, verwijdering, diefstal of openbaarmaking van data door ongeautoriseerde personen.
Cybersafety kent twee betekenissen:

1. De veiligheid en betrouwbaarheid van het geautomatiseerde systeem: dat componenten betrouwbaar werken en hun functies kunnen vervullen om, bijvoorbeeld, beschermd te zijn tegen oververhitting (2) en
2. Cybersafety is kort gezegd online veilig zijn. Cybersafety helpt je met het ontwijken van gevaren, maar helpt je ook je te beschermen tegen de gevolgen ervan. Je kunt namelijk niet alles ontwijken. Sommige aanvallen overkomen je, hoewel je aan alle gangbare beveiligingseisen voldoet (3).

Referenties

(1) Art. 1 onder k Besluit CIO-stelsel Rijksdienst 2021

(2) Fraunhofer magazine 3, 2021, p. 44: fraunhofer.de/s/ePaper/magazine/2021/03/index.html

(3) https://www.utwente.nl/nl/cyber-safety/cybersafety/

Kleine catalogus van cyberrisico's [1,2]

Cybercriminaliteit in enge zin
Het gebruik van informatiesystemen en computers niet alleen als middel, maar ook als doel. Bijvoorbeeld computers beschadigen, spamaanvallen, DDoS-aanvallen, virussen verspreiden.
Cybercriminaliteit in brede zin
Dit zijn alle strafbare activiteiten waarbij iemand een informatiesysteem of computer gebruikt. Denk aan diefstal en vervalsing van betaalpassen, oplichting, afpersing, kinderporno, racisme en belediging.
Georganiseerde cybercriminaliteit
Criminele netwerken die gebruik maken van IT, waarbij dat gebruik invloed heeft op hun criminele bedrijfsprocessen, maar meestal zonder enige ideologische achtergrond.
Dit kan theoretisch worden onderscheiden in: (3, 4)

– Traditionele georganiseerde criminaliteit, dat wil zeggen zaken zonder een sterke IT-component. Het gaat dan om gevallen van offline drugshandel, mensenhandel/-smokkel en andere (combinaties van) misdrijven;
– Traditionele georganiseerde criminaliteit met IT als belangrijk vernieuwend element in de modus operandi, zoals zaken van door IT gefaciliteerde drugshandel/-smokkel en een zaak waarin het witwassen van Bitcoins centraal staat.
– Georganiseerde low-tech cybercriminaliteit, waartoe skimming en phising wordt gerekend bij de low-tech cybercriminaliteit; hierbij maken daders gebruik van contacten die ze hebben in het criminele milieu;
– Georganiseerde hightech cybercriminaliteit: zaken als banking malware; kernleden van het criminele samenwerkingsverband de benodigde technische expertise verschaffen door het gebruik van forums.

Cyberterrorisme
Terroristische activiteiten die digitaal worden uitgevoerd, met (enige) ideologische achtergrond. Bijvoorbeeld het beschadigen of uitschakelen van belangrijke informatienetwerken via internet.
Cyberspionage
Het binnendringen van digitale systemen voor het verkrijgen van vertrouwelijke informatie, vaak strategisch, economisch of militair van aard, veelal door staten of (staats)bedrijven.
Cyberoorlog/cyberwar(fare)
Digitale (genetwerkte) technieken die gebruikt worden om de systemen van staten of organisaties aan te vallen. Vaak met een militair of strategisch doel.

Referenties

(1, 2) Verder ontwikkeld en geïnspireerd op:
Gaycken, S. (2015) Cybersecurity – Kleiner Katalog der Cyberrisiken. In: Jäger, T. (eds) (2015) Handbuch Sicherheitsgefahren. Globale Gesellschaft und internationale Beziehungen, Wiesbaden Springer, p. 230 en het Cyberveilig Nederland i.s.m. Cybersecurity Alliantie (2021). Cybersecurity Woordenboek : van cybersecurity naar Nederlands, 3e druk

(3) Kruisbergen, E. W., Leukfeldt, R., Kleemans, E. R., & Roks, R. (2018). Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit. (Cahier; Vol. 2018, No. 8). WODC.

