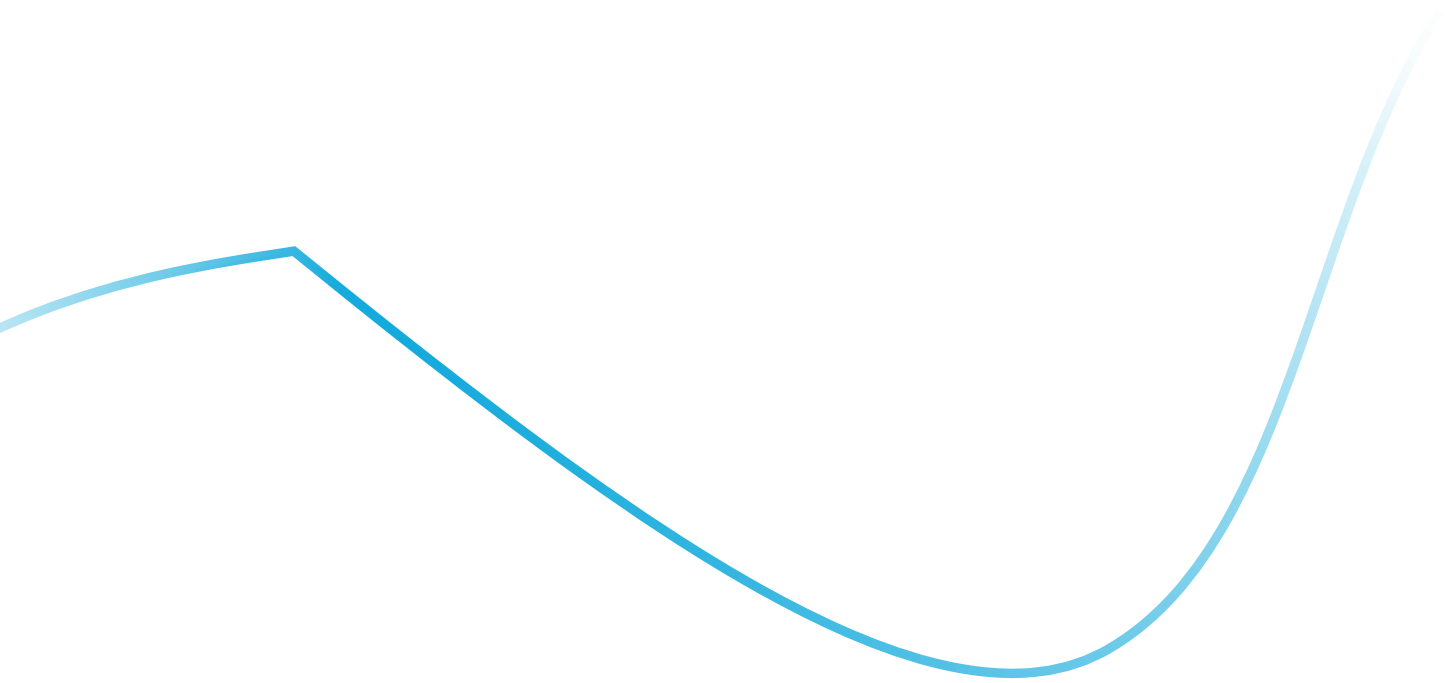
VEILIG BLIJVEN IN EEN VERBONDEN WERELD

Trends in Cybersecurity 2023



VEILIG BLIJVEN IN EEN VERBONDEN WERELD

Trends in Cybersecurity 2023

MANAGEMENT-SAMENVATTING: VEILIG BLIJVEN IN EEN VERBONDEN WERELD

Welkom bij deze gloednieuwe editie van Trends in Cybersecurity met als thema: 'Veilig blijven in een verbonden wereld'. In een steeds meer verbonden wereld is het handhaven van beveiliging essentieel. Compliant security operations, een onderwerp dat prominent aanwezig is in de artikelen van Trends in Cybersecurity, speelt een cruciale rol bij het waarborgen van beveiliging in deze digitale wereld.

Organisaties hebben de afgelopen jaren te maken gehad met diverse uitdagingen, zoals:

- Gedwongen thuiswerken;
- Bedreigingen van cybercriminelen en overheidsactoren;
- Verstoringen in de toeleveringsketen;
- Complexer compliancelandschap.

Het handhaven en aantonen van naleving vereist een flexibele securityorganisatie die in staat is om alle maatregelen en controles te handhaven.

Ik ben Hans Marcus. Met Ruud Koning, IT-manager bij Stichting Voorbereiding PALLAS Reactor, ben ik verantwoordelijk voor alle IT en bijbehorende cybersecurity.

Stichting Voorbereiding PALLAS Reactor (PALLAS) is bezig met het ontwerp en de bouw van de eerste kernreactor in Nederland in decennia. Deze reactor wordt speciaal ontwikkeld voor de productie van medische isotopen die cruciaal zijn voor de nucleaire geneeskunde. Deze medische isotopen ondersteunen diagnostiek en behandeling van diverse ziekten, waaronder kanker.

Naast de bouw van de reactor omvat de toekomstige PALLAS-organisatie ook het 'Nuclear Health Center', waar medicijnen op basis van isotopen worden vervaardigd. Vrijwel iedereen kent wel iemand die te maken heeft gehad met diagnostiek of behandeling van kanker waarbij nucleaire geneeskunde een rol speelt. PALLAS zal naar schatting 30% tot 40% van de wereldwijde vraag naar medische isotopen kunnen produceren, wat een enorm belangrijke bijdrage is aan de gezondheidszorg.

Het realiseren van een project zoals dat van PALLAS brengt echter complexe uitdagingen met zich mee. PALLAS moet voldoen aan verschillende wet- en regelgevingen, waaronder de Nederlandse Kernenergie Wet (KEW), NIS2 en GxP. Het naleven van deze regels en voorschriften vergt een uiterst goed georganiseerde security-operatie. Ruud Koning en zijn team zijn toegewijd aan het beantwoorden van alle vragen omtrent Compliant Security Operations, niet alleen voor de Stichting zelf, maar ook voor de toekomstige PALLAS-organisatie.

