INFORMATIEBEVEILIGING MAGAZINE

- NIS2: Versterken van Digitale Veiligheid in Europa's Cyberspace
- Risico's vinden en erover communiceren
- Privacycolumn: Op de evenwichtsbalk

JAARGANG 23 - 2023 - EDITIE 5

ISOPlanner **event**

Eenvoudig Compliance Management in **Microsoft 365**

In het kort

ISOPlanner is de enige integrale compliance oplossing in Microsoft 365: jouw beleid staat in SharePoint en alle activiteiten kunnen direct in Outlook worden gepland of via Teams worden afgehandeld. ISOPlanner brengt ISO naar jouw medewerkers toe. Uiteraard ook voor de overheid (BIO), zorg (NEN7510) en de NIS2.

Compliance automatisering

Het volgen van het juiste proces en het daarbij automatisch verzamelen van bewijsmateriaal via Power Automate zorgt voor minder werk en een efficiënte audit. ISOPlanner bespaart jou en je collega's tijd en zorgt daarmee voor betere acceptatie en borging van informatiebeveiliging in de organisatie.

Kom naar het event op 24 november

Op vrijdagmiddag 24 november, op een mooie locatie rond Utrecht, staat het thema "Compliance Automation" centraal. Neem deel aan discussies met auditors en andere experts op dit gebied.

Meld je nu aan op isoplanner.app/event. Deelname is gratis.

Eenvoudig en toegankelijk

Automatisering is de toekomst

Vertrouwd

Vakantiebezinningen

Chris de Vries

Voor de meesten van ons is de vakantie weer voorbij. Sommigen hebben deze zomer kunnen genieten van mooi weer, maar anderen hebben bar slecht weer over zich heen gekregen. Zo hoop ik dat je niet in Noord-Italië was toen hagel- en onweersbuien het land teisterden.

De vakantie hoort altijd een periode te zijn van tot rust komen, bezinning, genieten van het mooie dat we om ons heen waarnemen. En na de vakantie is het weer werken, wellicht stressen en van hot naar … ja, eigenlijk waarnaartoe rennen? Om deze sleur nog even uit te stellen adviseer ik je deze uitgave van IB Magazine aandachtig te lezen.

Vanuit BDO is er een NIS2-overzichtsartikel geschreven. In het komende jaar zal hier weer de nodige aandacht aan besteed worden en zullen organisaties hun beleid moeten aanscherpen. André Beerten heeft het over eigenaarschap en dan met name het opsporen van risico's en daar op de juiste manier over communiceren. Met zijn bekende directheid spoort hij jou als lezer aan de handschoen op te pakken en met elkaar en met hem van gedachten te wisselen over ons mooie vak en de daarbij behorende verantwoordelijkheden.

Dimitri van Zantvliet gaat in zijn blog even terug in de tijd en bespreekt het ontstaan van de functie van Change Agent, terwijl Abel Hoogeveen filosofeert over wie eigenlijk de in de mode zijnde GPT-modellen bezit. Dat artikel maakt duidelijk dat technologische innovatie bijna altijd gelijk opgaat met juridische consequenties.

Artikelen die stuk voor stuk stimuleren weer met frisse zin aan het werk te gaan: aan het eind van de zomer met aan de horizon alweer het begin van de herfst. Ook als redactieleden zijn of komen we binnenkort weer terug van vakantie. We hebben dit jaar nog één uitgave te gaan en we bestuderen al hoe we 2024 zullen gaan aanpakken. Meer daarover in de laatste uitgave van dit jaar.

Als blogschrijvers, auteurs en redacteuren blijven we altijd nieuwsgierig naar jullie reacties op onze artikelen en de onderwerpen die we behandelen in het magazine. We nodigen je daarom uit om ons te schrijven, te mailen of commentaar te leveren via LinkedIn. Verbetering en verdere professionalisering van het magazine staat niet alleen op het wenslijstje van het PvIB-bestuur, maar ook op dat van ons en van de auteurs die voor jullie en ons schrijven.

Schrijf dus ook eens, al is het een vakantiekaartje!

Chris

IN DIT NUMMER

Auteurs: Alle auteurs zijn werkzaam bij BDO. Rick van Dijk MSc RE CISA CISM CISSP CCSP, Sr. manager Cyber Security, BDO Digital, bereikbaar via: rick.van.dijk@bdo.nl. Mr. Ronald Westerveen, Senior Manager Cybersecurity, bereikbaar via: Ronald.westerveen@BDO.nl. Jeremy Costa Pires, Junior adviseur, bereikbaar via: jeremy.costapires@bdo.nl.

NIS2: Versterken van Digitale Veiligheid in Europa's Cyberspace

Nieuwe Europese wetgeving vereist proactieve cyberbeveiligingsmaatregelen

In een tijd van groeiende digitale afhankelijkheid en toenemende cyberdreigingen heeft de Europese Unie de Network and Information Security Directive herzien, resulterend in NIS2. Deze richtlijn, van kracht sinds januari 2023, versterkt de digitale weerbaarheid van lidstaten. Organisaties moeten zich voorbereiden op de eisen die in januari 2025 van kracht worden. Dit artikel onderzoekt de cruciale elementen van NIS2 en hoe organisaties er proactief aan kunnen voldoen, hun digitale veerkracht kunnen vergroten en de Europese digitale veiligheid kunnen verbeteren.

In het afgelopen decennium heeft een reeks ontwikkelingen geleid tot een toenemende druk op de digitale veiligheid van onze samenleving en economie. Dit is een gevolg van factoren zoals COVID-19, de voortdurende digitale transformatie en de groeiende dreiging van cyberaanvallen. Organisaties zijn steeds afhankelijker geworden van data en hebben zich ontwikkeld tot overwegend digitaal georiënteerde entiteiten. Deze afhankelijkheid gaat gepaard met het delen en verwerken van gegevens, wat het risico op ernstige bedrijfsstoringen verhoogt als deze gegevens of de bijbehorende verwerking niet beschikbaar zijn.

Bovendien worden deze gegevens niet alleen intern opgeslagen en verwerkt, maar ook bij hostingpartijen - cloudleveranciers - en gedeeld met diverse ketenpartijen, zoals leveranciers, dienstverleners en toezichthouders. Hoewel samenwerken met deze partners de focus op de kernactiviteiten van een organisatie vergroot, vereist het ook een centrale sturende rol in de beveiliging en betrouwbaarheid van de digitale gegevens.

Als reactie op deze dynamische ontwikkelingen heeft de Europese Unie sinds 2020 gewerkt aan de herziening van de Network and Information Security Directive (NIS) - de NIS2. Deze vernieuwde richtlijn trad op 16 januari 2023 in werking met als doel de digitale veerkracht van de lidstaten binnen Europa te versterken. Vanaf januari 2025 moeten organisaties die onder de NIS2 vallen, voldoen aan de eisen van deze wetgeving. Hoewel deze datum wellicht nog ver in de toekomst lijkt, bieden ervaringen met eerdere regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), waardevolle lessen over het belang van tijdige voorbereiding.

De NIS2 fungeert bovenal als een stimulans om de cyber- en informatiebeveiliging in de hele Europese Unie naar een hoger niveau te tillen - een doel dat elke organisatie zou moeten

omarmen. In dit artikel zullen we verkennen hoe organisaties proactief kunnen inspelen op de NIS2-vereisten. Bijvoorbeeld door de implementatie van ISO27001-richtlijnen, waarmee ze niet alleen aan de wetgeving voldoen, maar ook hun algehele digitale veerkracht versterken.

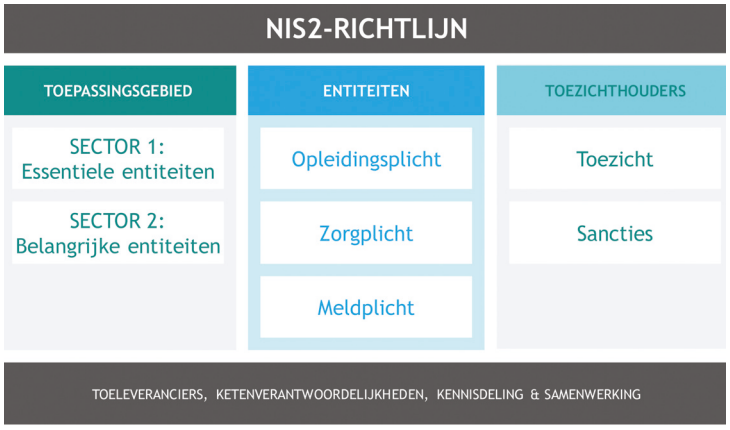
Wat is NIS2?

De NIS2-richtlijn, oftewel de 'Network and Information Security Directive', is de opvolger van de NIS-richtlijn: een belangrijke set regels en richtlijnen die bedoeld zijn om de digitale veiligheid en stabiliteit van essentiële diensten in de EU-lidstaten te waarborgen. De NIS2-richtlijn is opgesteld om ervoor te zorgen dat organisaties die vertrouwen op digitale systemen - zoals computers, netwerken en online diensten - robuuste beveiligingsmaatregelen implementeren. Ook streeft NIS2 naar het opzetten van een gemeenschappelijk kader voor de beveiliging van deze systemen, vooral die van kritieke sectoren zoals energie, transport, financiën en gezondheid. Dit is van cruciaal belang omdat cyberdreigingen, zoals hackers, malware en andere schadelijke activiteiten, steeds geavanceerder worden en de essentiële digitale infrastructuur kunnen verstoren of beschadigen.

De NIS-richtlijn is door de Nederlandse staat verwerkt naar nationale wetgeving. De Wet Beveiliging Netwerk- en Informatiesystemen (WBNI) is de Nederlandse wet die is opgesteld om te voldoen aan de verplichtingen van de NIS-richtlijn. De WBNI vertaalt de eisen en principes van de NIS-richtlijn naar nationale wetgeving en is bedoeld om de digitale veiligheid in Nederland te versterken. Met het herzien van de NIS-richtlijn ligt er dus een herziening van de WBNI in het verschiet en zullen herziene elementen uit de richtlijn nader moeten worden ingevuld of uitgewerkt. De omzetting en uitwerking van de NIS2-richtlijn in nationale wetgeving dient eind 2024 gereed te zijn, zodat entiteiten per januari 2025 kunnen en moeten voldoen aan de NIS2.

De NIS2-richtlijn omvat verplichtingen voor de Nederlandse staat om deze te verwerken naar nationale wetgeving, maar tevens verplichtingen om nadere invulling en verwerking vorm te geven. Bijvoorbeeld door het optuigen van toezicht en verantwoordingsstructuur, het faciliteren in een meldpunt voor incidenten (bij een zogeheten CSIRT – Computer Security Incident Response Team) en het faciliteren van samenwerkingen en kennisdeling.

Voor wie/wat is de NIS2 van toepassing?



Figuur 1: overzicht werking NIS2-richtlijn.

De NIS2 richt zich op organisaties die als essentieel of belangrijk worden beschouwd voor de continuïteit van vitale diensten en de digitale infrastructuur. Meer specifiek geldt dit voor die sectoren en diensten die van vitaal belang zijn voor belangrijke maatschappelijke en economische activiteiten.

De NIS2 is uitgebreider dan de NIS-richtlijn en beslaat een groter aantal organisaties waarop de richtlijn van toepassing is. De NIS maakt een onderscheid tussen essentiële en belangrijke entiteiten, verdeeld over twee categorieën/sectoren. Of een entiteit binnen een categorie/sector valt en wordt aangewezen

als essentieel of belangrijk, wordt mede bepaald door de omvang van de organisatie. Echter, wanneer een organisatie niet aan deze criteria voldoet, betekent dit niet dat deze niet hoeft te voldoen aan de NIS2. De Nederlandse overheid moet ervoor zorgen dat ook kleine ondernemingen en micro-ondernemingen voldoen aan de NIS2-richtlijn, wanneer deze een sleutelrol spelen in de samenleving of economie.

Hieronder staan de criteria die bepalen of een organisatie als belangrijk of essentieel wordt beschouwd:

SECTOREN - BIJLAGE I	SECTOREN - BIJLAGE II
Energie	Digitale aanbieders
Transport	Post- en koeriersdiensten
Bankwezen	Afvalstoffenbeheer
Infrastructuur	Levensmiddelen
Gezondheidszorg	Chemische stoffen
Drinkwater	Onderzoek
Digitale infrastructuur	Vervaardiging/manufacturing
Beheerders van ICT-diensten	
Afvalwater	
Overheidsdiensten	
Ruimtevaart	
Beheer van ICT-diensten	

Figuur 2: essentieel en/of van belang zijnde beoordelingscriteria.

Essentiële entiteiten zijn grote organisaties die actief zijn in een sector uit Bijlage I van de NIS2-richtlijn. Een organisatie is groot op basis van de volgende criteria: minimaal 250 werknemers of een jaaromzet van vijftig miljoen euro of meer en een balanstotaal van 43 miljoen euro of meer.

Belangrijke entiteiten zijn middelgrote organisaties die actief zijn in een sector uit Bijlage I en middelgrote en grote organisaties die actief zijn in een sector uit Bijlage II. Een organisatie is middelgroot op basis van de volgende criteria: vijftig of meer werknemers of een jaaromzet en balanstotaal van tien miljoen euro of meer.

Essentiële of belangrijke organisaties moeten als zodanig worden aangewezen door de Nederlandse overheid en/of toezichthouders die namens hen toezicht houden. Omdat de huidige criteria nog niet verder zijn uitgewerkt, is een expliciete aanwijzing nog niet bekend. Het is echter duidelijk dat de huidige categorisering op basis van de SBI-codering (Standaard BedrijfsIndeling) niet een-op-een zal worden toegepast.

Het is ook mogelijk dat een organisatie die niet aan de bovengenoemde criteria voldoet en niet wordt aangewezen als een essentiële of belangrijke entiteit, toch moet voldoen aan vereisten uit de NIS2. De NIS2 benadrukt namelijk ook de verantwoordelijkheden van een organisatie in de keten en samenwerkingen. Organisaties zonder directe aanwijzing zullen dus door opdrachtgevers of samenwerkingsverbanden de vereisten uit de NIS2 opgelegd krijgen, bijvoorbeeld in contractuele voorwaarden en/of verantwoordingsverplichtingen. Denk hierbij bijvoorbeeld aan een producent van verpakkingsmaterialen voor medische producten of een transporteur van levensmiddelen.

De impact en belangrijke veranderingen als gevolg van NIS 2

Hoewel de volledige uitwerking van NIS2 in nationale wetgeving nog moet worden bekrachtigd en eind 2024 moet worden afgerond, en de definitieve aanwijzing van organisaties die onder de NIS2 vallen nog moet plaatsvinden, is nu al duidelijk welke impact de NIS2 zal hebben en wat deze van organisaties zal vragen. Kort samengevat stelt de NIS2 dat:

- Organisaties moeten voldoen aan een **opleidingsplicht**;
- Organisaties hebben een **zorgplicht** met betrekking tot informatie- en cyberbeveiliging;
- Organisaties hebben een **meldplicht** om incidenten binnen gestelde termijnen te melden;
- Toezichthouders moeten **toezicht** houden en hiervoor informatie verkrijgen van of bij de organisatie;
- (Bestuurders van) organisaties zijn **aansprakelijk**;
- Er kunnen **sancties** worden opgelegd.

Daarnaast benadrukt de NIS2-richtlijn de noodzaak van samenwerking en informatie-uitwisseling tussen organisaties en de overheid om bredere digitale veiligheid te bevorderen. Dit betekent dat je als bestuurder van een organisatie moet begrijpen hoe jouw activiteiten passen binnen het grotere geheel van de digitale veiligheid in jouw sector en in de samenleving als geheel.