(4) Kruisbergen, E. W., Leukfeldt, R., Kleemans, E. R., & Roks, R. (2018). Criminele geldstromen en ICT: over innovatieve werkwijzen, oude zekerheden en nieuwe flessenhalzen. WODC: Justitiële Verkenningen 44(5), 23-39.

Enkele kwetsbaarheden

DigiNotar (2011)
DigiNotar was een publicly trusted Certificate Authority (CA)en verzorgde de beveiliging van de elektronische communicatie door en tussen overheden (de zgn. Public Key Infrastructure of PKI). In 2011 werd dit bedrijf gehackt. Hierdoor kreeg een externe partij de mogelijkheid valse SSL-certificaten uit te geven en werden de certificaten onbruikbaar.

WannaCry (2017)
WannaCry (ook WannaCrypt, WanaCrypt0r 2.0 of Wanna Decryptor) is een ransomware ontwikkeld voor het Microsoft Windows besturingssysteem. WannaCry bestaat uit twee componenten: een ransomwarecomponent en een worm. Een uitbraak van dit ransomware heeft plaatsgevonden en het besmette daarbij meer dan 230.000 computers in 150 landen. Door de cyberaanval WannaCry viel een deel van de Britse gezondheidszorg uit.

NotPetya (2017)
NotPetya legde de productie van belangrijke medicijnen plat en kostte één van de grootste containerrederijen ter wereld honderden miljoen euro's.

Universiteit Maastricht (2019)
Cyberaanval waardoor de goede voortgang van het onderwijs en onderzoek tijdelijk in gevaar was. Tien dagen was de universiteit digitaal op slot waardoor medewerkers en studenten geen gebruik konden maken van het netwerk en de ICT-diensten van de universiteit.

Citrix (2020)
Ernstige kwetsbaarheid in 2 Citrix-servers: Citrix ADC en Citrix Gateway. Door deze kwetsbaarheid in het Citrix-systeem kunnen hackers toegang krijgen tot het computersysteem van uw organisatie.

Hof van Twente (2020)
Criminelen kwamen de systemen van de gemeente Hof van Twente binnen via een openstaande RDP-poort die kan worden gebruikt voor beheer op afstand. Door middel van een bruteforceaanval ofwel het proberen van grote hoeveelheden gebruikersnaam/wachtwoord-combinaties, kregen de aanvallers toegang tot een van de servers met een testbeheerdersaccount.

SolarWinds Orion (2021).
Volgens SolarWinds is de kwetsbaarheid opzettelijk gecreëerd door een actor, met als achterliggend doel om de systemen te compromitteren van de afnemers van de betreffende versie van SolarWinds Orion. Deze kwetsbaarheid kan door kwaadwillenden worden misbruikt om toegang te krijgen tot bijvoorbeeld informatie of beheersfuncties van organisaties.

Log4J (2021)
Een Denial-of-Service-kwetsbaarheid van in Apache Log4j. Dit is software die veel gebruikt wordt in webapplicaties en allerlei andere systemen. Het is een Log4Shell-gat in Java-tool Log4j. Ontwikkelaars gebruiken die logbestanden om te kijken of hun programma's naar behoren functioneren. Door de registraties te manipuleren kunnen hackers Log4J hun eigen, kwaadaardige code laten downloaden en uitvoeren.

Rode Kruis (2022)
Het Internationale Comité van het Rode Kruis (ICRC) in Genève (Zwitserland) werd slachtoffer van een geavanceerde cybersecurityaanval. Daarbij werden van zeker 515.000, vaak kwetsbare mensen de privégegevens weggenomen. De data is over de hele wereld gestolen, ook bij lokale verenigingen van het Rode Kruis.