Ruud: *"De organisatie van PALLAS is het afgelopen jaar enorm gegroeid. Het ontwerp van een kernreactor en de ondersteunende systemen en processen is een hele klus. Waar de operationele IT-organisatie van de Stichting bedrieglijk klein is, zo'n drie of vier personen, is de groep mensen die zich bezighoudt met IT en cybersecurity voor de nieuwe reactor beduidend groter en dan hebben we de mensen die de reactor en de ondersteunende systemen ontwerpen nog niet meegerekend. In de cybersecuritygroep werken nu ruim 10 mensen aan het ontwerp van de technische systemen, het securitymanagementsysteem en de algehele cybersecurity architectuur. Samen ondersteunen deze mensen honderden ingenieurs en architecten die werken aan de fysieke systemen, de gebouwen, de besturingssystemen en de toekomstige organisatie om de hele machine te laten draaien."*

In het artikel "Digitale weerbaarheid en beveiligings baselines" wordt onderzocht of een baseline zoals de Baseline Informatiebeveiliging Overheid (BIO) voldoende is om digitaal weerbaar te zijn. Het artikel beschrijft hoe een solide security operations model en compliance hand in hand gaan. Volgens de auteurs wordt met een consistent operationeel model niet alleen compliant gehandeld, maar kan dit ook worden aangetoond.

Ruud: *"We ontwerpen niet alleen de reactor en zijn systemen, maar ook de toekomstige organisatie en het beoogde bedrijfsmodel. Gecombineerd met de personeelsunie van de huidige exploitant van de bestaande Hoge Flux Reactor brengt dat interessante uitdagingen met zich mee rond de herpositionering van mensen en operaties, niet alleen voor de toekomstige operaties, maar ook voor de periode tijdens de bouw en inbedrijfstelling. Het model voor beveiligingsoperaties is zeer relevant en een belangrijk onderdeel van ons huidige werk."*

PALLAS is nog geen werkelijkheid; de reactor en zijn organisatie bevinden zich nog in de ontwerp- en bouwfase. Er zijn echter al vele derde partijen betrokken bij het project, organisaties die (delen van) de reactor en de ondersteunende systemen moeten ontwerpen.

Ruud: *"Het ontwerp van de reactor en de organisatie ervan zijn ook veel mensenwerk: hoe krijg je iedereen zover dat hij samenwerkt aan een gemeenschappelijk doel. We volgen de systems engineering-methode met zijn engineering flows en bijvoorbeeld PDR's: Preliminary Design Reviews, waarbij we telkens opnieuw verifiëren of iedereen nog steeds op één lijn zit en vooruitgang boekt op weg naar dat gemeenschappelijke doel. Er wordt steeds meer aandacht besteed aan de logica en de toepassingsprogramma's die de besturings- en veiligheidssystemen zullen aansturen. Al dit werk wordt gedaan door verschillende bedrijven, met grote groepen mensen."*

Risicobeheer van derde partijen is een belangrijk aspect van dit werk, en de betrokkenheid van de juiste belanghebbenden is essentieel. In het artikel "De onmisbare rol van het bestuur in Third-Party Risk Management (TPRM)" wordt antwoord gegeven op de hoofdvraag: Hoe kunnen organisaties hun risicomanagement effectiever organiseren en het bestuur prioriteit geven aan TPRM? Het artikel benadrukt het belang van risicobeheer van derde partijen en de essentiële betrokkenheid van de juiste belanghebbenden. Het biedt inzichten over het verbeteren van risicomanagement binnen organisaties en hoe het bestuur TPRM kan prioriteren.

Een organisatie zoals PALLAS heeft diverse ondersteunende bedrijfsapplicaties nodig. In veel organisaties vervult SAP de rol van ERP-functionaliteit. Het beveiligen van dit platform, niet alleen op infrastructureel gebied, maar ook op andere aspecten, kan een grote uitdaging zijn. In het artikel "SAP-beveiliging: een allesomvattende blueprint voor optimale bescherming" wordt gedemonstreerd hoe beveiliging vanaf het ontwerpstadium op het SAP-platform geïntegreerd kan worden om te voldoen aan diverse regelgevende voorschriften. De focus van het artikel ligt op het beantwoorden van de hoofdvraag: "Hoe ontwerp je een blueprint voor de beveiliging van de SAP-applicatielaag?" Het benadrukt het belang van een allesomvattende aanpak om optimale bescherming te waarborgen.

De PALLAS-reactor is een zeer grote en complexe machine die veilig en beveiligd moet kunnen werken. De producten die in deze machine worden vervaardigd, moeten tijdig, in de juiste hoeveelheid en met de juiste samenstelling bij de patiënten terechtkomen. PALLAS streeft ernaar een digitale onderneming te worden, met een digitaal hart en een echte "Intelligent Industry".

Ruud: *"De DES, of Digital Enterprise Strategy, is het ontwerp voor de toekomstige PALLAS-organisatie. De DES heeft tot doel een digitale organisatie op te leveren, waarbij niet alleen het productieproces wordt geoptimaliseerd, maar dat proces ook wordt beschermd tegen invloeden van buitenaf. In deze DES ontmoet ons primaire proces de eisen op het gebied van security en compliance: vanaf het begin van het ontwerpproces en vanaf het fundament om ervoor te zorgen dat elk bedrijfsproces niet alleen zeer effectief en efficiënt, maar ook compliant en veilig is en dat kan laten zien. De DES geeft richting aan de architectuur en inrichting van het PALLAS applicatielandschap, zowel voor de business als de operatie. Een echte digitale blauwdruk!"*

Het gebied van OT-beveiliging is gespecialiseerd in het beveiligen van Cyber-Fysieke systemen, waar het productieproces en informatie samenkomen.