Het niet naleven van de NIS2-richtlijn kan niet alleen leiden tot financiële consequenties, maar ook tot reputatieschade en verstoring van de activiteiten van jouw organisatie.

Het niet naleven van de NIS2-richtlijn kan niet alleen leiden tot financiële consequenties, maar ook tot reputatieschade en verstoring van de activiteiten van jouw organisatie. Als bestuurder is het dus van groot belang om de richtlijn serieus te nemen, de nodige maatregelen te implementeren en te zorgen voor een cultuur van digitale veiligheid binnen jouw organisatie. Dit draagt niet alleen bij aan de bescherming van jouw organisatie, maar ook aan die van het algehele, digitale ecosysteem.

Opleidingsplicht

In artikel 20 van de NIS2-richtlijn wordt gesteld dat *'leden van de bestuursorganen een opleiding moeten volgen en daarmee voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.'* Daarnaast wordt gesteld dat wordt aangemoedigd om een soortgelijke opleiding aan werknemers aan te bieden.

Voor deze opleidingsplicht is nog niet bekend of er meer specifieke vereisten aan de opleidingsvorm of -duur zullen worden gesteld. In de markt zijn er al verschillende vormen van opleidingen, van meerdaagse trainingen tot enkele sessies van een paar uur, in-house trainingen tot groepstrainingen op externe locaties en met of zonder opleidingscertificaat. Ook is nog niet expliciet gedefinieerd wat er met 'bestuursorgaan' wordt bedoeld, aangezien dit niet als definitie is opgenomen in de NIS2. Dit kunnen dus de directe bestuurders zijn, de directie en het management, maar ook toezichthoudende functionarissen zoals een raad van commissarissen.

Naar onze mening staat de lengte en inhoud van een dergelijke training dan ook niet voorop, maar het te bereiken resultaat. Daarmee zal de vorm en inhoud dan ook aangepast dienen te worden aan de organisatie en onder meer het kennisniveau van de betreffende bestuursorganen en bestuurders.

Zorgplicht

In artikel 21 van de NIS2-richtlijn wordt de zorgplicht nader gedefinieerd. In dit artikel wordt gesteld dat een organisatie maatregelen moet nemen om zich te beschermen tegen incidenten. Deze maatregelen zijn zeer algemeen gedefinieerd en moeten omvatten:

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b) incidentenbehandeling;
c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van

kwetsbaarheden;
f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Om invulling te geven aan deze maatregelen kan heel goed worden gekeken naar bestaande certificeringen, best-practices en normenkaders, zoals de ISO27001:2022, NIST CSF en diverse sectorspecifieke, afgeleide of gerelateerde kaders. Deze kaders omvatten reeds maatregelen, hierboven benoemd, en kunnen daarmee prima voorzien in 'passende' beveiliging.

Opvallend, in deze maatregelen en relatief nieuw, zijn de vereisten rond beveiliging van de toeleveringsketen en beveiliging bij het verwerven van netwerk- en informatiesystemen. Deze zien expliciet toe op beveiliging in de keten en bij het inkopen van diensten of digitale oplossingen. Aangezien organisaties steeds meer gebruik maken van 'de cloud' is het dus ook belangrijk om toe te zien op veiligheid van deze ingekochte diensten en/of cloudsoftware. Deze normen vragen dus ook om goede kennis en kunde om risico's ten aanzien van toeleveranciers en cloudleveranciers te kunnen beoordelen en vragen om aantoonbare beheersing door deze leveranciers.

Meldplicht

In artikel 23 van de NIS2-richtlijn zijn tijdslijnen gespecificeerd waarbinnen een organisatie incidenten met betrekking tot informatie- en cyberbeveiliging moet melden bij een CSIRT. De Nederlandse overheid heeft vanuit de NIS2-richtlijn de verplichting om een gedegen meldstructuur en een CSIRT op te zetten. Voor een organisatie betekent dit dat binnen 24 uur een vroegtijdige waarschuwing, binnen 72 uur een incidentmelding, een tussentijds verslag en binnen een maand een eindverslag moet worden afgegeven. Deze meldingen zullen door het CSIRT op Europees niveau (geaggregeerd) worden gerapporteerd om zo zicht te houden op de algemene staat van informatie- en cyberbeveiliging en ontwikkelingen (per lidstaat).

Deze meldingsplicht lijkt sterk op de meldingsplicht voor datalekken onder de AVG. Door de daar reeds gebruikte werkwijze te kopiëren, kunnen al de nodige eerste stappen zijn gezet voor het verder invullen van deze vereiste.

Toezicht

In artikel 32 van de NIS2-richtlijn staat beschreven welke instrumenten de toezichthouders mogen toepassen bij toezicht op essentiële, respectievelijk belangrijke entiteiten. Deze variëren van audit en opvragen van informatie door de toezichthouder tot het aantonen van de gehanteerde instrumenten vanuit een onafhankelijke audit. Daarbij wordt beperkt onderscheid gemaakt tussen toezicht op een essentiële of een belangrijke entiteit, maar verwacht kan worden dat de mate van toezicht en de inzet van instrumenten in eerste instantie zal afhangen van de capaciteit van de toezichthouder. Vergelijkbaar aan toezicht op de Algemene Verordening Gegevensbescherming, waarbij de Autoriteit Persoonsgegevens als toezichthouder zich in eerste instantie richtte op 'de grote jongens' en overduidelijke 'overtredingen', mede omwille van beschikbare capaciteit om alle meldingen op te volgen.

In welke mate gesteund kan worden op het aantoonbaar voldoen aan certificeringen, best-practices of normenkaders, zoals de ISO27001:2022, is nog niet bekend. Of het bijvoorbeeld voldoende is om op basis van een self assessment aan te tonen dat passend invulling wordt gegeven aan de zorgplicht of dat een onafhankelijk oordeel nodig is? En of dan een certificering of een assuranceverklaring wordt gevraagd?

Hoe dan ook is duidelijk dat passend invulling moet worden gegeven aan de vereisten uit de NIS2 en dat toezicht om aantoonbaarheid hiervan zal vragen.

Cyberaanvallen wachten niet op nieuwe wetgeving en kunnen in elke fase toeslaan.

Aansprakelijkheid en sancties

In de NIS2-richtlijn worden expliciet de verantwoordelijkheden van bestuursorganen benoemd. Zij moeten maatregelen voor het beheer van cyberrisico's goedkeuren en zijn aansprakelijk voor het niet voldoen aan de zorgplicht. Hierbij wordt gedoeld op persoonlijke aansprakelijkheid. Dit is ook om te voorkomen dat slechts één bestuurder invloed uitoefent op de securitystrategie. Bij bestuurders is er vaak een verdeling van taken en is het nogal eens het geval dat de bestuurder die de informatiebeveiliging en cybersecurity niet in het takenpakket heeft, hier ook niets meedoet en of affiniteit mee heeft, terwijl dit zo langzamerhand (de data in en van een organisatie) welhaast een van de meest essentiële onderdelen is van een organisatie.

Als mogelijke sancties voor het niet voldoen aan de NIS2-richtlijn is een maximale sanctie van tien miljoen euro of twee procent van de wereldwijde jaaromzet voor een essentiële entiteit en een maximale sanctie van zeven miljoen euro of 1,4 procent van de wereldwijde jaaromzet voor een belangrijke entiteit genoemd. Onze verwachting is dat het toekennen van sancties op soortgelijke wijze als bij de AVG zal plaatsvinden en gelijke tred zal houden met de vormgeving van toezicht. Er hoeft niet direct tot boetes als sanctie te worden overgegaan door de toezichthouder. Deze kan ook waarschuwingen of de verplichting tot het oplossen van waargenomen tekortkomingen opleggen aan de organisatie.

Perspectief

Gezien de Network and Information Security Directive 2 (NIS2) wordt het duidelijk dat het versterken van de digitale veerkracht een dringende en voortdurende inspanning vereist. Hoewel de volledige uitwerking van NIS2 in nationale wetgeving nog enige tijd kan vergen, is het van cruciaal belang voor organisaties om nu al proactieve maatregelen te nemen. Het wachten op formele richtlijnen zou een riskante strategie zijn, gezien de voortdurende en steeds geavanceerdere cyberdreigingen.

Organisaties die vooruit willen kijken, dienen niet alleen te voldoen aan de wettelijke vereisten van NIS2, maar ook te investeren in de algehele weerbaarheid van hun digitale systemen. Door zich te concentreren op het implementeren van best-practices zoals ISO27001, het helder definiëren van verantwoordelijkheden en aansprakelijkheden, het uitvoeren van uitgebreide beoordelingen en het opzetten van effectieve monitoring en incidentrespons, kunnen zij een solide basis leggen voor een duurzame en adaptieve digitale beveiligingsinfrastructuur.

De realiteit is dat informatie- en cyberbeveiliging niet kan wachten. Cyberaanvallen wachten niet op nieuwe wetgeving en kunnen in elke fase toeslaan. Door nu al te investeren in beveiligingsmaatregelen, kunnen organisaties veerkracht opbouwen, zich voorbereiden op mogelijke dreigingen en de continuïteit van hun activiteiten waarborgen. NIS2 vormt niet alleen een verplichting, maar ook een kans voor organisaties om zichzelf te versterken in een digitaal landschap dat voortdurend evolueert. Het is tijd om niet langer af te wachten, maar proactief de leiding te nemen in het waarborgen van digitale veiligheid en veerkracht.

Daarnaast is het essentieel om te beseffen dat de impact van NIS2 zich niet beperkt tot alleen de aangewezen organisaties. De gehele keten zal worden getroffen, aangezien cybersecurity een onderling verbonden en gedeeld aspect is binnen moderne bedrijfsvoering. Verplichtingen en verantwoordelijkheden zullen naar verwachting verder doorsijpelen, waardoor het nemen van proactieve maatregelen niet alleen wettelijk vereist is, maar ook nodig om de integriteit en veiligheid van de bredere digitale ecosystemen te waarborgen.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Op de evenwichtsbalk

Op de hei staat een hutje. Verwarmd wordt het door een vuurtje waar ook de maaltijd op wordt klaargemaakt. Volledig zelfvoorzienend 'off-the-grid' en alles 'low-or-no-tech'. Als de bewoners iets nodig hebben wat van buiten komt, proberen ze dat alleen met contanten te betalen en als het kan door middel van goederen- of dienstenruil. Zwaar verzetten de bewoners van dit idyllische hutje op de hei zich tegen alles wat ruikt naar grote technologie die je in de gaten kan houden. En geef ze eens ongelijk, alle incidenten die gepubliceerd worden in de media voeden het negatieve beeld van onze maatschappij en de technologie die het omarmd heeft.

Ik snap de wens om afgesloten te zijn van alles wat inbreuk kan maken op je privacy heel erg goed. Een heel aantal incidenten heeft namelijk flinke impact op de levens van personen. Zeker als het gaat om het inzetten van technologie waar biases in zitten over bijvoorbeeld afkomst. Heel realistisch is het hutje op de hei hierboven echter niet. Hoe dan ook kom je altijd in aanraking met technologie, al was het alleen maar omdat je *burger* bent van een overheid die in toenemende mate de mens uit de keten verwijderd heeft. En misschien ook wel omdat je *werknemer* bent en je moet inklokken of gebruik moet maken van laptops en online beschikbaar gestelde ICT-middelen. In het kader van informatiebeveiliging komt daar vaak ook logging bij kijken.

Helemaal ontlopen kun je die technologie dus niet. Hoe graag je het ook zou willen. Absolute privacy bestaat niet, er spelen altijd ook andere factoren dan alleen privacy mee. Privacy kent daarom niet voor niets een risicogebaseerde aanpak – je kijkt naar een specifieke situatie, brengt de risico's in kaart, scoort die (hoog, midden, laag) en denkt na over hoe je die risico's kleiner kunt maken of zo kunt indammen dat het risico verwaarloosbaar is. Een enkele keer tref je zoveel hoge risico's aan die je bovendien niet kunt indammen. Dan weet je zeker dat je het niet moet doen. Maar zo vaak komt dat niet voor.

Als je privacy als een absolutisme behandelt, loop je onherroepelijk vast. Dus ga je op zoek naar het evenwicht. Waar stopt privacy en gaan andere belangen voor? En, wat vinden we apert onacceptabele risico's waardoor de privacy vooropstaat en de andere belangen daardoor het onderspit delven? Dit vraagt blijvende alertheid van iedereen, want de meest recente grote schandalen op het gebied van privacy kwamen pas naar boven door niet aflatend kritische betrokkenen. Gezond tegenwicht tegen al te datahongerige organisaties is absoluut noodzakelijk. Maar, blijf wel altijd met een echt open blik kijken – want hoe je het ook wendt of keert, technologie als zodanig is niet slecht of goed. Het is het gebruik dat wij er soms van willen maken waar de pijn te vinden is.

Rachel

Auteur: Pieter Muller IAM-/Security consultant, werkzaam bij Dux Group in Rotterdam. Hij staat altijd open voor een gesprek, je kunt hem benaderen via https://nl.linkedin.com/in/pieter-muller-61629563

Een bewuste manager is goud waard

Goud is waardevol, goud is mooi en veel mensen willen het hebben. Als je een medewerker binnen de organisatie aanspreekt en vraagt of goud waardevol is, is het antwoord al snel 'ja'. Dit komt omdat wij als mensen goud kunnen zien, het kunnen herkennen en zelfs kunnen opzoeken. Op het moment van schrijven is goud 58.800,64 euro per kilogram waard.

Als ik een kilo goud in bezit zou hebben, zou ik dit niet in mijn rugtas stoppen om vervolgens met het openbaar vervoer naar mijn werk te gaan. Ik zou dit goed beschermen en alleen toegankelijk maken voor de juiste personen. De Nederlandsche Bank heeft de goudvoorraad onlangs ook niet in rugtassen met het OV verplaatst naar het nieuwe DNB cashcentrum in Zeist.

Deze voorzichtigheid en voorzorgsmaatregelen zijn niet anders voor de toegang tot systemen en informatie.

Mijn ervaring is dat de toegang van identiteiten tot systemen en data niet vlekkeloos verloopt en dat voornamelijk het bewustzijn bij medewerkers en managers een groot pijnpunt is binnen organisaties wat betreft Identity- en Access Management. Tegenwoordig hebben we al vele manieren ontwikkeld om als organisatie een waarde te geven aan informatie, maar waarom vinden we het dan toch lastig om systeemtoegang tot deze informatie op de juiste manier te regelen?

Mijn ervaring

Als Young Professional kom je binnen bij een bedrijf en neem je een flinke scheut energie en prestatiedrang mee. Je wilt het goed doen bij een team, de klant goed bedienen en vooral je manager tevreden houden. Als een manager jou tijdens de start van je carrière onder druk zet om autorisatieverzoeken op een onjuiste manier te verwerken moet je van goeden huize komen om hier tegenin te gaan. *'Wil ik het juiste doen of wil ik een manager tevreden stellen?'*: deze gedachte heb ik wel eens gehad en ik kan me voorstellen dat ik niet de enige ben. Als de awareness niet bij de manager aanwezig is, kun je dit moeilijk vragen van de startende medewerker.

Binnen verschillende operationeel autorisatiebeheerteams ben ik verantwoordelijk geweest voor de koppeling van autorisaties aan de juiste medewerker. Een vraag die ik vaak voorbij heb horen komen is: *'Hoelang duurt het nog voordat H. van de Kool haar autorisaties in bezit heeft? Morgen begint zij met werken en ik heb dit gistermiddag doorgegeven aan HR.'* Ik denk dat veel autorisatiebeheerders zich hierin herkennen. Moet je jezelf eens voorstellen dat bovenstaande vraag van de leidinggevende wordt uitgesproken voor de toegang tot de goudkluis van de DNB… Het bewustzijn bij leidinggevenden en management over de toegang tot informatie en de benodigde activiteiten is vaak niet toereikend. Men wil zo snel mogelijk de medewerkers het werk laten uitvoeren in de systemen, maar op welke manier zij toegang krijgen, maakt vaak niet uit. Dit komt enerzijds door onwetendheid over autorisatiebeheer en anderzijds doordat de manager de medewerker zo snel mogelijk aan het werk wil zien gaan. Daarbij komt dat het functioneren van een beheerteam wordt beoordeeld op snelheid en aantallen (productiviteit) en niet op veiligheid (security). Dit komt niet overeen met het doel dat wij met Identity & Access Management nastreven:

De juiste medewerkers (identiteiten) op het juiste moment toegang geven tot de juiste informatie.