Nederlandse securitycentra

NCSC
Het Nationaal Cyber Security Centrum (NCSC) is, met het oog op het voorkomen en beperken van maatschappelijke ontwrichting door cyberdreigingen en -incidenten en het versterken van de digitale weerbaarheid van de samenleving, belast met:

a. het informeren, adviseren en bijstaan van de rijksoverheid en vitale aanbieders in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen;
b. het informeren van anderen;
c. het verrichten van analyses en technisch onderzoek naar aanleiding van cyberdreigingen en -incidenten;
d. het aan anderen verstrekken van analyses verkregen informatie over dreigingen en incidenten betreffende andere netwerk- en informatiesystemen;
e. de taken van het centraal contactpunt, bedoeld in de Wet beveiliging netwerk- en informatiesystemen;
f. het bevorderen en voeren van het secretariaat van de publiek-private samenwerking op het gebied van cybersecurity.

DTC
Het DTC waarschuwt niet-vitale bedrijven wanneer er sprake is van specifieke, ernstige cyberdreigingen. Dit zijn actuele cyberaanvallen of kwetsbaarheden in bedrijfsapplicaties die een grote kans op misbruik hebben en potentieel veel schade kunnen aanrichten.

Het DTC en NCSC vormen samen met verschillende sectorale computercrisisteams en schakelorganisaties het groeiende Landelijk Dekkend Stelsel (LDS) van cybersecurity- samenwerkingsverbanden

CSIRT

De taken van een Computer Security Incident Response Teams zijn onder andere:

- reageren op incidenten die vrijwillig of verplicht worden gemeld;
- incidenten op nationaal niveau monitoren, aanbieders vroegtijdig waarschuwen en informatie over risico's en incidenten verspreiden;
- deelnemen aan het internationale netwerk van CSIRT's en
- op samenwerking gerichte contacten onderhouden met de particuliere sector.

Het CSIRT-DSP is het nationale Cyber Security Incident Response Team voor digitale dienstverleners.

CERT

Een Computer Emergency Response Team (CERT) is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen. Naast reactie op incidenten richt een CERT zich ook op preventie en preparatie.

Er is een aantal sectorale CERT's: Z-CERT voor zorginstellingen, SURFcert voor onderwijsinstellingen, IBD voor gemeenten en WM-CERT voor waterschappen.
Daarnaast bestaan er Organisaties die Kenbaar Tot Taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten (OKTT's)

SOC

Een Security Operations Center (SOC) is een eenheid, die binnen de organisatie monitort om inzicht en grip te hebben op de digitale infrastructuur binnen uw organisatie en op wat daarbinnen allemaal gebeurt. Vanuit applicaties en apparaten wordt loginformatie verzameld en onderzocht op mogelijke aanvallen. Door correlatie van gegevens wordt bepaald of er afgeweken wordt van de standaard. De loginformatie is afkomstig van verschillende bronnen zoals servers, firewalls, (web)applicaties, infrastructurele componenten en endpoint-protectiesystemen.

SIEM

Een hulpmiddel dat onlosmakelijk verbonden is met een SOC is een Security Information & Event Management (SIEM) systeem. Het betreft software die in staat is om loginformatie vanuit verschillende bronnen te interpreteren en te correleren naar wat zich binnen en rondom het netwerk afspeelt op gebied van cyberaanvallen en andere beveiligingsincidenten.

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.

MS Teams niet te gebruiken voor gevoelige informatie!

Aldus een rapport opgesteld door Privacy Company in opdracht van onder meer het Nederlandse ministerie van Justitie en Veiligheid. Tweakers berichtte daarover op 22 februari 2022 (1). De essentie: er bestaat een 'hoog risico' voor de bescherming van gevoelige (persoons)gegevens van EU-burgers, gebaseerd op de omstandigheid dat Microsoft een Amerikaans bedrijf is.