Ruud: *"PALLAS omvat een groot aantal systemen die fysieke processen besturen en monitoren. Ongeveer 250 systemen verspreid over nucleaire en conventionele controlesystemen, transportsystemen, laboratoria, stralingsmonitoring, energiesystemen en klimaatbeheersing maar ook fysieke beveiliging en communicatie met interne en externe partijen en natuurlijk de bedrijfssystemen die worden gebruikt voor administratie, planning en analyse. Allemaal hebben deze systemen directe of indirecte invloed op het primaire proces: het produceren van nucleaire medicijnen. Al deze systemen dienen te worden beveiligd met inachtname van het fysieke proces. Daarom integreren we beveiliging vanaf het begin van de ontwerpfase om security by design te waarborgen."*

Wanneer alles is ontworpen en gebouwd, moet er iemand verantwoordelijk zijn voor de beveiliging. Veel organisaties kiezen ervoor om een Managed Security Service Provider (MSSP) in te schakelen. In het artikel "De perfecte match: hoe kies je de ideale Security Service Provider voor jouw organisatie?" gaan we in op de zoektocht naar de juist provider voor jouw organisatie. Want technische eisen zijn goed te bepalen, maar wat verwacht je aan service-ervaring?

Ontdek nu de complexe wereld van cybersecurity en blijf een stap voor in de snel veranderende digitale omgeving! Deze gloednieuwe editie van Trends in Cybersecurity onthult de uitdagende realiteit van het ontwerpen, implementeren en beheren van een veiligheidsorganisatie die voldoet aan de hoogste eisen. Veilig blijven in een verbonden wereld is essentieel en we zijn er trots op dat we je kunnen meenemen op deze reis naar een veilige toekomst.

We hopen dat je geniet van deze tweede editie van Trends in Cybersecurity en dat het je helpt om inzicht te krijgen in de uitdagingen en mogelijkheden van een veilige toekomst in een verbonden wereld.

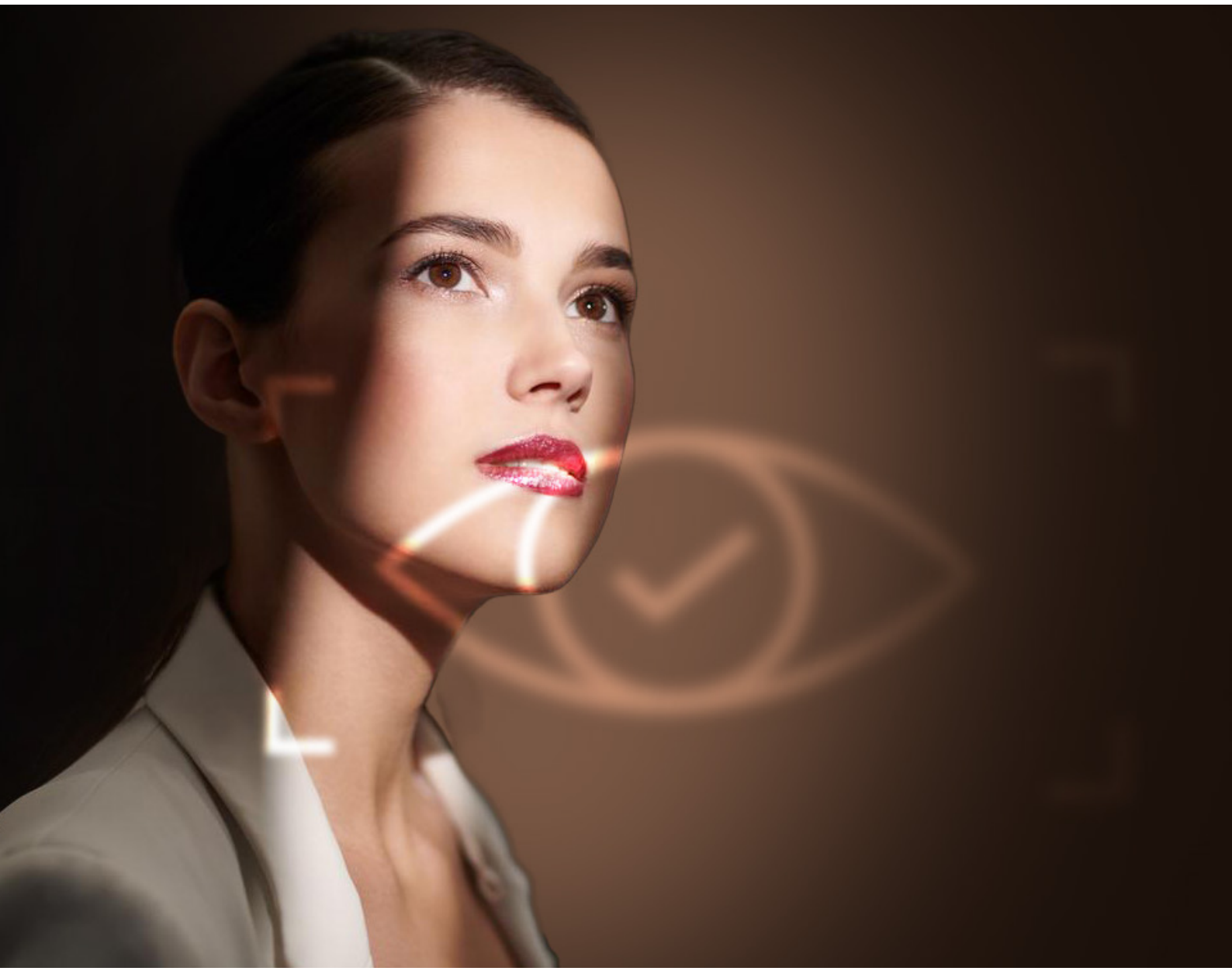
Over de auteurs:

Hans Marcus
Senior Security Manager

Ruud Koning
CISO bij PALLAS

INHOUD

DE EVOLUTIE VAN CYBERSECURITY BIJ NS: VAN NIEUWE UITDAGINGEN TOT TOEKOMSTGERICHTE STRATEGIEËN



Nederlandse Spoorwegen (NS) rijdt al 184 jaar met treinen. In al die jaren zijn verschillende veiligheidsgebieden ontwikkeld als antwoord op nieuwe inzichten en het veranderende veiligheidslandschap. Cybersecurity is het tiende veiligheidsgebied dat NS momenteel ontwikkelt. Het staat sinds een paar jaar duidelijk op de radar. In dit artikel bespreken we het heden en de toekomst van de cyber-functie binnen NS.