Wat mij verbaast, is dat veiligheid nog onvoldoende wordt opgenomen als kernwaarde bij het resultaat van een bedrijf of team. "Helaas hoor ik te vaak de welbekende zin vanuit security professionals 'eigenlijk moet een incident zich voordoen', want dan gaat het management de noodzaak van autorisatiebeheer als voorwaarde voor informatieveiligheid inzien."

Wanneer gaan we echt inzien dat de informatie van de organisatie, natuurlijke persoon of van een klant niet een testomgeving is, maar dat het data is die het verdient om beschermd te worden?

Awareness voor managers

We kunnen niet alleen vertrouwen op regels en techniek. Het bewustzijn van medewerkers met verantwoordelijkheid speelt een cruciale rol bij het succes van deze regels en techniek. Er zijn verschillende manieren bedacht om de awareness te verhogen en de meeste bedrijven voeren deze al uit. Denk hierbij aan online trainingen, posters en andere communicatiemiddelen. Mijn ervaring is dat de resultaten van deze middelen vaak tegenvallen, aangezien we gewoon doorklikken tot we honderd procent behaald hebben in het geval van e-learning. Zoals eerder geschreven willen mensen graag resultaten behalen en als dat met een work-around moet, doen we dat liever dan het veilige (en onbegrepen) proces volgen.

Het is belangrijk om niet alleen te steunen op het informatiebeveiligingsbewustzijn van de manager, dit kan ook op een formele manier benaderd worden. Zij hebben tenslotte al genoeg aan hun hoofd met de dagelijkse werkzaamheden. Het is belangrijk dat een gestructureerde aanpak wordt gehanteerd om het bewustzijn van medewerkers te vergroten en de veiligheid van informatie te waarborgen.

Door middel van het leggen van formele verantwoordelijkheid bij managers kan informatieveiligheid betrokken wor-

Autorisatiebeheer KPI's

Het is belangrijk op te merken dat de drempelwaarden voor het beoordelen van KPI's zoals hieronder genoemd, afhankelijk zijn van de specifieke context en doelen van de organisatie.

- Percentage onjuiste toegangsverzoeken dat wordt geweigerd of gecorrigeerd per risiconiveau of gevoeligheidsniveau van de informatiebronnen ☛ Dit geeft inzicht in de effectiviteit van het weigeren of corrigeren van onjuiste toegangsverzoeken op basis van het potentiële risico.
- Aantal beveiligingsincidenten gerelateerd aan ongeautoriseerde toegang per beveiligingsmaatregel ☛ Dit meet het aantal incidenten dat wordt veroorzaakt door ongeautoriseerde toegang, zoals pogingen tot inbraak, misbruik van gebruikersreferenties of ongeautoriseerde toegang tot gevoelige gegevens. Het wordt uitgesplitst per beveiligingsmaatregel, zoals sterke authenticatie, toegangscontroles, logging en monitoring, om de effectiviteit van specifieke maatregelen te evalueren bij het voorkomen van ongeautoriseerde toegang.
- Gemiddelde tijd (in dagen) die nodig is om toegangsrechten in te trekken of te wijzigen bij personeelsverloop, uitgedrukt als een percentage van de totale doorlooptijd van het proces ☛ Dit meet de efficiëntie van het proces voor het beheren van toegangsrechten wanneer medewerkers het bedrijf verlaten of van functie veranderen. Het geeft inzicht in hoe snel toegangsrechten worden aangepast om ongeautoriseerde toegang te voorkomen en de beveiliging te waarborgen.

Nog een aantal losse KPI's zonder toelichting:

- Percentage van de identiteiten met de juiste en actuele toegangsrechten
- Aantal herstelacties na interne audits of beveiligingscontroles
- Percentage van de identiteiten met te veel toegangsrechten (overprivilege)
- Percentage van de identiteiten met afwijkende of ongebruikelijke toegangsactiviteiten
- Het aantal unieke referenties (zoals gebruikersnamen en wachtwoorden) in verhouding tot het aantal toegangspunten
- De gemiddelde tijd die nodig is om een nieuwe gebruiker volledige toegang te geven tot alle benodigde bronnen

den in de resultaten die teams behalen. Op deze manier worden leidinggevenden op een gestructureerde en formele manier bewust gemaakt van het belang van informatiebeveiliging en worden de risico's op incidenten geminimaliseerd. Hier zijn KPI's (zie kader) voor op te stellen zodat de score op informatieveiligheid betrokken wordt in de resultaten en ook tastbaar wordt. Op deze manier kunnen we in plaats van bewustzijn creëren, bewustzijn opleggen bij leidinggevenden. Zinnen als 'kunnen jullie de autorisaties even snel toevoegen' hoop ik daardoor minder te horen op de werkvloer.

Ondertussen schaar ik mezelf niet meer tot de Young Professionals en heb ik mezelf laatst ook betrapt op hetzelfde gedrag: even snel autorisatiekoppelingen laten doorvoeren door autorisatiebeheer om resultaat te laten zien aan de opdrachtgever. Doe ik gewoon hetzelfde! Meer dan menselijk natuurlijk, maar het benadrukt wel de resultaatgerichte werkomgeving in Nederland. Gelukkig heb ik dit nog op tijd teruggetrokken, want ik wil zelf het resultaat niet alleen beoordelen op snelheid en aantallen, maar ook op juistheid en veiligheid.

Het nieuwe goud

Deel dit met je manager en laten we de verantwoordelijkheid voor de bescherming van het nieuwe goud samen pakken. Samen kunnen we ervoor zorgen dat de berg van informatie niet alleen groter wordt, maar ook veiliger. Laten we toegangsbeheer niet langer zien als een kostenpost, maar als een waardevol resultaat dat het management met trots kan presenteren. Laten we samen de weg banen naar een toekomst waarin de waarde van informatie wordt gekoesterd en waarin veiligheid een van de essentiële (formele) pijlers is waarop we bouwen.

Niet bang zijn voor de toekomst

De wereld van de informatiebeveiliging lijkt nooit stil te staan, nietwaar? We hebben het steeds over nieuwe dreigingen, nieuwe technologieën en nieuwe verdedigingsstrategieën. Maar een van de meest besproken onderwerpen van de laatste tijd is ongetwijfeld ChatGPT. Ik hoor de discussies op mijn werk, thuis, maar ook vanuit onze leden binnen het PvIB.

OpenAI had in vijf dagen tijd één miljoen gebruikers en in twee maanden honderd miljoen. Nog nooit heeft een bedrijf in zo'n korte tijd, zoveel gebruikers aan zich weten te binden. ChatGPT, momenteel het meest 'bekende' taalmodel, is zowel veelbelovend alsook een mogelijke dreiging.

Aan de ene kant hebben we een technologie die in staat is om ons werk op ongekende manieren te verbeteren: van het schrijven van beleid tot het analyseren van technische vraagstukken. Want, wie zit er nou niet te wachten op tijdbesparing binnen zijn werk? Maar aan de andere kant hebben we een instrument dat gevoelige informatie kan lekken of verkeerde informatie kan verspreiden. Stel je voor wat de gevolgen kunnen zijn wanneer een developer binnen een organisatie ChatGPT inzet om code te schrijven of te analyseren. Het incident binnen Samsung heeft al aangetoond hoe dit verkeerd kan aflopen.

We hebben ChatGPT gebruikt tijdens het Capture the Flag-evenement in juni. De taak voor de deelnemers was ChatGPT ervan te overtuigen een vlag op te geven. Als tafelcoaches hadden we de mogelijkheid om de dialogen te volgen. We merkten dat ChatGPT onwaarheden vertelde, misleiding toepaste en zich niet aan de afspraken hield, maar we zagen ook de vindingrijkheid en humor terug in de reacties. Dit was een mooie en veilige plek om de mogelijkheden te testen.

Daarom is mijn gedachte tweeledig: laten we deze technologieën omarmen, maar laten we onze gebruikers ook leren hoe ze deze op de juiste manier kunnen gebruiken en hen waarschuwen voor de risico's. We moeten niet bang zijn voor de toekomst, maar ons op de juiste manier voorbereiden om er optimaal van te profiteren.

Met dat in gedachten is de zomervakantie voor mij voorbijgevlogen: het was een periode om even te pauzeren, te reflecteren en te genieten. Ik hoop van harte dat jij als lezer ook even hebt kunnen genieten van een welverdiende rustperiode. We werken immers allemaal in een uitdagend vakgebied. Dat maakt het belangrijk goed voor onszelf te zorgen en op tijd even wat gas terug te nemen.

Het PvIB heeft ook even een pauze genomen en toch een aantal leuke activiteiten weten te organiseren voor het einde van de zomer. Zo hebben we op 24 augustus het CyberSQUAD-evenement, speciaal voor de jonge PvIB 'ers onder ons, gehouden. En op 13 september het Cyber Verzekeringen-evenement. Gezien de complexiteit en impact van recente cybersecurity-incidenten een zeer actueel onderwerp.

Wellicht hebben we elkaar op een van deze evenementen al gezien. Zo niet dan gebeurt dat hopelijk binnenkort: uitgerust en klaar voor de uitdagingen die voor ons liggen.

Stefan Veenendaal

Auteur: Abel Hoogeveen is werkzaam als Legal Tech Consultant bij ICTRecht. Hij houdt zich binnen het Legal Tech Team met name bezig met het stroomlijnen en automatiseren van juridische bedrijfsprocessen. Daarnaast ontwikkelt hij regelmatig software om processen binnen ICTRecht en bij klanten te versnellen. Hij is bereikbaar via e-mail: a.hoogeveen@ictrecht.nl.

Wie bezit GPT-modellen?

Large Language Models, zoals bijvoorbeeld ChatGPT, staan momenteel in het middelpunt van de belangstelling. Het aantal aanbieders van zulke modellen neemt sterk toe, waarbij de ene innovatie de andere innovatie lijkt op te volgen en de taalmodellen steeds beter worden. Een van de belangrijkste innovaties van de afgelopen paar maanden was de ontdekking dat deze modellen van elkaar kunnen leren (1). Door bijvoorbeeld ChatGPT op een slimme wijze uit te vragen is het mogelijk om de eigenschappen en kennis van ChatGPT over te dragen naar open source modellen. Op deze manier kan iedereen voortbouwen op de innovaties van anderen.

Met deze techniek is het goedkoper dan ooit om een fatsoenlijk taalmodel te trainen en te gebruiken voor allerlei al dan niet commerciële toepassingen. Het roept echter de vraag op wat hiervan de juridische gevolgen zijn en in het bijzonder de vraag wie zulke modellen nou eigenlijk bezit. ICTRecht gaat hier in dit artikel dieper op in.

Dat OpenAI, de maker van ChatGPT, niet blij was met bovenstaande ontwikkeling viel te verwachten. Het kwam dan ook niet als een verrassing dat OpenAI, Microsoft en Google hebben aangekondigd dat het niet langer toegestaan is om hun modellen te gebruiken voor het trainen van andere modellen (2). Dit nieuwe beleid hebben deze partijen geïncorporeerd in hun algemene voorwaarden. Naast de vraag wat dit met innovatie doet in de open source ruimte is er ook een juridische vraag voor gebruikers. Want als je als bedrijf een commerciële chatbot inkoopt, die gebouwd is op een open source model; en wanneer dat model geleerd heeft van ChatGPT, in hoeverre ben je dan juridisch kwetsbaar?

Het is belangrijk om op te merken dat het verdere trainingsverbod is opgenomen in de algemene voorwaarden van OpenAI en andere partijen. Deze voorwaarden hebben dan ook alleen betrekking op de partijen die eventueel een model verder trainen; en kunnen niet derde partijen bij het verbod betrekken. Als een commercieel bedrijf een taalmodel traint op basis van ChatGPT, dan is alleen dát commerciële bedrijf in overtreding en niet diens klanten.

Auteursrecht

Maar de vraag is vooral in hoeverre OpenAI beschermd wordt op grond van het auteursrecht en andere intellectuele eigendomsrechten. Het moeilijke daarvan is dat het auteursrecht eigenlijk niet gebouwd is voor een creatie zoals een taalmodel. Het auteursrecht is gemaakt voor geschreven boekwerken, gemaakte muziek en andere creatieve voortbrengselen van de menselijke geest. Een 'large language model', dat bestaat uit allemaal 'neuronen' die patronen herkennen en labels toekennen aan woorden en concepten; dat past niet helemaal binnen de kaders die we kennen. Dus in hoeverre kan het auteursrecht taalmodellen beschermen?

Om bij het begin te beginnen: een auteursrechtelijk werk is ieder voortbrengsel van letterkunde, wetenschap of kunst, op welke wijze of in welke vorm het ook tot uitdrukking is gebracht. Het werk dient een eigen oorspronkelijk karakter te hebben en het resultaat te zijn van creatieve keuzes. Bij taalmodellen is vooral problematisch in hoeverre er sprake is van creatieve keuzes om het model tot stand te laten komen.

De keuze hoe interne neuronen en labels zijn georganiseerd heeft weinig met creativiteit te maken en meer met feitelijke en technische keuzes. Dat een taalmodel opmerkt dat in een zin na een onderwerp vaak een werkwoord volgt, dat is een feitelijke observatie. Dat heeft weinig te maken met creatieve keuzes. Hetzelfde is het geval als een model opmerkt dat Koningin Wilhelmina de Koningin van Nederland was; dat is ook een feitelijke constatering. Natuurlijk maken de makers van taalmodellen hierbij keuzes en zullen sommige modellen het daardoor beter of slechter doen, maar dit betreffen slechts rationele wetenschappelijke keuzes en weinig schepping vanuit de creativiteit. Het is dan ook niet waarschijnlijk dat de werking van een large language model beschermd kan worden door het auteursrecht.

Databankenrecht

Het auteursrecht biedt dus waarschijnlijk geen bescherming aan taalmodellen, maar kan het databankenrecht misschien soelaas bieden? Een databank is een verzameling van gegevens die systematisch geordend zijn en waarbij het maken daarvan een substantiële investering nodig had (3). Het recht heeft als doel bedrijven te beschermen die met veel geld en moeite een databank of dataset maken; zodat niet iedereen daar zonder compensatie zomaar mee vandoor kan gaan.

Large Language Models passen best goed binnen die definitie. Ze zijn heel anders opgebouwd dan traditionele databases waarvoor de wet is gemaakt, maar de definitie is breed genoeg dat zo een taalmodel er waarschijnlijk wel onder valt. Het concept 'substantiële investering' is niet exact vastgelegd in de wet, maar gezien de enorme financiële investering en moeite die bedrijven als OpenAI en Google hebben gestoken in de ontwikkeling van taalmodellen vallen deze vrijwel zeker onder de beoogde beschermingsruimte.

Maar zelfs als taalmodellen onder het databankenrecht vallen, is nog maar de vraag of dit recht ook beschermt tegen de manier waarop andere modellen daarvan leren. Het databankenrecht beschermt op twee wijzen tegen het maken van kopieën van de databank (4). Ten eerste beschermt het tegen het maken van een gehele kopie; en ten tweede beschermt het tegen het maken van een kopie van een 'substantieel deel'. Het overnemen van kennis en vaardigheden van taalmodellen ziet op dat tweede, maar er is niet echt sprake van het maken van letterlijke kopieën.