Naast MS Teams zou dit ook opgaan voor de OneDrive-dienst (cloud-opslag) en SharePoint, echter voor de twee laatstgenoemde diensten zou Microsofts 'Double Key Encryption' het risico matigen, hetgeen een eigen encryptiesleuteltoepassing inhoudt boven op de bestaande product/dienst-encryptie. Ook voor MS Teams wordt deze oplossing geadviseerd. Het Data Protection Impact Assessment (DPIA)-rapport bespreekt ook – het aldaar als minder ernstig risico geclassificeerde korte doorgifte van telemetriegegevens naar de V.S. – de analytische en de personeel volgsystemen.

Ander software van Microsoft die door de Privacy Company geanalyseerd werden, zijn o.a. Windows 10 Enterprise en Microsoft Office, waar eveneens aanpassingen volgden nadat de Rijksoverheid en haar Strategisch Leveranciers Management (SLM) in gesprek waren gegaan met Microsoft. Doel: het kunnen blijven gebruiken van die software en wel door ze binnen het kader van de General Data Protection Regulation (GDPR), hier te lande dus de Algemene Verordening Gegevensbescherming (AVG), te brengen. Tweakers besluit haar artikel met de aanhaling van de conclusie dat Microsoft meer aanpassingen heeft te realiseren met het oog op de overblijvende risico's.

Europa en onafhankelijkheid – Chris de Vries

Oorlog in Oekraïne, cyberwar en '*a human-centred and ethical development of digital and industrial technologies 2022* '(2) … eh ….? Denkt u en wat heeft dat te maken met MS Teams en het DPIA-rapport? De titel die wordt aangehaald betreft een zogenoemde oproep (`call') van de Europese Unie die als zorg onder andere uitspreekt: '*This raises concerns about its digital sovereignty in crucial domains such as digital interaction services that are being adopted by a growing number of European users and industries.*' Verder een doelstelling zoals: '*Leadership in AI based on trust*' alsook een zorg: '*Distrust in the internet is causing people to change the way they behave online, for example by disclosing less personal information. Users also express an increasing level of distrust of social media platforms.*'; terwijl als ideaal beeld staat: '*The solutions will benefit from the increasing will of citizens to participate in the sharing economy* (alle cursiveringen door de auteur).'

Hier een tegenspraak in het menselijk gedrag versus de wensen van de Europese Unie. Dit nu, gevoed door de oorlog in Oekraïne, waardoor Facebook besloot Oekraïense gebruikers de optie te geven om hun profiel met één klik te laten blokkeren, zoals eerder voor Afghaanse gebruikers (08.2021) (3). Verder zien wij dat de Oekraïense overheid hackers oproept om deel te gaan nemen in offensieve en defensieve teams tegenover Rusland (4). Dus wij hebben een hete – en een cyberoorlog met repercussies in de ICT-werkelijkheid.

En wat zou een constatering kunnen zijn uit het DPIA-rapport? Dát, de Europese Unie te afhankelijk is van buitenlandse empires (Amerika, China, Rusland)!? Dát, als puntje bij paaltje komt, de Europese Unie - met haar democratische normen, haar mens-georiënteerde en ethi-

Chris de Vries | Fook Hwa Tan | Maarten Hartsuijker

sche ontwikkeling - van de ene op de andere dag weggevaagd kan worden!? En dát, als zij niet werkt aan hard- en softwarematige onafhankelijkheid, besluitende haar gevoelige (persoons)gegevens binnenshuis te houden? Laten wij onze Europese idealen handhaven, maar niet als Chamberlain, destijds, geloven in vrede, terwijl de tanks al zichtbaar aan komen rijden.