Aanvalsoppervlak

Dat cybersecurity voor NS een focusgebied is geworden heeft een aantal oorzaken. Ten eerste is het aanvalsoppervlak groter dan ooit; alles staat tegenwoordig in de cloud, wat zijn eigen kwetsbaarheden met zich meebrengt. En de dienstverlening van NS draait steeds meer rond mobiele devices. NS biedt bovendien meer reisproducten aan – voor reizen in Nederland, maar ook steeds meer daarbuiten. In totaal zijn zo'n 520 Application Programming Interfaces (API's) ontstaan, met 12 miljard calls op jaarbasis. De scope voor bedreigingen is daarmee enorm.

Compliance

Ten tweede heeft NS zich te verhouden tot Nederlandse en internationale wetgeving. Sinds NS in december 2021 werd aangewezen als Aanbieder van Essentiële Diensten (AED), valt de vervoerder bovendien onder de Europese Network and Information Systems-wetgeving (NIS). In dit rapport gaan we dieper in op naleving met betrekking tot cybersecurity. Ook spreken we in een ander artikel over NIS2, de meest recente versie van die wetgeving. Ontdek hoe deze twee onderwerpen naadloos samenkomen om een solide basis te leggen voor een veilige digitale toekomst.

OT Security

Ten derde; het aanvalsoppervlak is niet alleen enorm gegroeid, het dreigingslandschap is ook enorm verslechterd. Dit is een ontwikkeling die een grote vlucht heeft genomen sinds de uitbraak van de oorlog in Oekraïne. Ook Operationale Technologie (OT) blijkt daarbij kwetsbaar; zo is bijvoorbeeld malware en wiperware gemaakt die de spoorwegen in Oekraïne gericht aanvalt. Dergelijke malware is tot nu toe niet overgeslagen naar Nederland – en NS heeft daar ook beleid op ontwikkeld – maar waakzaamheid blijft geboden. In dit rapport gaan we dieper in op de kwetsbaarheden van OT en de noodzaak voor voortdurende waakzaamheid in Nederland.

Cyberstrategie

Onder leiding van directeur cybersecurity, Dimitri van Zantvliet, heeft NS haar eerste lange termijn cyberstrategie vastgesteld. De cyberstrategie weerspiegelt de grote maatschappelijke rol die NS speelt. De spoorwegen liggen onder een vergrootglas; reizigersaantallen moeten worden teruggewonnen, groene mobiliteit moet worden gefaciliteerd – en vanuit haar rol als vervoerder is NS een belangrijke schakel in economische en maatschappelijke bedrijvigheid. Het vertrouwen dat bestaat in die rol hangt mede af van de cybersecurity die het bedrijf weet te realiseren.

Kortom: het is niet voor niets dat cyber voor NS een prioriteit is op boardroom niveau. Om die prioriteit gestalte te geven, is enige tijd geleden cyber afgesplitst van IT. Dimitri heeft als directeur cybersecurity periodiek een eigen plek aan tafel, met een eigen directoraat.

Bouwblokken

De cyberstrategie van NS steunt op een aantal bouwblokken. Ten eerste schrijft de strategie een radicale shift-left voor als het gaat om cyber; cyber en privacy worden by design meegenomen in elk functioneel en non-functioneel ontwerp. Dat doet NS niet alleen uit veiligheidsoverwegingen; als de benodigde cyber layer achteraf nog moet worden ingevoegd, kost dat veel meer tijd, geld en menskracht. De afdeling levert daartoe gecentraliseerde en gestandaardiseerde cyberdiensten aan de developers; denk aan threat modelling, secret scanning en PEN testing. Developers kunnen dergelijke diensten daardoor eenvoudig meenemen in de pipeline en hoeven er verder niet over na te denken. Door op deze manier cyber by design mee te nemen, is NS beter gepositioneerd als het gaat om het opsporen en voorkomen van cyberdreigingen. Meer inzicht over hoe deze opsporing wordt uitgevoerd, vind je in het artikel over threat hunting.

De implementatie van zero trust is een ander bouwblok. Op dit moment maakt NS nog voornamelijk gebruik van perimeter based security. De komende jaren zal dat verschuiven naar identity based security. Een totaal nieuwe filosofie, gebaseerd op zero trust, die ergens tussen 2026 en 2030 overal gestalte moet hebben gekregen. Het vierde bouwblok omvat het versterken van de cybersafe cultuur.

Mensenwerk

Vanwege de groeiende complexiteit en omvang van het aanvalsoppervlak, samen met de verslechterende dreigingssituatie, wordt de behoefte aan een deskundig personeelsbestand steeds groter. OT security, cloud security, identity security: het zijn allemaal eigen vakgebieden met een eigen complexiteit. Daar zijn specialisten voor nodig – en gezien de wereldwijde schaarste aan cybertalent ligt daar een flinke uitdaging. NS leidt daarom steeds meer zelf mensen op, in de eigen cybersecurity academy. Daarbij ligt de focus ook bij horizontale doorstroming; zo nam NS recent een machinist aan die hacker wilde worden en in cybersecurity wilde werken. Die persoon wordt niet alleen intern opgeleid, maar hij neemt ook zijn eigen ervaringen mee en zijn inzichten vanuit de cockpit; die zijn ook voor de versterking van cybersecurity heel waardevol. In het artikel over security service providers, dat je eveneens in deze context kunt vinden, wordt dieper ingegaan op de rol van externe partijen en hun specialisten en hoe zij kunnen bijdragen aan het versterken van je menselijk kapitaal.