Wanneer een open source taalmodel leert van ChatGPT dan stelt deze vragen aan ChatGPT net zoals wij dat zelf ook doen. Het vraagt niet: 'geef mij een lijst van al je labels en neuronen', maar het stelt simpelere vragen zoals: 'Geef het proces weer van de evolutietheorie' of 'Vertel mij hoe een koelkast werkt'. ChatGPT geeft hierop dezelfde antwoorden zoals het doet aan iedere andere gebruiker. Het open source taalmodel analyseert deze antwoorden en leert hier uit de kennis en patronen hoe het antwoord in elkaar steekt. Hierdoor leert het langzaamaan hoe het ChatGPT kan nabootsen. Is dit te kwalificeren als het maken van een kopie? Ik durf dat niet met vertrouwen te zeggen.

Wat het antwoord op de vraag ook is, het zal OpenAI niets helpen. Het databankenrecht beschermt alleen databanken opgezet door bedrijven in de Europese Unie. OpenAI is tot de dag van vandaag een Amerikaans bedrijf en geniet dan ook geen bescherming op basis van dit recht. Toch biedt het databankenrecht kansen voor bescherming van commercieel ontwikkelde GPT-modellen.

Conclusie

De ontwikkelingen van de afgelopen maanden laten zien dat het mantra van Silicon Valley - 'Go fast and break things' - vol in leven is. Voor even leek het of de voorsprong van OpenAI zo groot was dat niemand deze meer in zou kunnen halen; en nu korte tijd later is dat vertrouwen verdampt. De schrik zit erin en OpenAI en Google halen de ophaalbrug omhoog om hun koninkrijk te beschermen. Of het genoeg is, is nog maar de vraag. Want met zulke rappe ontwikkelingen is het onmogelijk om te zeggen wie morgen de kroon van beste large language model draagt.

Referenties

(1) https://arxiv.org/abs/2212.10560

(2) https://www.businessinsider.com/openai-google-anthropic-ai-training-models-content-data-use-2023-6?international=true&r=US&IR=T

(3 Artikel 1 lid 1 onder a Databankenwet

(4) Artikel 2 lid 1 onder a Databankenwet

Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl.

Hoe beveilig je een Mac laptop?

HULPGIDS BEVEILIGING VOOR HET KLEINBEDRIJF (DEEL 4)

In het vorige artikel hebben we uitgebreid gekeken naar het beveiligen van Windows-laptops en -computers. Maar wat als je een Mac-laptop gebruikt? In dit artikel zullen we dieper ingaan op de beveiliging van Mac-laptops en hoe je ervoor kunt zorgen dat je apparaat beschermd blijft tegen bedreigingen.

Zijn Mac-laptops veiliger? Dat wordt veelal gedacht en dan heb je waarschijnlijk gelijk. Op het gebied van malware hadden Mac-systemen, in 2020, maar 75.000 malware detecties tegenover 111 miljoen malware detecties bij Windows systemen (1). Deze getallen zeggen nog niet zoveel omdat hierin geen rekening is gehouden met de veel grotere hoeveelheid Windows-systemen die in omloop zijn in verhouding tot Mac-systemen. Volgens de statistieken draait 74,48 procent van alle laptops en desktops op een Windows-systemen en slechts 16,67 procent op Mac-OS (2). Dat betekent 4.450 malware detecties per 1 procent marktaandeel voor Mac en 1,49 miljoen malware detecties per 1 procent marktaandeel voor Windows.

Mac-systemen (b)lijken dus daadwerkelijk veiliger of zij worden in elk geval minder aangevallen

Zit het verschil dan misschien in de gebruikers van de Mac-laptops? Creatieve professionals, zoals grafisch ontwerpers en videobewerkers gebruiken de Mac voor hun artistieke projecten. Ondernemers en *tech-savvy* professionals vertrouwen op de betrouwbaarheid en integratiemogelijkheden met andere Apple-producten voor een soepel Apple-ecosysteem. Allemaal op dezelfde hardware aangeleverd door Apple.

Aan de andere kant hebben Windows-laptops ook een brede gebruikersbasis, en zij trekken vaak gebruikers aan die waarde hechten aan diverse hardware-opties. Windows-laptops zijn populair onder zakelijke professionals vanwege de beschikbaarheid van een scala aan software en hardware die op Windows draait.

Zou het soort gebruiker invloed hebben op de lagere dreiging van de Macbooks?

De Mac lijkt wel een stuk veiliger te zijn, maar dat betekent niet dat je geen rekening hoeft te houden met betrekking tot de beveiliging van jouw Mac-laptop! Net zoals bij Windows bestuderen we bij de beveiliging van jouw Mac-systeem drie thema's, te weten:

- Hygiëne
- Veilige configuratie
- Systeemkennis

Hygiëne

Net als bij Windows-laptops is het ook bij Mac-laptops belangrijk om regelmatig opruiming te houden. Verwijder onnodige bestanden, programma's en tijdelijke gegevens die opslagruimte in beslag nemen en prestaties vertragen. Dit doe je door regelmatig de door jou geïnstalleerde applicaties door te nemen en ongebruikte programma's te verwijderen. Gelukkig is dit bij Mac een stuk makkelijker en kan je via de 'applicaties' folder al jouw applicaties inzien en gemakkelijk verwijderen. Daarnaast adviseren wij: maak gebruik van de ingebouwde tool 'Opslagbeheer' om tijdelijke bestanden en andere overbodige gegevens te verwijderen.

Tegenwoordig creëren wij ook veel chaos binnen en met onze webbrowsers. Webbrowsers slaan tijdelijke bestanden, cookies en browsegeschiedenis op. Dat beïnvloedt de prestaties en brengt de privacy en security in gevaar. Het opschonen van de browser verloopt voor Mac- en Windows-laptops via eenzelfde route. Zorg ervoor dat je regelmatig de cache en cookies van de browser leegt en de browsegeschiedenis verwijdert om jouw browse-ervaring fris en veilig te houden. Bekijk ook de instellingen van de browser om extensies te beheren en verwijder onnodige of verouderde add-ons. Ons advies: installeer twee belangrijke add-ons met betrekking tot de browser:

1. UBlock Origin - een adblocker die virussen blokkeert die via advertenties verspreid worden. Vermijd andere adblockers, aangezien deze een reputatie hebben om virussen te bevatten. Zie ook ons voorgaand artikel in dit magazine (3).
2. Cookie Auto Delete - zorgt ervoor dat de cookies van jouw webbrowser(s) netjes opgeruimd worden.

Naast het opruimen van onnodige bestanden is het cruciaal om sterke wachtwoorden en een wachtwoordbeheerder te gebruiken om wachtwoorden veilig op te slaan. Als je volledig in het Apple-ecosysteem zit, gebruik dan eventueel de password manager van Apple (ICloud keychain). Een persoonlijke mening: concentreer niet al jouw sleutels op één plek en benut dus een aparte passwordmanager, zoals Bitwarden. Zie ook hier ons vorig artikel (3).

Veilige configuratie

Macbooks worden geleverd met ingebouwde beveiligingsfuncties die je kunt activeren om jouw systeem te

beschermen. Meestal staan deze functies al aan, maar toch is het goed om de functies nog even te controleren. Hier zijn enkele stappen die je kunt nemen:

1. zorg ervoor dat jouw Mac-OS up-to-date is door regelmatig de software-updates te installeren. Dit gaat automatisch, maar veel Mac-gebruikers herstarten niet vaak genoeg de laptop om de updates door te voeren;
2. activeer de ingebouwde firewall op jouw Mac om ongeautoriseerde toegang tot jouw systeem te voorkomen. Ga naar 'Systeemvoorkeuren' > 'Beveiliging en privacy' > 'Firewall' en zet de firewall aan;
3. gebruik FileVault om de gegevens te versleutelen. FileVault is een ingebouwde encryptiefunctie op de Mac waarmee je de volledige harde schijf kunt versleutelen en
4. activeer de 'Gatekeeper'-functie om te voorkomen dat je ongewenste software installeert. Ga naar 'Systeemvoorkeuren' > 'Beveiliging en privacy' > 'Algemeen' en kies voor 'App Store en geverifieerde ontwikkelaars'.

Bekijk naast deze features ook de 'privacy & security'-instellingen van jouw laptop. Met een Mac specificeer je namelijk per applicatie de te gebruiken features. Zo gebruik ik (Vincent) Firefox voor het dagelijks browsen; deze browser heeft geen camera of microfoon toegang. Moet ik dan toch videobellen over de browser, dan gebruik ik expliciet de Chromebrowser die toegang tot deze features heeft.

Eén van de toegangen, welke vaak even gecontroleerd moet worden, is de 'Full Disk Access'. Eigenlijk moeten nagenoeg alle applicaties geen '**álle** bestanden'-toegangsrechten bezitten. Hetzelfde geldt voor 'file access'. Controleer bij file access of de applicaties geen toegang hebben tot folders die ze eigenlijk niet nodig hebben.
Ook net zoals bij de Windows-systemen is het goed om een onderscheid te maken tussen een gebruikers- en een administratieve account. Met een apart beheerdersaccount en een standaardgebruikersaccount verminder je de kans dat schadelijke software of malware wordt geïnstalleerd zonder dat je het weet. Het standaardgebruikersaccount heeft geen toegang tot belangrijke systeeminstellingen en systeembestanden, waardoor het minder vatbaar is voor onbedoelde wijzigingen die het systeem kunnen beschadigen.
Om een standaard (niet-admin) account aan te maken op een Macbook, volg je deze stappen:

1. ga naar het Apple-menu (linksboven in de menubalk) en selecteer: 'Systeemvoorkeuren';
2. klik in het venster 'Systeemvoorkeuren' op 'Gebruikers en groepen';
3. klik op het hangslotpictogram in de linkerbenedenhoek van het venster en voer het beheerderswachtwoord in om wijzigingen aan te brengen;
4. klik op het plusteken (+) onderaan de lijst van gebruikers om een nieuwe gebruiker toe te voegen;
5. kies bij het drop-down menu 'Nieuwe account' voor 'Standaard';
6. vul de vereiste velden in voor de standaardgebruiker, zoals de volledige naam en een accountnaam. en
7. klik op de knop 'Maak aan'.

Systeemkennis

Mac is net even wat anders gestructureerd dan Windows. Het is goed om dat verschil te zien, want dan begrijp je ook waarom alles anders functioneert bij Mac dan bij Windows, dus ook security.

Mac en Windows zijn twee verschillende besturingssystemen die worden gebruikt op computers. Mac-OS is het besturingssysteem dat wordt ontwikkeld door Apple en is exclusief ontworpen voor Apple-computers, zoals Macbooks en iMacs. Het is gebaseerd op de Darwin-kernel, die afstamt van UNIX, en deelt daarom bepaalde kenmerken met UNIX, zoals een op UNIX-gebaseerd bestandssysteem en een UNIX-terminal genaamd 'Terminal'.

Aan de andere kant wordt Windows ontwikkeld door Microsoft. Het is beschikbaar voor een scala aan computers van verschillende fabrikanten. Het maakt gebruik van de Windows NT-kernel, die een ander ontwerp en een andere

functionaliteit heeft dan de Darwin-kernel. Het verschil in hardware zorgt ervoor dat Mac minder kwetsbaar is met betrekking tot hardware bedreigingen, maar met als nadeel dat Mac minder types hardware ondersteunt.

Wat toegangsbeheer betreft heeft Mac-OS vaak een strenger beleid dan Windows. Mac-OS gebruikers moeten vaak hun wachtwoord bevestigen wanneer ze bepaalde systeemwijzigingen willen aanbrengen, wat een extra beveiligingslaag biedt. Windows-gebruikers hebben niet altijd dit niveau van toegangscontrole. Ondanks dat Windows hier wel zeker verbeterslagen aan het maken is, merk je dat de Mac dat vanuit de *core* echt wat beter voor elkaar heeft - veel van de Linux-principes zijn hier overgenomen.

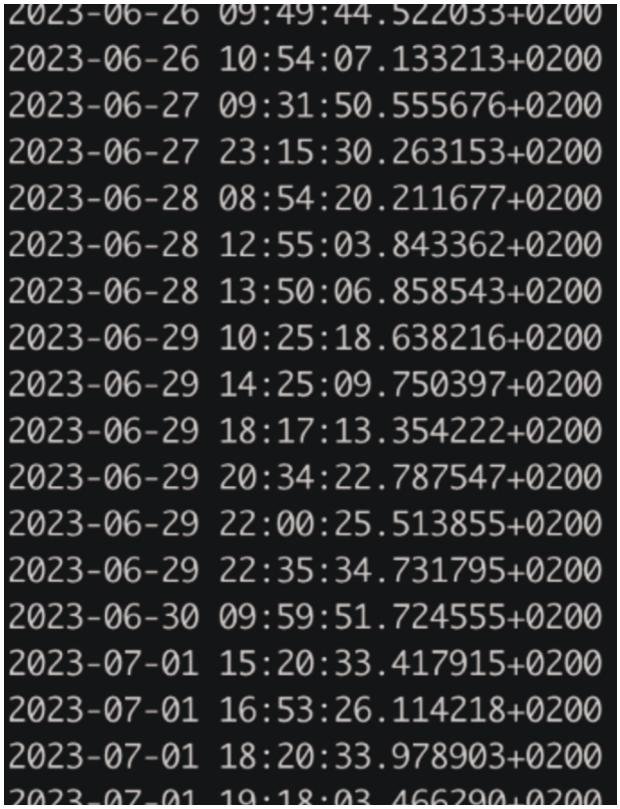
Logging werkt bij OSX echt even anders dan bij Windows. Je hebt niet een mooie interface waar je lekker door de logs heen kunt scrollen. Daarnaast zijn de logs ook minder toegankelijk. Om de logs te doorzoeken moet je de terminal leren te gebruiken. Via het commando 'sudo logs show' lees je de logs uit.

Als voorbeeld: met het commando 'sudo logs show\' zie je wanneer jouw laptop toegankelijk is/was (dus de 'unlock' functie geactiveerd is/was). Dit is handig als je vreest dat iemand fysiek heeft ingebroken op jouw laptop. Na toepassing van het commando zie je alle databestanden die via jouw laptop toegankelijk zijn geweest.

```
sudo log show --style syslog  --last 1d | awk '/Enter/ && /unlockUIBecomesActive/ {print $1 " " $2}'
```

Om de logs te bekijken moet je wel eerst de terminal openen. Om de terminal te kunnen openen moet je de volgende stappen doorlopen:

1. Zoek de 'Terminal'-applicatie. Ga naar de map 'Hulpprogramma's' in de map 'Programma's';
2. Dubbelklik op de 'Terminal'-applicatie: klik twee keer op het 'Terminal'-icoontje om de terminal te openen en
3. de terminal wordt geopend: je ziet een venster met een opdrachtregel waarin je commando's kunt typen.