Wat zijn de alternatieven! – Fook Hwa Tan

Initieel kwam de uitgevoerde DPIA als een schok binnen. Een veelgebruikt programma zou opeens niet meer te gebruiken zijn vanwege privacyoverwegingen. De DPIA was initieel uitgevoerd om impact van het delen en opslaan van persoonsgegevens te wegen. Het resultaat voelt alsof je helemaal geen data meer mag delen met Microsoft. Wat nu? Er zijn hier en daar wat alternatieven, maar sinds covid-19 heeft de Microsoftoplossing een nog verdere vlucht genomen in alle opzichten. Of het nou gaat om een productiviteit suite, videoconferencing software, planningssoftware en heel veel andere integraties. Microsoft heeft gezorgd dat haar software erg veelzijdig is geworden, waardoor er veelvuldig gebruik van gemaakt wordt. Als je navraag doet naar de beveiliging van de software, die je van deze leverancier wilt gebruiken, krijg je toegang tot een bos aan certificaten en beveiligingsrapporten, waarin kwetsbaarheden, maar natuurlijk ook de beveiliging netjes is beschreven. Afhankelijk van je eigen risicobereidheid kun je niet klagen. Wel natuurlijk dit geconstateerde issue; dat het mogelijk nog niet helemaal voldoet aan de AVG. Natuurlijk wil je best wel kijken naar een alternatief. Maar welk alternatief is gebruikersvriendelijk, integreert met allerlei software en wordt veelvuldig gebruikt, wat niet van Amerikaanse makelij is? Die zijn nog niet zo makkelijk te vinden. Het enige dat je dan overhoudt is dan het risico te accepteren en te wachten op verbetering van de leverancier of aangepaste regels. Je kunt natuurlijk ook nieuwe software implementeren specifiek voor het delen van persoonsgegevens, maar daar krijg je waarschijnlijk de businesscase niet voor rond. Dus nog even wachten?

Behoefte aan richting – Maarten Hartsuijker

Hoe goed ik het signaal ook vind: adviseren geen gevoelige data bij Microsoft op te slaan, voelt een beetje als mosterd na een maaltijd die al jaren voorbij is. Laten wij even in ons collectieve geheugen graven. Voor Edward Snowden waarschuwden wij, professionals, in overvloede voor het gat tussen 'safe harbor' en de werkelijkheid. Als we het niet voorzichtig genoeg brachten kregen we aluminium hoedjes cadeau. Toen was er Edward Snowden. We hoefden niets meer uit te leggen. Ineens kregen wij vragen wat de organisatie met deze 'nieuwe werkelijkheid' moest. Dat bedaarde al snel. Want serieuze alternatieven waren er vaak niet. Dus werd het devies: 'Zolang de overheid zelf niets doet, kijken wij het ook even aan'. Over privacyshield wil ik het eigenlijk niet eens hebben. Iedereen wist dat het niets oploste. Maar iedereen deed alsof de Safe Harbor-issues ermee verdwenen. En toen hadden we Schrems. En weer Schrems. De privacytoezichthouders morden hier en daar wat, maar nog altijd merk je vanuit de overheden vrij weinig echte actie. Door covid zijn inmiddels ook de laatste 'terughoudende' organisaties de cloud ingestapt. Geen keus meer. En in die cloud kun je voor goed werkende IAAS kiezen uit Amazon, Microsoft, Google en nog wat randverschijnselen er omheen. Goed werkende Office diensten: Microsoft en dan heel lang niets. Videobellen, Microsoft, Google, Zoom en dan heel lang niets. CRM: Salesforce, Dynamics. Krijgt een Europees idee succes (Elastic, Booking, Blueconic…), hap… slik… weg...

Ik weet niet goed wat het SLM Rijk en Privacy Company met de publicatie van hun interne onderzoek beogen. Inhoudelijk brengt het niets nieuws. Waar echt behoefte aan is, is richting. Voldoen we nu met elkaar aan de wet als een cloudbeheerder (indirect) toegang tot onze (klant)data heeft, of niet? En helpt versleuteling met eigen encryptiesleutels eigenlijk wel bij een bedrijf dat ook jouw IDP is? Of is deze maatregel een 'privacyshield' waar we veel geld instoppen om onszelf weer een paar jaar voor de gek te houden dat het er veiliger van wordt? En als dit niet het geval is: moeten overheden dan niet het goede voorbeeld geven? Als overheden zelf niet acteren op onderzoek in eigen gelederen, kun je dan van de rest van het continent verwachten dat ze hun bedrijfsvoering stilleggen door dit wel te doen?