Tegelijkertijd is NS zich ervan bewust dat er sprake is van asymmetrische oorlogvoering. Winnen kun je nooit. Wat je wel kunt doen is een infinite game-mindset adopteren, continuous learning omarmen – en je focussen op wat je kunt beïnvloeden. In de wetenschap dat cybersecurity altijd deels reactief zal zijn, zijn snelle detectie en een snelle respons cruciaal. En mocht het een keer echt misgaan, dan heeft NS playbooks klaarliggen om de gevolgen zoveel mogelijk te beperken. In dit rapport hebben we een artikel gewijd aan een essentieel aspect van cybersecurity: Business Continuity Management.

Nieuwe trends versus legacy-platformen

Grote organisaties als NS draaien vaak deels nog op oude legacy-platformen. Het gaat dan vaak om offline platformen die al end-of-life zijn en waar geen onderhoud meer op zit. Toch hebben ze vaak nog een functie binnen complexe organisaties als NS, met al zijn (lokale) materieel, vastgoed en infrastructuur. En ook al is legacy vaak niet verbonden met de buitenwereld, helemaal onkwetsbaar is het niet – en het is niet ondenkbaar dat legacy platformen een besmettingsbron worden voor de rest van de organisatie. Dergelijke installaties mogen niet ontbreken in een cyberstrategie. Zolang ze nodig zijn moeten ze immers ongehinderd door kunnen draaien – onbedreigd, en niet-bedreigend.

AI

Helemaal aan de andere kant van het spectrum staat Artificial Intelligence (AI). Generative AI heeft ook binnen NS bruikbare use cases. Chatbots zijn interessant voor reisinformatie, voor contractinformatie, je zou ze kunnen 'opleiden' met handleidingen van treinen, er is veel mogelijk. NS zet ook nu al AI in om de logistiek van treinwagons, de 'bakken', zo efficiënt mogelijk in te richten, bijvoorbeeld rond knooppunten en opstelplaatsen waar treinen worden samengesteld en soms worden gerepareerd en gewassen. Het gaat om duizenden bakken; daarin is met AI veel winst te behalen. Tegelijkertijd waakt NS ervoor AI-gerelateerde data onder te brengen bij een externe partij. Voor meer inzicht in de relatie tussen AI, privacy en security verwijzen we je het AI-artikel uit dit rapport.

Dat een van origine traditioneel 'nuts and bolts'-bedrijf als NS, cybersecurity ook als een voorname prioriteit ziet, geeft wel aan hoe snel het veld zich ontwikkelt. Zowel als het gaat om de bedreigingen, maar ook om wat we kunnen doen om die bedreigingen te weerstaan en erop te anticiperen.

We wensen je veel leesplezier met deze editie van Trends in Cybersecurity.

Serge Dujardin
Vice President - Global Head Cyber GTM, Capgemini Nederland B.V.

Dimitri van Zantvliet
Directeur cybersecurity / CISO, NS

01

Trends in Cybersecurity 2023

ORGANISATORISCHE ASPECTEN VAN VEILIGHEID

BENUT DE KRACHT VAN DE CLOUD VOOR HET WAARBORGEN VAN SECURITY EN COMPLIANCE

Hoe kunnen organisaties het potentieel van de cloud volledig benutten en tegelijkertijd hun security en compliance waarborgen?

Highlights

- De cloud zorgt voor meer schaalbaarheid, innovatie en efficiëntie.
- Cloudcomputing levert behalve voordelen ook uitdagingen op.
- Het model voor gedeelde verantwoordelijkheid voor ieders rol in cybersecurity is vaak complex.
- Door de nodige maatregelen te nemen, kunnen organisaties potentiële risico's beperken.
- GRC-tools ondersteunen de security en compliance, maar hebben ook beperkingen.

Cloudcomputing: een overzicht

Het digitale tijdperk heeft het zakelijke landschap ingrijpend veranderd. Vooral cloudtechnologie speelde hierin een belangrijke rol. Maar nog steeds vormt cloudtechnologie een spil in de transformatie van de manier waarop we zakendoen in het huidige digitale tijdperk. Cloudtechnologie biedt bedrijven aanzienlijke mogelijkheden om op te schalen, te innoveren en hun efficiëntie te verbeteren.

Cloudcomputing brengt tal van uitdagingen voor organisaties met zich mee wat betreft security en compliance. In dit artikel gaan we in op deze uitdagingen en delen we onze inzichten in hoe je deze uitdagingen effectief het hoofd kunt bieden.

Een van de grootste voordelen van cloudcomputing is kostenefficiëntie; het neemt de noodzaak van dure servers en bijbehorende infrastructuur weg. Het hybride cloudmodel van Dropbox is een goed voorbeeld van hoe organisaties de kosten omlaag kunnen brengen zonder dat de gegevensbeveiliging in het geding komt. Daarnaast bieden cloudservices schaalbaarheid en flexibiliteit, waardoor organisaties hun IT-middelen beter kunnen afstemmen op de vraag. Het gebruik van AWS door Netflix[1] laat zien dat het mogelijk is om effectief op de fluctuerende vraag van gebruikers in te spelen. Cloudtechnologie zorgt daarnaast voor meer mobiliteit en een efficiëntere samenwerking, omdat het werken op afstand en realtime samenwerking mogelijk maakt. Google Workspace[2] illustreert de transformatieve kracht van cloudgebaseerde samenwerkingstools, die de productiviteit en de efficiëntie verbeteren. Aanbieders van cloudservices bieden solide beveiligingsopties voor de opslag en beveiliging van data. Het gebruik van AWS door Capital One[3] laat zien hoezeer organisaties kunnen vertrouwen op de veiligheidsmaatregelen van cloudaanbieders voor de bescherming van gevoelige informatie. Daarnaast bieden cloudplatforms betrouwbare en kosteneffectieve oplossingen voor calamiteitenherstel. De gegevensback-up van AWS, waar Airbnb[4] gebruik van maakt, laat goed zien hoe de cloud kan worden ingezet voor effectief calamiteitenherstel. Tot slot draagt cloudcomputing ook bij aan een beter milieu door het energieverbruik omlaag te brengen en de CO_2-voetafdruk te verkleinen, zoals te zien is in het Azure-platform van Microsoft.