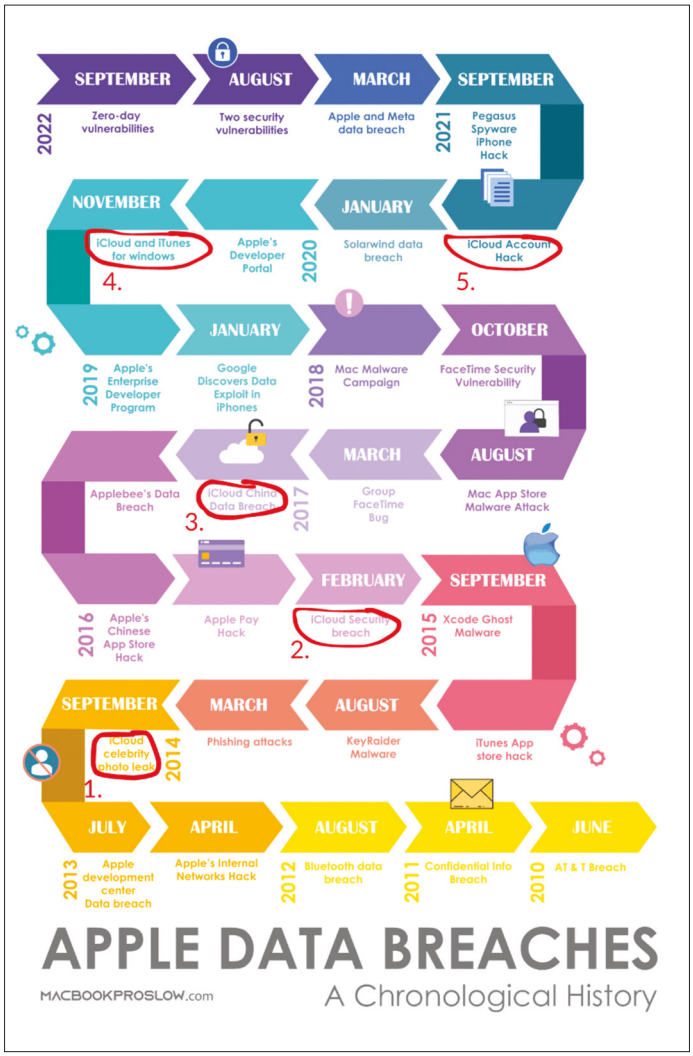


Data en tijden dat de computer unlocked was, zoals te zien in de logging.

Of voor de snelle gebruiker: (command) + (spatie), dit opent een zoekvenster. Typ dan in 'terminal' en dan ben je er ook.

iCloud

iCloud speelt een cruciale rol in het Apple-ecosysteem en biedt gebruikers verschillende voordelen. Het stelt je in staat om naadloos gegevens te synchroniseren en te delen tussen al jouw Apple-apparaten, waaronder: iPhones, iPads, Macs en zelfs Apple Watches. Hierdoor krijg je altijd en overal toegang tot de voor jou belangrijke informatie en beheer je jouw digitale leven efficiënter. Hoewel iCloud een waardevolle dienst is, zijn er in het verleden enkele



In deze afbeelding van Devansh Kamdar zie je 5x wat grootschalig fout is gegaan met iCloud

incidenten geweest die de beveiliging in twijfel hebben getrokken.

Neem de Celebrity Photo Leak: in 2014 vond er een inbreuk op de iCloud-beveiliging plaats, waarbij de privéfoto's van verschillende beroemdheden werden gestolen en online verspreid. Dit incident benadrukte het belang van sterke wachtwoorden, tweestapverificatie en het vereiste gebruikersbewustzijn bij het beveiligen van iCloud-accounts.

In een afbeelding van Devansh Kamdar zie je 5x wat grootschalig fout is gegaan met iCloud. En omdat iCloud verbonden is met al jouw apparaten, waar al jouw documenten in opgeslagen staan alsook dat er kritische services aan verbonden zijn (zoals ApplePay) is iCloud een gezocht doelwit van criminelen, waar je op zich weinig aan kan doen, behalve 2FA aanzetten en ervoor zorgen **dat je de best mogelijke beveiliging hebt geregeld**.

Linux

Zoals al eerder in dit artikel is genoemd: Mac-OS is gebaseerd op UNIX. Tal van Linux-principes rond beveiliging en het beheren van het OS-systeem zie je daarom terug bij Mac-OS. Dat is een mooie aanzet voor ons volgende artikel over Linux-systemen. Ondanks dat Linux-systemen weinig ingezet worden voor laptops (behalve door programmeurs), zijn Linux-systemen wel zeker de standaard voor stabiel draaiende (applicatie) servers. En dat ondanks het feit dat veel organisaties ervaren Linux-beheerders missen om deze servers goed te beveiligen.
Heb je van tevoren al vragen over Linux-systemen? Of onderwerpen die je graag terugziet in het artikel? Laat het vooral weten door ons een bericht te sturen of de vraag in te brengen via het LinkedIn-account van het IB Magazine.

Referenties

(1) MalwareBytes, 2020: https://go.malwarebytes.com/rs/805-USG-300/images/MWB_StateOfMalwareReport2021.pdf?aliId=eyJpIjoieW4rRGx6MFlJbDJkWEZnbiIsInQiOiJ3V1ZTSVBHSVdzdWRNVVNHRzVtVWNBPT0ifQ%253D%253D

(2) Statcounter, 2023: https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202001-202307-bar

(3) InformatieBeveiliging Magazine, uitgave 4 2023 https://www.macrumors.com/2021/08/24/scammer-hacks-icloud-accounts-for-nude-photos/

Dimitri van Zantvliet is Directeur Cybersecurity bij de Nederlandse Spoorwegen

COLUMN DIMITRI

The C stands for Change

In de hedendaagse (bedrijfs)wereld, waar cybersecurity een steeds prominentere rol inneemt, is de rol van de Chief Information Security Officer (CISO) fundamenteel veranderd. Traditioneel gezien was de CISO een functionaris, verantwoordelijk voor het beschermen van de IT-infrastructuur van een organisatie tegen bedreigingen. De Cyberbaas - die rond 1994 het levenslicht zag toen Citibank, Steve Katz aanstelde als eerste CISO ter wereld - zat eerst verstopt in de IT-operatie en had vaak een technische achtergrond. Tegenwoordig wordt er echter van CISO's verwacht dat zij zich niet enkel meer met de techniek bemoeien, maar zich met name als een 'Change Agent' opstellen. Hatsjikidee!

Wat houdt dat dan precies in? Een Change Agent is iemand die een organisatie, een team of een project leidt in het aannemen en inbedden van nieuwe processen, technologieën of gedragingen. In het geval van CISO's betekent dit dat zij een organisatiebrede cultuur van cybersecurity moeten creëren en bevorderen. Dit is een enorme verschuiving van het beveiligen van netwerken en systemen naar het beïnvloeden van de houding en het gedrag van mensen in de operatie en in de boardroom.

Als Change Agents nemen CISO's nu het voortouw om de perceptie van cybersecurity te veranderen van een belemmering naar een bedrijfsfunctie die waarde toevoegt. Ze zijn degenen die de strategie en processen voor cybersecurity bepalen, maar ze zijn ook verantwoordelijk voor het begeleiden van individuen en teams bij het begrijpen en toepassen van deze strategieën in hun dagelijks werk. Dit vereist sterke communicatieve vaardigheden, empathie en de mogelijkheid om mensen te inspireren en motiveren. Van Officers naar Enablers! Bovendien moeten CISO's als Change Agents een brug slaan tussen technische en niet-technische medewerkers binnen hun organisatie. Ze moeten in staat zijn om complexe technische concepten op een toegankelijke en begrijpelijke manier uit te leggen, en het belang van cybersecurity voor iedereen binnen de organisatie duidelijk te maken. Maar we zijn er nog niet, dit cyberschaap krijgt minstens vijf poten!

Want naast bovenstaande vraagt deze nieuwe rol van CISO's om een proactieve benadering. In plaats van reactief te handelen na een beveiligingsincident, moeten zij anticiperen op mogelijke dreigingen en voorbereidingen treffen om deze te voorkomen. Ze moeten zich ook richten op continue verbetering, door het aanpassen en verbeteren van beveiligingsmaatregelen naar gelang de ontwikkelingen in de bedrijfscontext en het bedreigingslandschap. Ze moeten jaren vooruitkijken, scenario's kunnen voorleggen en een koers naar weerbaarheid kunnen uitstippelen. Zeker geen Fabeltjeskrant verhaal!

Deze proactieve rol van de CISO komt namelijk ook goed naar voren in de 'shift left'-beweging binnen cybersecurity. 'Shift left' betekent in essentie het eerder in het ontwikkelproces integreren van veiligheidsoverwegingen, in plaats van ze als een nacontrole of correctieve maatregel te behandelen. Voor de CISO houdt dit in dat ze een faciliterende rol spelen in het mogelijk maken van 'cyber by design' voor de business en haar DevOps-teams. Cybersecurity als vertrekpunt noemen wij het.

En zo, lieve kijkbuiskinderen, transformeerde de CISO van een technische poortwachter naar een visionaire Change-agent die samenwerkt aan de paradigmaverschuiving. Een leider die zowel de technische diepgang als de interpersoonlijke vaardigheden bezit om een organisatie de weg te wijzen in een steeds veranderend cyberlandschap. En deze transformatie was niet alleen noodzakelijk, maar vooral ook onontkoombaar.

Auteur: André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en ook associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. Hij is te bereiken via andre@octopus-ib.nl of via https://www.linkedin.com/in/andre-beerten/

Risico's vinden en erover communiceren

Eigenaarschap van de derde soort [1]

Ik ben geen specialist in risicomanagement, heb er nog niet eens een cursus in gevolgd, maar vat het gewoon op als de kerntaak van de CISO en de kerndoelstelling van het ISMS: *beheers informatierisico's met passende maatregelen*. Vanuit die gedachte deel ik met jullie mijn praktische inzichten, inclusief hun beperkingen. Dus weet je het beter, heb je een vraag of opmerking, deel het met me, dan komen we in gesprek en kan ik wat leren. Ik ga in deze bijdrage zeker ook niet in op alle prachtige methoden die er bestaan, omdat dat maar afleidt van de kern: *wie* doet het risicovinden en -beoordelen, *waar* in de organisatie en in welke fase in het ISMS (en ook een beetje *hoe*). De norm zwijgt daarover, dus schrijf ik erover.

Risico's (ongeplande gebeurtenissen met (negatieve) invloed op de informatiehuishouding van je organisatie) zijn de *raison d'être* van informatiebeveiliging. Zonder risico's geen CISO, geen ISO/NEN/BIO en geen ISMS (en natuurlijk geen firewalls, virusscanners, cryptografie et cetera). Het kennen of vermoeden van informatierisico's is van groot belang voor ons als beroepsgroep, dus moeten we het zoeken naar, vinden en opvolgen van risico's goed organiseren. ISO27001 geeft de opdracht in 6.1.2 om een (herhaalbare) methode voor het identificeren en beoordelen van informatierisico's vast te stellen. De CISO (2) moet dus aan de bak.

Mijn stelling: risico's voor je informatieverwerking vind je niet op één plek in je organisatie en niet met één zoekmethode.

Dé methode

Ik heb gerespecteerde collega's (die ik óók waardeer) die bijna heilig geloven in 'dé risicoanalyse' - zoals de norm die ook lijkt te vragen - waarbij een groep mensen (vaak een kamer vol adviseurs) zich buigt over een lange lijst dreigingen. Deze groep weegt de dreigingen naar kans en impact en het resultaat is – bijvoorbeeld - een prioriteitstelling van de ruim 112 controls. Soms worden ze voorzien van wat achtergrondinformatie.

Werkt deze werkwijze?

Mijn vragen bij dé methode zijn:

- **Compleetheid:** kan een groep adviseurs en experts over genoeg kennis & informatie beschikken om álle dreigingen en kwetsbaarheden te kennen?
- **Kwaliteit:** kan een groep adviseurs en experts over genoeg kennis & informatie beschikken om álle scenario's en potentiële impacts te doordenken?
- **Actualiteit:** als de inspanning groot is, ga je hem dan wel vaak genoeg herhalen terwijl het dreigingsbeeld intussen wel verandert?
- **Toepasbaarheid:** heeft de informatie uit de analyse de juiste vorm en detaillering om te gebruiken voor het doel?

Mijn beeld is dat dé risicoanalyse in een project een korte impact kan hebben, maar snel verwordt tot een vinklijstje voor acties en zo maanden of jaren op agenda's kan staan, maar steeds minder steun krijgt. Zolang de lijst niet is afgewerkt, maakt een nieuwe poging tot inventarisatie niet veel kans. Daarnaast zet de beschikbaarheid van een 'lijst' niet aan tot zélf nadenken. Daarom vermijd ik 'dé risicoanalyse'. Ik doe het daarom anders.

Risico's zijn overal

Ik doe het anders, ik onderscheid de volgende bronnen van risico-informatie:

1. het bestuur van de organisatie (RvB),
2. de 'verwerkingseigenaren',
3. de 'control-eigenaren',
4. de CISO,
5. alle medewerkers in de organisatie.

1.Bestuur

De eerste (en belangrijkste) bron van risico-informatie is voor mij het bestuur. Het bestuur is namelijk de risico-eigenaar in laatste instantie (of gelijk Harry S. Truman: *'the buck stops here'*). Het bestuur geeft de opdracht tot beveiligen niet voor de lol. Het kost namelijk aandacht, tijd, geld en die zijn, zo heb ik geleerd, nergens ongelimiteerd voorhanden. Het gaat ten koste van de dingen die een RvB écht graag wil, namelijk bedrijfsdoelen bereiken.

De risico-opvatting van het bestuur is essentiële informatie voor het ISMS: het verwoordt ambitie en richting van 'de baas'. Iedereen die een rol speelt in de informatiebeveiliging van de organisatie moet die motivatie kennen en vertalen naar zijn eigen handelen, maar dit geldt vooral de verschillende 'eigenaren'.

Je kunt verslag maken van de sessie met de RvB, met daarin aangemerkt een 'risk-appetite' met van die gekleurde vakjes (een 'heat map') met een schuine lijn die aangeeft welk risico wel en welk risico niet wordt behandeld. Dat werkt vooral goed voor de auditor, maar het is ook een mogelijke basis voor een aanvalsplan.

Gevoel en betrokkenheid

Of de risico-informatie vanuit de RvB helemaal compleet en juist is, boeit mij eerlijk gezegd niet zo, want het gaat er primair om dat de RvB betrokken is en dat kan (en *durft* te) tonen aan de hele organisatie. IB is *'spooky stuff'* voor de gemiddelde bestuurder, dus als je ze al een uitspraak kunt ontlokken, heb je maximaal gescoord.

Natuurlijk moet je ze helpen met enige inspiratie uit - voor de RvB - herkenbare bronnen zoals het NCSC, de 'big 4' en de branche-organisatie. Laat in een interactieve sessie ook de IT-manager en de controller aanschuiven om support te leveren. Wat een formeel - door het bestuur - vast te stellen resultaat oplevert.

Rapportage

De risicobeleving van de RvB levert je ook een prachtkans op om de in de norm gevraagde doelen voor het ISMS te formuleren en je periodieke rapportage over het ISMS en de projectvoortgang hierop af te stemmen. De herkenning dat je concreet aan de slag gaat met hun *wakkerligpunten* zal hen verrassen en bij de les houden. EN het 'eigenaarschap' bij hen verder verankeren. Het vormt het zeer belangrijke startpunt van je ISMS.

Communicatie

De uitkomsten van de Bestuurlijke RisicoAnalyse (BRA), zoals ik hem noem, moeten conform de eis in 'de norm' gedeeld worden met 'relevante personen'. Als het kan door de RvB zélf en bij elke gelegenheid. Ik vind dat iedereen in de organisatie de bestuurlijke risicoboodschap moet ontvangen 'from the horses mouth'. Een uitstekend beginpunt van een veiligheidscultuur.

2.De Verwerkingseigenaren

Deze groep duiden we ook vaak aan als proces- of systeemeigenaren. In mijn tweede artikel heb ik hun takenpakket breed uitgemeten en een van de belangrijke taken (ze zijn allemaal belangrijk, natuurlijk) is het in kaart brengen van de specifieke risico's rond de informatieverwerking. Namens het bestuur moet die verantwoordelijkheid expliciet belegd zijn en leiden tot bijvoorbeeld een 'aangeklede' BIA of DPIA (dus met meer dan alleen een BIV-klasse (3)).