Referenties

(1) https://tweakers.net/nieuws/193528/advies-aan-nederlandse-overheid-gebruik-ms-teams-niet-voor-gevoelige-informatie.html

(2) https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2022-human-01-19;callCode=null;freeTextSearchKeyword=eXtended%20Reality%20Learning%20-%20Engage%20and%20Interact%20%28IA%29;matchWholeText=true;typeCodes=0,1,2,8;statusCodes=31094501,31094502,31094503;programmePeriod=null;programCcm2Id=null;programDivisionCode=null;focusAreaCode=null;destination=null;mission=null;geographicalZonesCode=null;programmeDivisionProspect=null;startDateLte=null;startDateGte=null;crossCuttingPriorityCode=null;cpvCode=null;performanceOfDelivery=null;sortQuery=sortStatus;orderBy=asc;onlyTenders=false;topicListKey=topicSearchTablePageState

(3) https://tweakers.net/nieuws/193660/facebook-laat-oekraiense-gebruikers-profiel-blokkeren-met-enkele-klik.html?utm_source=nieuwsbrief&utm_medium=-email&utm_campaign=twk_nieuwsbrief

(4) https://tweakers.net/nieuws/193665/oekraine-roept-oekraiense-hackers-op-te-helpen-bij-zijn-cyberveiligheid.html?utm_source=nieuwsbrief&utm_-medium=email&utm_campaign=twk_nieuwsbrief

15 PvIB reconnect in cyber security

COLOFON

iB is het huisorgaan van het Platform 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

(Advertorial)

REUZADO INTRODUCEERT DATAVERNIETIGING OP LOCATIE

Reuzado is gespecialiseerd in het veilig inzamelen, vervoeren en vernietigen van data en datadragers. Elke stap in dat proces voldoet aan strenge eisen, is 100% beveiligd en milieuvriendelijk. Zelfs de minuscule, onbruikbare snippers die overblijven na het vernietigen van datadragers worden zoveel mogelijk op duurzame wijze gerecycled. Het is nu ook mogelijk om data en datadragers op het terrein van de klant te vernietigen.

Wat zijn de voordelen:

- Transport is overbodig; voor bepaalde branches een must;
- De klant, of een bevoegde controleur, kan ter plekke vaststellen dat de datadragers en/of data definitief zijn vernietigd;
- Iedere stap in dat proces wordt gedocumenteerd;
- De klant ontvangt van elke vernietigde datadrager een vernietigingsbewijs met serienummer;
- Reuzado garandeert dat vernietiging 100% veilig en volledig heeft plaatsgevonden;
- Het vernietigen van data en/of datadrager wordt altijd door eigen personeel uitgevoerd.

Meer weten?

Meer weten over mobiele datavernietiging of de andere diensten van Reuzado ICT Services? Neem dan contact met ons op via e-mail (circulair@reuzado.nl) of telefonisch via 023 5519821. De medewerkers leggen graag uit wat er mogelijk is. Reuzado staat voor transparante communicatie, glasheldere offertes en 100% veilige datavernietiging.

Over Reuzado

Reuzado, Esperanto voor 'hergebruik', is dé expert voor alles op het gebied van ICT. Het bedrijf is ISO 9001 gecertificeerd en alle werkzaamheden worden verricht conform DIN 66399. Op dit moment wordt gewerkt aan zowel ISO 14001 als ISO 27001 certificering en Weeelabex/Cenelec 50625. Voor meer informatie: https://reuzado.nl/

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