Toonaangevende cloudaanbieders spelen in op de zakelijke behoeften van bedrijven in tal van sectoren. In 2022[5] had AWS 32% van het wereldwijde marktaandeel in handen. Daarmee was het bedrijf het grootste cloudplatform ter wereld. AWS geniet de voorkeur van ondernemingen in allerlei soorten en maten, waaronder van prominente bedrijven als Netflix en Airbnb. Vanwege het uitgebreide aanbod en de expertise van AWS op het gebied van AI, ML, analyses en IoT-diensten is dit bedrijf vaak de eerste keus van ondernemingen die op zoek zijn naar geavanceerde technologische mogelijkheden. Op de voet gevolgd door Microsoft Azure, dat met een marktaandeel van 23%[6] met name dominant is in Europa. Microsoft Azure is vooral populair bij de gebruikers van de software van Microsoft, vanwege de naadloze integratie en compatibiliteit met de andere producten van Microsoft. Hierdoor heeft Azure de voorkeur in sectoren als de financiële dienstverlening, de maakindustrie en de retailsector.

Google Cloud Platform (GCP) is een snelgroeiende leverancier met een marktaandeel van 10%, die uitblinkt in machine learning, big data en analyses. Twitter en PayPal kozen voor GCP vanwege de expertise van het bedrijf op deze vakgebieden. Bij het kiezen van een cloudprovider gaan bedrijven uit van hun eigen unieke vereisten, gewenste technologieën, gespecialiseerde diensten en reputatie op het gebied van betrouwbaarheid en prestaties. Security en compliance zijn dan ook cruciale aspecten van cloudgebaseerde systemen. Cloudbeveiliging waarborgt de veiligheid van data, applicaties en infrastructuren door functies als firewalls, inbraakdetectie, IAM (Identity and Access Management) en versleuteling.

Compliance zorgt voor de naleving van wet- en regelgeving waar niet-naleving zou leiden tot boetes en reputatieschade. Zo was er sprake van een bekende medische dienstverlener die een miljoenenboete boven het hoofd hing voor het overtreden van de Amerikaanse Health Insurance Portability & Accountability Act (HIPAA). Met behulp van gespecialiseerde tools en toegewijde beveiligingsteams kunnen cloudaanbieders dergelijke organisaties helpen om aan alle nalevingsvereisten te voldoen.

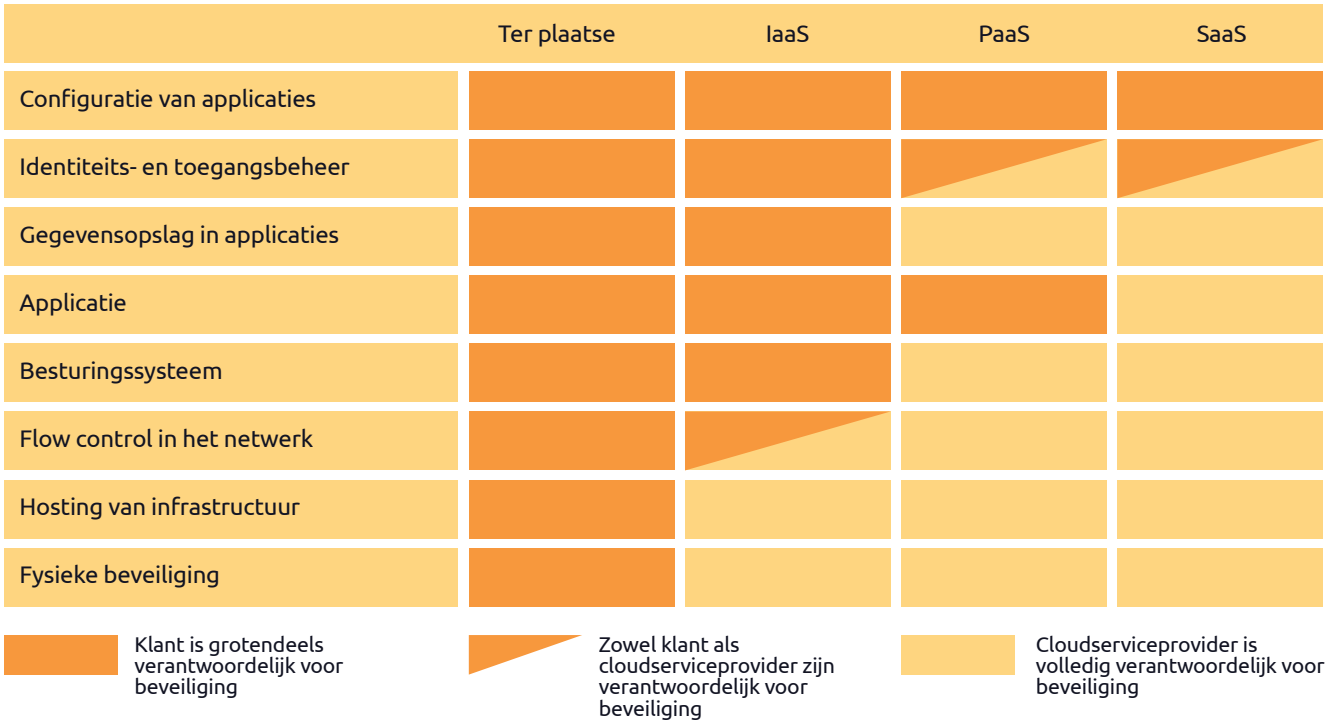
Kortom, de overstap naar de cloud levert bedrijven aanzienlijke voordelen op, maar brengt ook de nodige uitdagingen met zich mee wat betreft security en compliance. Door te weten wat deze uitdagingen zijn en door gebruik te maken van de mogelijkheden van toonaangevende cloudaanbieders, en daarbij prioriteit te geven aan security en compliance, kunnen organisaties het potentieel van de cloud volledig benutten zonder dat hun gegevensbeveiliging en reputatie in het geding komen.