Aangeklede BIA

Een aangeklede BIA bevat voor mij primair een analyse van de 'scope', het bereik van de verantwoordelijkheid: voor welke informatieverzamelingen, systemen en diensten ben ik als eigenaar verantwoordelijk. En wie verrijkt en gebruikt 'mijn' informatie, wie heeft toegang, wie beheert wat? Niet zelden is dit gesprek voor de betrokkenen een ontdekkingsreis. Er duiken soms ook spoken uit het verleden op zoals oude systemen 'in de kelder', contracten die nooit opgezegd zijn et cetera.

Natuurlijk doen we ook even een 'BIV-je', maar we moeten vooral in gesprek raken over *verwerkingsrisico's* die vermijdbaar of behandelbaar zijn. Deze moeten gewogen en gecommuniceerd

Figuur 1 - Eigenaarschap in de hele verwerkingscyclus

worden.

Communiceren

Door de BIA/DPIA met de aangewezen verwerkingseigenaar in een gesprek te verkennen vestigen we 'eigenaarschap'. Dat is ook weer een bijdrage aan de veiligheidscultuur.

Uitkomsten van het gesprek moeten uiteraard niet op de plank belanden. Ik hoor jullie denken 'natuurlijk niet', maar ik vraag me wel eens af wat er dan wél mee gebeurt?

De uitkomsten (BIV-klasse én specifieke risico's voor de hele verwerkingsscope) dienen opgenomen te worden in het risicoregister. Ik zal daar later dit jaar (in IB Magazine 6) meer over schrijven. Dít is de informatie waarmee de control-eigenaar (IB Magazine 2) aan de slag moet.

3.De Control-eigenaren

Door de control-eigenaren wordt 'passende veiligheid' geleverd. Ze doen dit (als het goed is) door optimaal aan te sluiten bij de wensen en eisen van de directie en van verwerkingseigenaren, wetgeving en brancheregels, de risicobeelden van NCSC, Z-Cert et al én de operationele kennis van direct betrokkenen. Althans zo moet het mijns inziens gebeuren. Dit loffelijk streven wordt optimaal ondersteund door mijn MMA (zie artikel in IB Magazine 2 van dit jaar).

Met die MMA registreren we bij dit streven de tekortkomingen en óók de 'restrisico's die we daarbij vanuit operationeel perspectief bezien: wat kan er fout gaan nu we het niet volledig in de klauwen hebben?

Niemand kan beter inschatten wat die restrisico's zijn dan de control-verantwoordelijke (met zijn mensen), liefst in een goed gesprek met de CISO.

Communiceren

Al te vaak zijn de (operationele) restrisico's welbekend maar dringen niet door tot de bestuurder. Dat vindt zijn oorzaak vooral in de manier waarop erover gecommuniceerd wordt: inhoudelijk, anekdotisch en incidenteel. Als je er daarentegen in slaagt de aansluiting te vinden bij de beleving van de 'business' word je gehoord en ontstaat ruimte voor verbetering.

Alle risico's in de organisatie verdienen een plek in het risicoregister, dat risico's naar aard en urgentie moet onderscheiden. Het risicoregister is dé manier om de boodschap aan het bestuur over te brengen, mits structureel/regelmatig en via de juiste boodschapper bezorgd (stuurgroep en/of CISO). Want het bestuur is immers '*where the buck stops*'.

4.De CISO

De CISO zorgt voor een eenvoudig en toegankelijk risicoregister dat 'geconsumeerd' (gekend, geanalyseerd) wordt, door zowel control-eigenaren als het bestuur van de organisatie. Geïmplementeerde controls geven direct antwoord op dreigingen, de bestuurder zorgt voor de middelen om dat te kunnen realiseren. Verder zorgt de CISO dat signalen van binnen en buiten de organisatie over dreigingen en risico's een plek vinden in het register en de passende weging ontvangen.

Bronnen

'De normen' stellen dat iemand contact moet houden met overheden en andere relevante organisaties (ISO/NEN/BIO 6.1.3 en 6.1.4). Voor risico-informatie uit de buitenwereld, zoals branche-organisaties en partijen in het vakgebied (NCSC, Z-CERT, DTC en uiteraard open bronnen) moet dat de CISO zijn.

Business-impacts of BIV

Operationele risico's blijk je niet goed in business-impacts te kunnen uitdrukken, zo heb ik gemerkt in de praktijk. Een falende bescherming tegen malware kan zoveel verschillende effecten hebben en dat geldt ook voor een openstaande deur of een falende screening. Dus heb ik me aangeleerd bij operationele (rest-)risico's met BIV en de kwalitatieve beoordeling 'laag-

midden-hoog' te werken. Dit uiteraard aangevuld met een beschrijving van de mogelijke gevolgen en een plan voor mitigatie.

5.Alle andere medewerkers

Het melden en verwerken van (vermoedens van) zwakke plekken heeft een prominente plek in de norm. Ik denk dat veel organisaties het best aardig hebben geadresseerd, omdat het een manier is om 'awareness' te bevorderen. Of het ook het gewenste resultaat heeft, daar heb ik vrees ik geen beeld bij.

Wél word ik verdrietig van het woord awareness dat nog steeds breed gebruikt wordt. Immers, vrijwel alle rokers zijn zich bewust van hun ongezonde gedrag, maar dat verandert hun gedrag níet. Dat je aan veel meer knoppen moet draaien om het gewenste gedrag te bewerkstelligen bij je medewerkers is genoegzaam behandeld in goede artikelen, onder andere van de hand van Inge Wetzer.

Melden en verwerken

Natuurlijk moet er een simpele en goed vindbare meldmogelijkheid bestaan van dreigingen, kwetsbaarheden en security-incidenten met aansluitend ook een snelle verwerking (triage) en opvolging. Opname in het algemene risicoregister (ook al zijn ze gemitigeerd) lijkt me ook verstandig, omdat je meldingen dan meeneemt in perioderapportages en deze bij herhalingen ook een hogere prioriteit kunt geven.

Het risicoregister

Het risicoregister bevat alle informatie over actuele dreigingen en gewogen risico's. Ik gebruik daarvoor de voorspelbare opzet van impact in businesstermen (financiën, reputatie, processen et cetera) dus met relatie naar impact op proces-/bedrijfsniveau. Verder natuurlijk de berekening **kans*impact** voor prioritering, mitigerende actie, relatie met control & control-eigenaar en de status.

Houd daarbij de scoring eenvoudig: onderscheid niet meer dan drie niveaus voor kans en impactcategorieën, hoe je dat doet is weer een ander onderwerp. Heldere ideeën om de gevonden risico's te mitigeren mogen natuurlijk niet ontbreken, voorzien van gebudgetteerd geld, tijd & mensen.

Rapporteren

Het register moet regelmatig op de bestuurstafel belanden en niet in de organisatorische kleilaag vastlopen. Daar ligt een belangrijke taak voor de CISO, als maker en bewaker van het ISMS. Als de Bestuurlijke RisicoAnalyse succesvol was dan zal de bestuurder ook ontvankelijk zijn geworden voor andere risicoboodschappen en er iets mee willen doen. **Overal geldt: cultuur begint bij de toon in de bestuurskamer ('the tone at the top').**

Accepteren, vermijden en overdragen

Ik schrijf hier vooral over het identificeren en behandelen van risico's, maar we hoeven ze niet per se te behandelen we mogen ze ook accepteren, dat hoort bij ondernemerschap. *'Zonder risico's geen kansen'*, zegt de ondernemer. Maar we zijn veel vaker *'manager'* dan *'ondernemer'* en een manager is inherent *'risico-avers'*. Dus formuleren we overwegingen -'criteria' zegt de norm - om risico's te accepteren of over te dragen. In relatie tot norm-controls hoor ik vaak op luchtige toon 'comply or explain', alsof je altijd zomaar mag accepteren, onbeargumenteerd. Ik denk dat een 'explain' gekoppeld moet zijn aan een formeel proces en formele acceptatie, daar ga ik hier verder niet op in.

Samenvattend

Risico's voor je informatieverwerking vind je niet op één plek en niet met één zoekmethode. Ik zie eigenaren op verschillende niveaus (strategisch, tactisch en operationeel) die op verschillende manieren risico's moeten vinden (actief en passief).

De communicatie over risico's van 'vinders' naar 'behandelaren van risico's' en omgekeerd over de stand van de behandeling (beheersing met controls) is de kern van je ISMS (je PDCA-cyclus). Een belangrijk hulpmiddel daarbij is je risicoregister dat de basis vormt voor rapportage naar het bestuur.

De rapportage naar het hoogste organisatieniveau is je doorlopende 'awareness'-actie 'naar boven', dat daardoor de uitdaging op zijn bordje krijgt om te kiezen uit de vier opties: accepteren, vermijden, behandelen of overdragen.

Referenties

(1) Vrij naar Steven Spielberg, naast eigenaarschap van 1. verwerkingen en 2. controls.

(2) De term CISO gebruik ik hier - in arren moede - als dekmantel voor alle soorten adviseurs en coördinatoren informatiebeveiliging, ook waar er geen sprake is van een 'concern'.

(3) BIV – Beschikbaarheids-, Integriteits- en Vertrouwelijkheidsklasse.

COLUMN LEX

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

De zachte materialenlijst

Wat is een SBOM? Het is een relatief nieuw begrip in het security werkveld waar ik flink aan moet wennen. In eerste instantie omdat de afkorting nog niet gangbaar is, maar ook omdat het gebruik van de term in het onderbewustzijn een alarm laat afgaan. Een bom, welke soort dan ook, moet toch slecht nieuws zijn?

SBOM staat voor 'Software Bill of Materials' Het is een document dat een gedetailleerde lijst omvat van de componenten en afhankelijkheden van een softwarecomponent. Het is vergelijkbaar met een traditionele Bill of Materials (BOM) die wordt gebruikt in de maakindustrie om de samenstellende onderdelen van een product te identificeren. Er is ook een belangrijk verschil: het gebruik ervan. Een traditionele BOM is een belangrijk sturend element in de processen rond industriële planning en productie. Bij de productie van tastbare producten moeten onderdelen in voldoende aantallen beschikbaar zijn. We hebben tijdens de COVID-19-crisis gezien wat een verstoring in de beschikbaarheid kan doen. We hadden te maken met warenhuizen vol met koelkasten en parkeerplaatsen vol met auto's die wachtten op de montage van chips. En toen alle processen weer opgestart werden, duurde het maanden voordat beschikbaarheid en planning weer helemaal op orde waren, als ze dat al zijn.

Software is anders. Een softwareproduct bestaat uit bits. Het is onbeperkt te kopiëren en elektronisch te leveren. Je hebt geen last van een scheepligger in het Suezkanaal. Waar je wel last van hebt, zijn kwetsbaarheden die meegebakken worden in het productieproces. Daar is al zo'n twintig, dertig jaar een standaardantwoord op: software updates. Na productie kwetsbare componenten in hardware vervangen is complex. Dat vergt terugroepacties om het product te vervangen of te laten repareren: logistiek complex, heel kostbaar voor de fabrikant en iets wat zoveel mogelijk voorkomen wordt door strenge eisen te stellen aan de hele productieketen. De BOM speelt hierin een grote rol, alle eisen die gesteld worden staan hierin en worden bij het betrekken van de componenten al meegenomen.

Deze rol heeft de SBOM niet. Wellicht kan het in de toekomst hier naartoe groeien, maar de software-industrie is hier nog lang niet aan toe. De SBOM stelt je wel in staat makkelijk en snel vast te stellen welke kwetsbaarheden in je softwareproducten zitten. Dan moet je er zelf nog iets mee doen. In het beste geval worden updates meegenomen in een automatische dienst van de leverancier, in alle andere gevallen is het aan jou om de kwetsbaarheid te detecteren en te repareren.

De verhalen over incidenten waarbij het misging zijn talrijk. 'Heartbleed', 'SolarWinds', 'Colonial Pipelines' en 'log4j' zijn wereldnieuws geweest. SBOM is een handige component in de detectie van de kwetsbaarheden, doordat de informatie in de SBOM te combineren is met publicaties van kwetsbaarheden. Dit is ondoenlijk met de hand, hier heb je automatisering voor nodig. Zonder SBOM zou je de software zelf moeten scannen en hopen dat je daarmee alles vindt. En dan updates krijgen die de kwetsbaarheden oplossen of zorgen voor andere acceptabele alternatieven.

Dus qua beveiliging is de bijdrage van een SBOM primair detectie. En dan alleen wanneer je dit kunt integreren in je vulnerability scanning-proces. Andere responsprocedures rond patch management kunnen hierdoor geïnitieerd worden, maar dan moeten die wel beschikbaar zijn en de capaciteit hebben. Het geeft ook de mogelijkheid om kwaliteitseisen te stellen aan de leveranciers in je ketens. Je kunt eisen dat een leverancier vulnerability management aantoonbaar op orde heeft met integratie van SBOMs. En de aantoonbaarheid hiervan is ook relatief eenvoudig door een check op de current state SBOM. Wellicht wordt dit iets om te standaardiseren voor NIS 2...

Auteur: Rob Wassink is sinds 2019 werkzaam bij De Nederlandsche Bank als TIBER-NL Test Manager. Daarnaast geeft hij parttime les bij InHolland. Hij werkte eerder bij NN Group als Information Security Officer. Hij is bereikbaar onder j.b.wassink@dnb.nl.

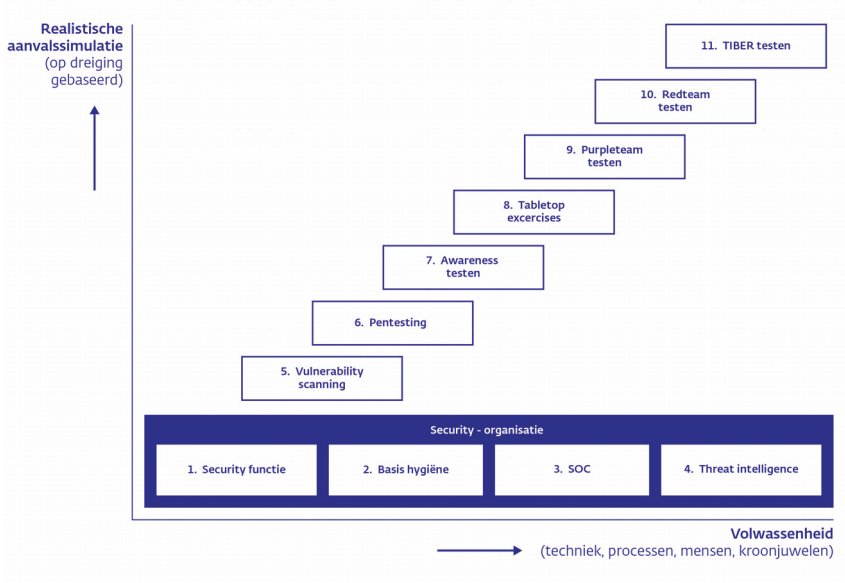
Ben ik voorbereid op een cyberaanval?

Het doel van securitytesten is de kwetsbaarheid van organisaties te onderzoeken. Met het uitvoeren van securitytesten en het oplossen van bevindingen wordt tevens de cyberweerbaarheid van organisaties verhoogd. In de Good Practise Informatiebeveiliging van DNB komt het belang van securitytesten ook duidelijk aan de orde. Er zijn verschillende type securitytesten om kwetsbaarheden van technische (IT) systemen, medewerkers en (business)processen binnen de organisatie te onderzoeken.

Dit artikel beschrijft aan de hand van het model in figuur 1 kort welke soorten security-testen er zijn en hoe ze onderling samenhangen. Het op ervaring gebaseerde model kan worden gebruikt om tot een securitytest-roadmap te komen die organisaties helpt zich stap voor stap beter voor te bereiden op een cyberaanval.

Een model om tot een securitytest-roadmap te komen

Op de horizontale as van figuur 1 wordt de mate van volwassenheid van de security-organisatie weergegeven. De verticale as toont het 'trappetje' van steeds realistischer wordende securitytesten (aanvalssimulaties). De volgorde van stappen is niet in beton gegoten. Het kan goed zijn dat bepaalde testen regelmatig terugkomen, terwijl de meest geavanceerde testen niet jaarlijks worden uitgevoerd. Het gaat erom dat de organisatie optimaal leert van de testervaring en zich continu blijft verbeteren.



Figuur 1: Model om tot een securitytest-roadmap te komen (Bron: DNB TIBER-team).

Eerst de security-organisatie op orde brengen

Een volwassen security-organisatie heeft vier basisvoorwaarden ingevuld (figuur 1: blokje 1 t/m 4):

1. **De security-functie**, meestal een CISO krijgt de opdracht om een volwassen information security-organisatie te beschrijven. Het bestuur is verantwoordelijk voor een goede implementatie.

Het doel is beheerste bedrijfsvoering doordat de cyberweerbaarheid van de organisatie in lijn is met de cyberdreiging.

2. Een volwassen security-organisatie heeft een goede **basishygiëne** en voldoet daarmee aan de vereiste ISO27001- en ISO27002-normering, of een afgeleide daarvan zoals de NEN7510 of de BIO.
   Bij DNB zien we de cyberdreiging ten aanzien van de sector verder toenemen terwijl de basismaatregelen bij verschillende financiële instellingen niet altijd op orde zijn of in lijn met bestaande cyberdreiging (1).
   Het is belangrijk voor organisaties om een goed beeld te hebben van de kritieke functies (kroonjuwelen) en onderliggende systemen en services. Deze vormen het doelwit voor verschillende internationale hackersgroepen.
3. **Een Security Operating Center (SOC)** of soortgelijk team doet aan logging en monitoring van events, en verzorgt de operationele incident response na detectie van een security incident. De SOC-functie kan intern aanwezig zijn of (deels) uitbesteed zijn bij een security provider.
4. **Threat intelligence** kan de organisatie van relevante dreigingsinformatie voorzien zodat tijdig geanticipeerd kan worden op nieuwe en veranderende dreiging. Gebaseerd op deze informatie kunnen de juiste maatregelen getroffen worden en kan wanneer deze samen worden genomen, de cyberweerbaarheid van de organisatie worden ingeschat. Meestal wordt hierbij een onderverdeling gemaakt naar strategisch, tactisch en operationeel niveau. Ook wordt er gekeken op verschillende onderdelen van de organisatie: techniek, fysiek, processen en mensen.

Met securitytesten verhoog je de cyberweerbaarheid

In de Good Practise Informatiebeveiliging van DNB komt het belang van securitytesten aan de orde. Als de vier basisvoorwaarden voor de security-organisatie zijn ingevuld en de volwassenheid aantoonbaar toeneemt, kunnen technische securitytesten overgaan in steeds realistischer wordende aanvalssimulaties (Fig. 1: blokje 5 t/m 11):

5. Met **vulnerability scanning**, een technische securitytest, kunnen bekende kwetsbaarheden met scanning tools geautomatiseerd worden opgespoord in configuraties binnen het IT- en applicatielandschap van de organisatie.
6. Bij **penetratietesten (pentesten)** wordt niet alleen gezocht naar kwetsbaarheden, maar ook of deze gebruikt kunnen worden om in te breken. Vaak gebeurt dat met een beperkte scope op bijvoorbeeld een IT-systeem of applicatie.
7. In security **awareness-testen** worden ook eindgebruikers en het management in de scope meegenomen. Deze testen worden gebruikt om het security-bewustzijn van de mensen te verhogen met als doel een gedragsverandering te realiseren. Dit kan bijvoorbeeld via trainingen tijdens 'onboarding', via online campagnes, of door middel van social engineering en (spear) phishing testen.
8. Tijdens **tabletop exercise**s gaat het crisismanagementteam (CMT) om tafel zitten en wordt een scenario geoefend waarbij een security-incident een crisis heeft veroorzaakt. Een geactualiseerd CMT en bijbehorend crisismanagementplan zijn een vereiste voor elke organisatie. Het regelmatig oefenen van verschillende scenario's, waaronder cyberaanvallen die de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) ondermijnen, verhoogt de weerbaarheid van organisaties.
9. Voor **purpleteam-testen** huurt de organisatie 'ethical hackers' in (een 'redteam') om met het SOC en de verdedigende organisatie (het 'blueteam') te testen of maatregelen in de praktijk ook echt effectief zijn (Red + Blue = Purple, vandaar deze naam). Denk aan detectiemaatregelen en of deze zijn afgestemd op de laatst bekende aanvalstechnieken die volgen uit threat intelligence.
10. Bij **redteam-testen** huurt de organisatie wederom ethical hackers in die minimaal één aanvalsscenario spelen, maar nu zonder het blueteam vooraf op de hoogte te stellen. Derhalve nog realistischer. Redteam-testen worden bijna altijd afgesloten met purpleteaming om het blueteam inzicht te geven in wat er is gedaan en ze de kans te geven om met terugwerkende kracht van de test te leren.
11. **TIBER-testen** (2) zijn van toepassing op bedrijven die van vitaal belang zijn voor een stabiele samenleving. Hierbij worden een aantal elementen toegevoegd aan het reguliere redteamen. Er wordt getest op de live productie systemen, er is begeleiding vanuit de competente autoriteit (zoals DNB). Slechts een klein team binnen de organisatie weet van de test, waaronder iemand uit het bestuur. Het verbeterplan krijgt hiermee automatisch aandacht op bestuurdersniveau. De test is gebaseerd op threat intelligence zodat alleen realistische aanvallen worden nagespeeld. De uitkomsten van de test worden na afloop gedeeld met de toezichthouder.

Een securitytest-roadmap om de organisatie voor te bereiden

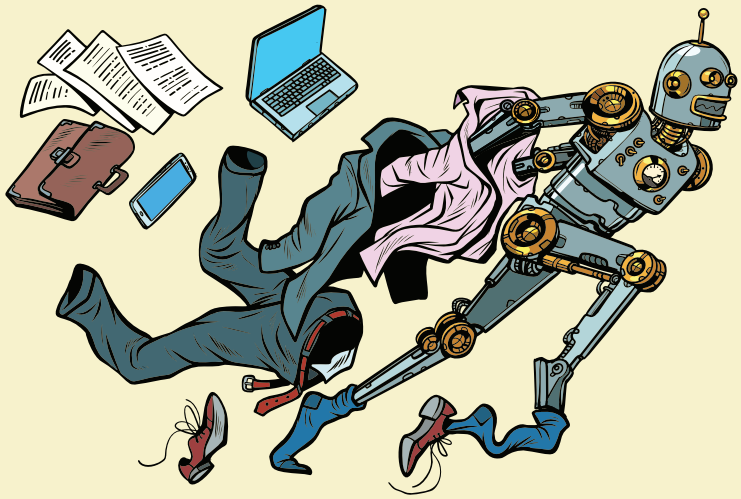
Onder aansturing van de CISO kan een securitytest-roadmap gemaakt worden. Deze roadmap geeft een meerjarig inzicht in welke securitytesten uitgevoerd kunnen worden. Door het volgen van de roadmap, zal de organisatie stap voor stap volwassener worden. En door toenemende weerbaarheid steeds beter voorbereid zijn op een echte cyberaanval.

Referenties

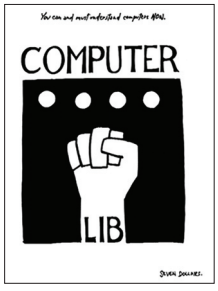
(1) https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/
(2) https://www.dnb.nl/voor-de-sector/betalingsverkeer/tiber-nl/

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

BLOG



Hoe je alles kunt leren met Ted Nelson's tips



Ted Nelson publiceerde Computer Lib / Dream Machines in 1974. Zijn bijzondere boek [1] heeft twee titels en voorkanten. De helft van de tekst is ondersteboven afgedrukt. Nelson had toen al aandacht voor computer liberation en bescherming van het publiek tegen het nietsontziend toepassen van algoritmes en andere uitwassen van de informatiemaatschappij. Ook beschreef hij zijn dromen over een ideale kenniswereld: Xanadu.

Nelson bedacht onder andere dat je in een tekst een woord moest kunnen aanwijzen zodat je meer informatie over dat onderwerp kon lezen. En dan opnieuw over een woord op die detailpagina, enzovoort. Hij noemde dat 'hyperlinks' en liep daarmee ver vooruit op het world wide web en internet. In een tijd dat 'klikken' in Nederland nog 'iemand bij de leraar verraden' betekende, want ook de computermuis was nog niet uitgevonden. Zijn boek (2) behandelt allerlei aspecten van IT- ook het beschermen van informatierechten van individuen - en was zo een zeer vroege voorbode van de **A**lgemene **V**erordening **G**egevensbescherming **(AVG)**.

Computer Lib / Dream Machines is ingewikkeld om te lezen. Je gaat het pas zien als je alles hebt doorgelezen (geïnspireerd op: Johan Cruyff), door de vele onderlinge verbanden. Zo is het wat mij betreft ook in het security werkveld. Je moet als security professional een brede en diepe kennis hebben van onderwerpen als IT, development, psychologie, economie en recht. Ook moet je de vele soms onverwachte, onderlinge verbanden zien om goed je werk te kunnen doen.

Als informatie op het gewenste moment beschikbaar moet zijn, dient een systeem, release of scrum-deliverable op tijd geleverd te worden. Om integriteit van gegevens te beschermen, moet je

'Een collega die zelf meldt op een link in een phishing mail te hebben geklikt, kun je beter een bos bloemen dan een uitbrander geven'

fraudemogelijkheden zo veel mogelijk beperken. Onvoorzichtige insiders kunnen de vertrouwelijkheid van (test)data schaden. Daarom heb ik zelf in het security werkveld bij het bewaken van beschikbaarheid, integriteit en vertrouwelijkheid veel nut van onderstaande security weetjes:

- IT-systeem bestaat uit software en hardware en beide zaken kunnen fouten of 'glitches' vertonen: juist als het niet uitkomt.
- Om op tijd een werkend IT-systeem te verkrijgen, moet je ontwerpen, bouwen (programmeren), testen, repareren, uitrollen, uitleggen en onderhouden. Activiteiten die liefst door verschillende specialisten worden uitgevoerd, het zogenoemde **'sa-men-wer-ken'**; een nieuw werkconcept, waar ik veel van verwacht.
- Negen vrouwen kunnen niet in één maand een zwangerschap volbrengen. In software-development bestaat ook geen manmaand: als één persoon in drie maanden een systeem bouwt, kunnen zes personen dat samen niet in een halve maand. Meer personeel op een vertraagd project inzetten, laat het nog verder uitlopen.
- Een incrementele back-up maak je veel sneller dan dagelijks een full back-up. Maar bij de 'restore' lever je veel van die tijdwinst weer in. 'Was dit nu het 15e of 17e increment?' – want ze moeten in de juiste volgorde worden teruggezet.
- Testen uitstellen tot laatste maand, week, dag of middag van de geplande projectduur verlaagt inderdaad het aantal issues *tijdens* het project. Maar het maakt daarna de testers heel impopulair binnen afdelingen die de onderzochte producten (of services) hebben gemaakt. Ruzies ontstaan dan over 'waarom kom je daar nu pas mee?' in plaats van een dialoog te voeren over de issue-oorzaken.
- Tijdens het testen moet je niet alleen vaststellen dat alle levensmiddelen van het vooraf opgestelde boodschappenlijstje zijn geleverd. Je moet op dat lijstje ook een riskante combinatie van alcohol en zwangerschapstest opmerken. En ontdekken dat een emballagebon met barcode voor 9,75 euro op dezelfde dag meerdere keren kan worden ingeleverd. Dus: je moet ook vaststellen dat de software niet doet, wat ook niet de bedoeling is.
- Een directeur die hiërarchie sterk benadrukt en regeert via een angstcultuur, met SMS-opdrachten (zonder alsjeblieft) ook 's avonds en vanaf zijn vakantieadres, schept een ideale omgeving om zijn organisatie slachtoffer te laten worden van 'Business Email Compromise'.
- In de speciale bestelapp voor verjaardaggebak op kantoor ('zo leuk joh, was in twee dagen klaar!') verlaag je door het bestellen van min 4 chocoladebollen van 2,85 euro elk, het totaal te betalen bedrag voor 12 appelgebak met 4 x 2,85 = 11,40 euro; dit omdat in die twee dagen niemand in het voor de app verantwoordelijke scrumteam dacht aan inputvalidatie en checken van grenswaarden.
- Ook als het gaat om security awareness vang je meer vliegen met stroop dan met azijn. Toch moet je tegen *bepaalde* overtredingen van de computer gedragscode hard optreden: zoals iemand die de complete productiedatabase kopieert naar zijn externe harde schijf, om er 'thuis mee te kunnen testen'.
- Een collega die zelf meldt op een link in een phishing mail te hebben geklikt, kun je beter een bos bloemen dan een uitbrander geven. Zeker als het 'en public' gebeurt.

Er is natuurlijk nog veel meer nuttigs om te weten over security. Hoe kun je al die ingewikkelde, samenhangende security kennis het best verzamelen? Ik ben blij met je vraag, want veel mensen durven geen vragen te stellen omdat ze bang zijn dom over te komen. Maar het stomme is om géén vragen te stellen. Als ik mijn eigen opleidingsinstituut begin, wordt mijn enige cursus: **How to learn anything.**

Volgens Ted Nelson zijn dit de technieken die slimme mensen gebruiken als ze iets willen leren *zonder* er cursussen in te volgen. Het is hoe promovendi een tweede veld (in het boek voor Nelson een 'werkveld of kennisgebied') oppikken, het is de manier waarop goede journalisten en 'genieën' werken; het brengt je het algemene begrip van een veld dat kinderen van vooraanstaande mensen in dat veld krijgen als een geboorterecht. Het is de manier waarop *iedereen* iets kan leren, als hij tenminste het lef heeft.