Wegwijs in de matrix voor gedeelde verantwoordelijkheid

Cloudproviders spelen een cruciale rol in het waarborgen van de cloudsecurity en compliance. Ze zijn tenslotte verantwoordelijk voor een enorme hoeveelheid gevoelige gegevens en actief in allerlei omgevingen met uiteenlopende wet- en regelgeving. Het gedeelde verantwoordelijkheidsmodel voor cloudsecurity en compliance bestaat uit fundamentele principes die de verantwoordelijkheid voor de veiligheid van de cloud tussen de cloudaanbieder en de klant verdelen. Kort gezegd komt het erop neer dat de beveiliging ván de cloud (de infrastructuur, het fysieke en visuele platform) onder de verantwoordelijkheid van de cloudaanbieder valt, terwijl de klant de verantwoordelijkheid draagt voor de beveiliging van alles wat zich ín de cloud bevindt (gegevens, applicaties en toegangsbeheer). Hoewel deze uiteenzetting de rolverdeling tussen klanten en cloudaanbieders duidelijk lijkt aan te geven, brengt dit in de praktijk toch talloze vragen en problemen met zich mee wat betreft security en compliance.

De rolverdeling varieert niet alleen afhankelijk van de modellen die klanten voor hun cloudoplossingen gebruiken, maar wisselt ook in verdeling van de taken die aan de klant en aan de cloudprovider zijn toegewezen. Zoals te zien is in figuur 1 van het Britse National Cyber Security Centre kan voor de werking van een applicatie in een IaaS-ontwikkelingsmodel (Infrastructure as a Service) gesteld worden dat de verantwoordelijkheid voor de security en compliance meer bij de klant wordt neergelegd.

Een aantal van de aspecten waarvoor cloudproviders stelselmatig certificeringen moeten verwerven en behouden, hebben betrekking op internationale en regionale regelgeving, zoals de AVG, de HIPAA en GxP-richtlijnen. Dit om aan te tonen dat ze aan alle regelgeving voldoen. Maar een goede naleving van alle regels is ook een gedeelde verantwoordelijkheid. Cloudproviders zijn verantwoordelijk voor de naleving van de richtlijnen voor hun infrastructuur en voor het leveren



Figuur 1: Het Shared Responsibility Model van het NCSC geeft de gedeelde verantwoordelijkheid aan tussen klanten en cloudproviders[8]

van de tools en diensten waarmee klanten aan hun eigen compliance-eisen kunnen voldoen. Aan de andere kant moeten klanten er op hun beurt ook voor zorgen dat hun data en gebruik van clouddiensten aan de desbetreffende wet- en regelgeving voldoen.

Hoewel de cloudproviders veel van de beveiligingsaspecten voor hun rekening nemen, is de klant uiteindelijk verantwoordelijk voor de beveiliging van de eigen activiteiten. Daaronder valt ook het gebruik van de clouddiensten. Cloudproviders bieden daartoe GRC-tools (voor governance, risicobeheer en compliance) waarmee klanten zelf hun beveiligings- en nalevingsvereisten kunnen beheren. Maar ondanks dat de afnemers van clouddiensten met behulp van GRC-tools zelf moeten, en kunnen, zorgen voor de security en compliance van hun bedrijfskritische applicaties en financiële processen, hebben deze tools ook hun beperkingen. Naast het ontbreken van duidelijkheid over de taken en verantwoordelijkheden van enerzijds de klant en anderzijds de provider, worden diverse beperkingen vaak over het hoofd gezien. Zoals onvolledige automatisering, het onvoldoende waarborgen van nieuwe regels en nalevingsvereisten met betrekking tot het cloudlandschap en beperkte integratie met de bestaande architectuur van de klant.

Het cloudvraagstuk: de juiste aanpak voor de risico's en uitdagingen waar organisaties voor staan

Het handhaven van cloudsecurity en compliancesvereisten plaatst organisaties voor talloze uitdagingen en ingewikkelde situaties. Denk aan gegevensbescherming, de naleving van diverse wettelijke voorschriften, het waarborgen van inzicht en controle, effectief identiteits- en toegangsbeheer (IAM), snappen hoe het model voor gedeelde verantwoordelijkheid in elkaar steekt, en het beperken van dreigingen van binnenuit. Door alle taken en processen duidelijk af te bakenen zijn ieders verantwoordelijkheden duidelijk en kan iedereen actief bijdragen aan het handhaven van de security en compliance in de cloudomgeving.

Maar behalve dat de rolverdeling duidelijk moet zijn, moeten organisaties ook gebruikmaken van solide beveiligingstools om eventuele kwetsbaarheden proactief te identificeren en aan te pakken. Met deze tools kunnen bedrijven beveiligingsincidenten monitoren en beheren, ongeautoriseerde toegangspogingen opsporen en snel op mogelijke dreigingen reageren. Naast deze beveiligingstools zijn uitgebreide trainingsprogramma's voor het personeel essentieel om medewerkers te informeren over best practices op het gebied van cloudbeveiliging en om ervoor te zorgen dat ze over de juiste kennis en vaardigheden beschikken om de cloudomgeving veilig en compliant te laten zijn.