'Een directeur die hiërarchie sterk benadrukt en regeert via een angstcultuur schept een ideale omgeving om zijn organisatie slachtoffer te laten worden van Business Email Compromise'

1. Bepaal *wat* je wilt leren. Maar je kunt dat vooraf natuurlijk niet precies weten, want je weet niet hoe een veld is gestructureerd totdat je er überhaupt iets van weet.
2. Lees alles wat je erover kunt vinden en vooral wat je *leuk* vindt. Want zo kun je er meer over leren, en sneller.
3. Grijp naar *inzichten*. Ongeacht de punten die anderen naar voren proberen te brengen, wanneer je een inzicht herkent dat betekenis voor jou heeft, maak het dan je eigen inzicht. Het kan te maken hebben met de vorm van moleculen, de modus operandi van een geslaagde hack, de persoonlijkheid van een specifieke keizer (of je IT-directeur), of eigenaardigheden van een grote man (Bruce Schneier) in het veld. Het belang ervan is niet hoe centraal het staat, maar hoe duidelijk, interessant en gedenkwaardig het is voor jou. *Onthoud het*. En ga dan op zoek naar een ander inzicht.
4. Koppel inzichten aan elkaar. Snel heb je dan je eigen *reeks inzichten* in een veld, zoals de lichtketting rond een kerstboom.
5. Concentreer je op *tijdschriften*, niet op boeken. Tijdschriften hebben veel meer inzichten per centimeter tekst, zijn actueler en kunnen veel sneller worden gelezen. Maar als een boek je echt aanspreekt, schenk er dan overvloedige aandacht aan. En schrijf bijvoorbeeld een boekbespreking voor je vakgenoten in je favoriete vakblad.
6. Zoek je eigen speciale onderwerpen en volg die. Hongaarse APT's. Redenen om toch niet meteen te patchen. Hint: vaak is dit een *nieuw* onderwerp in het veld.
7. Ga naar *conventies*. Om een of andere reden zijn conventies een geweldige, geconcentreerde manier om dingen te leren; *praten* met mensen helpt. Denk niet dat je een speciaal iemand moet zijn om naar een (security) conventie of seminar te gaan; betaal gewoon en ga er heen. Maar je moet wel een 'titel' hebben voor op je badge! Jezelf 'Consultant' noemen, past altijd, maar ook 'Student' is volkomen eervol, zeker aan het begin van je 'studiereis'.
8. *Vind je man/vrouw*. Ergens op de wereld (niet per se: in jouw huis, straat of land) is iemand die jouw vragen buitengewoon goed zal beantwoorden. Als je hem/haar vindt, achtervolg hem/haar dan. Misschien is het een conciërge of een tiener; maakt niet uit. Volg hem/haar met je bedelnap als hij/zij dat wil, of neem hem/haar mee naar dure restaurants, of wat dan ook. Voor wat, hoort wat.
9. Blijf je *vragen verbeteren*. Waarschijnlijk heb je vragen in je hoofd, die *niet* lijken te passen bij wat je hoort. Ga er *niet* vanuit dat je het niet begrijpt; blijf je vragen aanpassen tot je een antwoord kunt krijgen dat past bij wat je zocht (jouw veld of speciale onderwerp).
10. Je veld is begrensd waar jij het wilt hebben. Alleen omdat andere mensen dingen op conventionele manieren groeperen en stereotyperen, wil nog niet zeggen dat ze noodzakelijkerwijs *gelijk* hebben. Intellectuele onderwerpen zijn op alle mogelijke manieren met elkaar verbonden; jouw veld is wat jij denkt dat het is. Ted Nelson benadrukt hier: 'Nogmaals, dit is één van de dingen waardoor je in de problemen komt als je zo probeert een diploma te behalen'.

Kun je zo *alles* leren? Hartchirurgie, sleepbootkapitein, zonnepanelen leggen? Nee, er zijn beperkingen. Deze 10 tips geven je geen laboratoriumervaring en je zult voortdurend hiaten moeten inhalen. Ted Nelson zegt hierover: 'Maar voor alertheid en het vermogen om zijn geest te gebruiken, geef me de man die op deze manier heeft geleerd, in plaats van met oogkleppen op te zijn doodgegooid met clichés binnen het onderwijssysteem.'
En daar ben ik het geheel mee eens.

Referenties

(1) Meer info op: https://en.wikipedia.org/wiki/Computer_Lib/Dream_Machines
(2) http://worrydream.com/refs/Nelson-ComputerLibDreamMachines1975.pdf

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

COLUMN MARTIJN

Wat ga jij doen aan de kennisschaarste?

Het beste moment om een boom te planten was twintig jaar geleden; het tweede beste moment is nu. Hadden we twintig jaar geleden geweten dat we zo veel mensen nodig hadden in de cybersecurity, hadden we er wellicht meer in geïnvesteerd. Maar, wat betekent deze situatie voor nu?

Dat er een kennisschaarste is op het gebied van cybersecurity is een bekend fenomeen voor iedereen die ermee te maken heeft. In de IT is er al een schaarste: en hoe gespecialiseerder je mensen zoekt, hoe ernstiger die schaarste is. Het betekent dat de kennis alleen al waarde heeft. Goede trainingen zijn prijzig en deze zijn er niet in overvloed. Kennis delen staat centraal in ons vakgebied en de mensen die in het vakgebied werken, worden van alle kanten bestookt met de vraag om hun kennis in te zetten.

Het heeft positieve kanten - zo ben ik altijd razendenthousiast over de continu veranderende en interessante cyberwereld - maar er zijn ook negatieve kanten. In een markt waarin kennis zo schaars is, is het lastig om een goed kwaliteitsniveau te waarborgen. In het land der blinden is eenoog koning en zo komen securityvraagstukken vaak bij mensen terecht die er wellicht iets van afweten, maar daar toch niet de aangewezen personen voor zijn. De aangewezen personen daarentegen overvragen we. Vaak omdat het niet anders kan. Met als resultaat dat zij overwerkt raken.

Maar wat als we de boom vandaag gaan planten, wat kunnen we dan doen? Eén van de belangrijkste dingen die ik zie, is dat we moeten blijven opleiden. Daarmee bedoel ik niet iedereen weer terug naar de schoolbanken of allemaal dure trainingen volgen, maar juist intern de tijd maken om mensen meer te leren over het vakgebied. En ja, ik ben me er zeker van bewust dat juist dat nóg een vraag is die we op het overvolle bordje van onze experts leggen. Maar we moeten keuzes gaan maken.

En bij het maken van die keuzes moeten we ons realiseren dat we nu meer moeten investeren in de groei van kennis, zodat we over twee, vijf, tien of zelfs twintig jaar de vraag beter kunnen beantwoorden. Het betekent nu een beetje pijn om grotere pijn later te voorkomen. Dat is niet alleen zo voor een enkele organisatie, maar juist voor onze hele maatschappij. Als wij ons niet keihard verder ontplooien, gaan we weer ver achterlopen in de wapenwedloop.

Dus nu mijn vraag: wat kun jij doen? Wat is jouw rol in cybersecurity en hoe kun je die overbrengen op een collega, een vriend, een concullega of een klant? Of je nu strategisch, technisch, aan de menselijke of aan de bestuurlijke kant bezig bent, iedereen heeft wat over te brengen. Neem iemand een dag mee in wat je doet en hoe je het aanpakt, schrijf je 'standard operating procedures' op, geef wekelijkse dertig minuten trainingssessies tijdens de lunch, neem een podcast op of geef een gastcollege bij een onderwijsinstelling.

Neem mensen mee in wat je doet, zodat zij het weer een tikkeltje beter kunnen. Of ze het willen of niet, zij gaan op een gegeven moment ook een extra vraag op hún bordje krijgen.

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.

Waar komt nou echte innovatie op het gebied van informatiebeveiliging vandaan?

Op veel vlakken van de informatie technologie is het duidelijk wie de aanjager is van innovaties. De ontwikkeling van Graphics Processing Units (GPU's) was bijvoorbeeld niet mogelijk geweest zonder de gaming industrie.

Chris Miller beschrijft in zijn fascinerende boek Chip War (1) hoe de innovatie van Central Processing Units (CPU's) altijd gedreven is door de defensie industrie. Dat begon al eind jaren 50 van de vorige eeuw in de Koude Oorlog. Maar ook in de Vietnamoorlog was de ontwikkeling van rekenkracht cruciaal. In het begin waren bombardementen (zoals Operation Rolling Thunder van 1965 tot 1968) gebaseerd op 'spray' en 'pray' met een marginale impact. Texas Instruments was het eerste bedrijf dat begin jaren 70 de microchips ontwikkelde voor geleide wapens, met een voor die tijd ongekende precisie. Met een cynische blik zou je kunnen zeggen dat de oorlog in de Oekraïne een proeftuin is voor AI-geleide wapens die zelfstandig hun doel zoeken.
Informatiebeveiliging is natuurlijk een veel oudere wetenschap. De behoefte om informatie te beveiligen, is waarschijnlijk zo oud als de mensheid zelf. Iedereen kent Caesar's cipher uit de schoolboeken, de eerste gedocumenteerde encryptiemethode.

Wordt echte innovatie nou geïnitieerd door de 'good guys' of de 'bad guys'? Of maken we het de bad guys zo gemakkelijk omdat security vaak nog het vijfde wiel aan de wagen is bij de ontwikkeling van een nieuw product?

Alex Dingemanse - Stem met je voeten

Nieuwsgierigheid zit diep in ons brein gebakken. Zonder deze eigenschap had de mensheid nooit de ontwikkeling meegemaakt zoals we die hebben meegemaakt. Ik kan me nog herinneren dat ik begin jaren 90 van de vorige eeuw de eerste spam mails toch wilde lezen; je wist immers maar nooit of er iets interessants in zou staan. Het heeft mij heel wat discipline gekost om het spiergeheugen te trainen om verdachte e-mails ongelezen te verwijderen.

En heb ik nou echt dat connected koffiezetapparaat nodig? Of is het een onnodige gadget waarbij het niet ondenkbaar is dat er een hardcoded admin-password wordt gebruikt. Alles dat Internet toegang heeft, kan worden gehackt.

We zijn nog steeds jagers-verzamelaars. Alleen verzamelen we nu apps, likes en volgers. In een studie uit 2019 van meer dan 82.000 voorgeïnstalleerde Android apps van 1.700 modellen van 214 merken, bleek dat deze telefoons buitengewoon onveilig waren (2). Volg de adviezen van Carissa Véliz (3) en maak je eigen privacy tot een prioriteit. Maak er een gewoonte van om geregeld apps van je telefoon te verwijderen als blijkt dat je ze toch niet gebruikt.
In een zakelijke omgeving moeten leveranciers bereid zijn om openheid van zaken te geven. En sorry, het standaardant-

Maarten Hartsuijker | Alex Dingemanse | Fook Hwa Tan

woord: 'we kunnen een SOC 2 Type 2 rapport delen', is gewoonweg niet voldoende. Maar misschien nog wel erger zijn de vele pagina's met van het internet gekopieerde detailvragen in aanbestedingen die niet ter zake doende zijn. Het zegt vaak meer over de gebrekkige kennis van de schrijver en ze hebben zelden toegevoegde waarde. Het maakt vaak pijnlijk duidelijk dat Informatiebeveiliging een vak apart is. Heb je de kennis niet, koop die dan in. Want alleen als je je eisen goed kunt formuleren kun je de juiste productkeuze maken. Maak beveiliging een van de standaardeisen in alle componenten van je IT-omgeving. En durf 'nee' te zeggen en weg te lopen, als je niet bent overtuigd.
En wat de koffie betreft: ga voor de kwaliteit van je bakkie troost en weiger je apparaat op je wifinetwerk aan te sluiten, de smaak wordt er niet beter van.

Maarten Hartsuijker - Basale fouten

Nieuwe technische snufjes zijn mooi, maar wellicht winnen we nog wel het meest met de innovatie van onszelf. Door nauwgezetter de basis op orde te brengen en te houden. Je kunt 10-factor authenticatie toepassen, maar als je IDP de bescherming van zijn sleutelmateriaal niet op orde heeft dan maak je het vooral je gebruikers moeilijk. Je kunt de meest intelligente applicatie firewalls plaatsen, maar als een groot deel van de communicatie er vervolgens gecodeerd doorheen wordt gesluisd dan had je dat dubbeltje beter anders kunnen besteden. Je kunt een slim versleuteld communicatiesysteem met sterke encryptie voor hulpdiensten ontwikkelen, maar als je de sleutels van weinig willekeurigheid voorziet of zelfs hergebruikt dan faalt zelfs de allersterkste cryptografie. We zijn met z'n allen jarenlang redelijk weggekomen met 'slordig' beveiligingswerk. Helaas lijken de bedreigingen (noem het innoverende bad guys) nu sneller toe te nemen dan we onze kwetsbaarheden kunnen verminderen (de innoverende good guys). Met een toenemend risicoprofiel tot gevolg. Die balans zien we natuurlijk liever weer de andere kant op doorslaan...

Fook Hwa Tan - Informatiebeveiliging en de cruciale rol van chipontwikkelingen in moeilijke tijden

In tijden van toenemende digitale afhankelijkheid worden informatiebeveiliging en chipontwikkelingen steeds essentiëler. De snelle opkomst van technologie en de groei van cyberdreigingen vragen om innovatieve maatregelen om onze gegevens te beschermen. In deze context spelen ontwikkelingen op het gebied van chips een cruciale rol in het waarborgen van een veilige digitale omgeving.
Chips vormen de ruggengraat van elk elektronisch apparaat. Ze zijn verantwoordelijk voor het verwerken en opslaan van gegevens. Met de groeiende complexiteit van cyberaanvallen moeten chips zich aanpassen om geavanceerde versleutelingsmethoden en beveiligingsprotocollen te ondersteunen. Dit vereist nauwe samenwerking tussen fabrikanten, cybersecurity-experts en beleidsmakers om ervoor te zorgen dat alle veiligheidsaspecten in acht worden genomen. In tijden van crisis, denk aan de COVID-19-pandemie, vertrouwen we nog meer op digitale technologieën om te blijven functioneren. Het massale thuiswerken en het dito gebruik van online diensten vergroot echter het aanvalsoppervlak voor cybercriminelen. Waardoor de ontwikkeling van robuuste, veilige chips nog urgenter wordt. Naast hardwarematige oplossingen spelen ook softwarematige beveiliging en bewustwording bij gebruikers een belangrijke rol. Een geïntegreerde aanpak waarbij chips fungeren als veilige toegangspoorten en waarbinnen gegevensversleuteling centraal staat, is de sleutel tot een betere bescherming tegen datalekken en cyberaanvallen.
Een ander aspect dat aandacht verdient, is de bescherming van persoonlijke gegevens in het Internet of Things (IoT)-tijdperk. Aangezien steeds meer apparaten verbonden zijn, moeten chips in deze apparaten ook voldoende beveiliging bieden om te voorkomen dat ze worden gemanipuleerd of misbruikt voor kwaadwillende doeleinden.
Concluderend: in tijden van moeilijkheden krijgt informatiebeveiliging een hogere prioriteit dan ooit tevoren. Chipontwikkelingen spelen een cruciale rol in het waarborgen van een veilige digitale omgeving. Door te investeren in geavanceerde chips met ingebouwde beveiligingsmechanismen, kunnen we de toenemende dreigingen effectief het hoofd bieden en het vertrouwen in onze digitale samenleving behouden. Samenwerking tussen alle betrokken partijen is essentieel om deze uitdaging aan te gaan en een robuuste, veilige toekomst te waarborgen.

Referenties

(1) Miller, C. (2022). Chip War. The fight for the world's most critical technology. Simon & Schuster, Inc.

(2) Gamba, J., Rashed, M., Razaghpanah, A., Tapiador,J., and Vallina-Rodrigeus, N. (2019). An Analysis of Pre-Installed Android Software', 41 IEEE Symposium on Security and Privacy

(3) Véliz, C (2021). Privacy Is Power. Why and How You Should Take Back Control of Your Data. Melville House Publishing

Hoe stuur jij op security in de board room?

Kijk op **cisomasterclass.nl** om uit te vinden hoe je daar grip op krijgt en schrijf je in voor de masterclass op 6, 7 en 8 november 2023.

Kennis brengt je naar de top, skills zetten je aan het stuur!

CISO masterclass

www.cisomasterclass.nl info@cisomasterclass.nl 079-360 4268

PvIB Platform voor InformatieBeveiliging

COLOFON

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

HOOFDREDACTEUR
Chris de Vries

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

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

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

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

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

creative commons

Tenzij anders vermeld valt de inhoud van dit tijdschrift onder een Creative Commons Naamsvermelding-gelijkeDelen 3.0 Nederland Licentie (CC BY-SA 3.0)

ISSN 1569-1063

VERSTERK UW ISO/IEC 27001 MANAGEMENTSYSTEEM!

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

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

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

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

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

DNV

TSTC

ICT en Security Trainingen

Ransomware? Log4j?

ADVANCE YOUR CAREER WITH SECURITY IN 2023

WR - Workshop Ransomware
EHE - Ethical Hacking Essentials
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v12
OSCP - Offensive Security PEN-200

GET SKILLED
WWW.TSTC.NL

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

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

SECURITY MANAGEMENT TRAININGEN

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

PRIVACY TRAININGEN

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

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

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

www.tstc.nl

Onze trainingen zijn weer klassikaal of Live Online te volgen