Door te zorgen voor transparante en tijdige communicatie kunnen organisaties uitdagingen proactief aanpakken en weloverwogen beslissingen nemen. Om deze uitdagingen het hoofd te bieden en de overstap naar de cloud succesvol te laten zijn, zijn organisaties het meest gebaat bij een holistische aanpak, waarbij rekening wordt gehouden met zowel de mensen als de processen en de technologie. Er moet sprake zijn van robuuste versleuteling en gedegen toegangsbeheer om de veiligheid van alle gegevens te waarborgen tijdens de overdracht en opslag van deze data in de cloud. Er moeten duidelijke verantwoordelijkheden en overeenkomsten worden gedefinieerd, zodat alle betrokkenen weten wat hun taken en verplichtingen zijn tijdens het migratieproces. Hieronder valt ook het afbakenen van de verantwoordelijkheden van de organisatie, de cloudprovider en eventuele andere leveranciers of partners. Door deze verantwoordelijkheden duidelijk te definiëren, kunnen organisaties misverstanden en hiaten in hun security of in de compliance van de wet- en regelgeving voorkomen. En door het implementeren van diverse strategieën (zoals robuuste versleuteling en toegangsbeheer, het uitvoeren van grondige risicobeoordelingen, het naleven van branchevoorschriften, het vaststellen van duidelijke verantwoordelijkheden en overeenkomsten, en het stimuleren van effectieve communicatie en samenwerking) kunnen organisaties deze uitdagingen het hoofd bieden en de migratie naar de cloud succesvol laten verlopen.

Je organisatie beveiligen: belangrijkste stappen om de security en compliance te handhaven

De snelle invoering van cloudcomputing heeft de manier waarop organisaties werken en meer schaalbaarheid, flexibiliteit en kostenbesparingen kunnen bieden, ingrijpend veranderd. Deze verschuiving brengt echter ook de noodzaak met zich mee om de security en compliance in de cloudomgeving prioriteit te geven.

Maar belangrijke dingen eerst, en daarom adviseren beleidsmakers, deskundigen en auditors de afnemers van clouddiensten vooral om goed te weten wat ieders taken en verantwoordelijkheden zijn volgens het gedeelde verantwoordelijkheidsmodel. Klanten wordt aanbevolen om best practices te hanteren, beleid en procedures bij te werken en hun controlemechanismen in lijn te brengen met de effectief ontworpen procedures. Door deze documenten regelmatig bij te werken en af te stemmen op nieuwe dreigingen, technologische ontwikkelingen en wettelijke voorschriften blijven de beveiligingsmaatregelen van de afnemer van de clouddiensten up-to-date en effectief om eventuele kwetsbaarheden te beperken.

Verder wordt het belang benadrukt om regelmatig uitgebreide beoordelingen uit te voeren om potentiële risico's in kaart te brengen. Door inzicht te hebben in de risico's kunnen cloudklanten gerichte strategieën ontwikkelen en hun middelen effectief inzetten om deze risico's te beperken. Het opstellen van een vastomlijnd plan voor incidentrespons helpt om beveiligingsincidenten effectief te beheren.
Door regelmatig logbestanden te beoordelen, voortdurend beveiligingsaudits uit te voeren en gebruik te maken van geavanceerde opsporingsmechanismen voor dreigingen kunnen kwetsbaarheden en eventuele inbreuken beter worden geïdentificeerd.

Op de hoogte blijven van relevante voorschriften en industriestandaarden is essentieel om aan alle regels en identificeren en ervoor zorgen dat organisaties best practices uit hun sector volgen. In deze context is regelmatige training nodig om iedereen alert te laten zijn op de juiste gang van zaken rondom security en compliance. Afnemers van clouddiensten wordt geadviseerd om de professionele ontwikkeling van hun medewerkers te ondersteunen. Bijvoorbeeld door kennisuitwisseling te stimuleren en medewerkers via cursussen, hubs of platforms op de hoogte te houden van best practices. Zo blijven medewerkers geïnformeerd over de nieuwste ontwikkelingen in het continu veranderende landschap van cloudbeveiliging.

Door deze aanbevelingen op te volgen, kunnen afnemers van clouddiensten hun beveiligingsstatus aanzienlijk verbeteren en de kans op significante inbreuken op hun beveiliging of overtredingen van de wet- en regelgeving verkleinen. Uitgebreide GRC-tools helpen cloudklanten bij het handhaven van deze basisvereisten. Deze tools bieden centraal beheer, vereenvoudigen risico-identificatie en -beoordeling, ondersteunen nalevingsbeheer, stroomlijnen het beheer van beleidsregels en controles, helpen bij incidentrespons en -beheer, faciliteren audits en rapportages, en

bevorderen voortdurende monitoring en beoordeling. Organisaties die gebruikmaken van deze tools kunnen hun cloudbeveiligingsstatus verbeteren, aan alle regelgeving voldoen en potentiële risico's effectief beperken.

Samengevat: security en compliance zijn cruciale aspecten van cloudcomputing vanwege de unieke risico's die ermee gepaard gaan. Het gedeelde verantwoordelijkheidsmodel schetst de taakverdeling tussen cloudproviders en hun klanten. Desalniettemin levert de interpretatie en effectieve implementatie van dit model de nodige uitdagingen op. Cloudgebruikers lopen tegen uiteenlopende moeilijkheden aan wat betreft het handhaven van hun cloudsecurity en compliance. Dit levert ingewikkelde situaties op waarvoor de oplossingen niet direct helder zijn. Om hun security en compliance te borgen doen organisaties er verstandig aan om risico-beoordelingen uit te voeren, de toegang tot hun omgevingen goed te beveiligen in lijn met de best practices, op de hoogte te blijven van de regelgeving, en ondersteuning te bieden aan hun teams om de implementatie van clouddiensten veilig en volgens de regels te laten verlopen. GRC-tools (voor governance, risicobeheer en compliance) bieden centraal inzicht en automatisering voor gestroomlijnde bestuursprocessen. Deze tools hebben echter wel beperkingen en vereisen aanvullende menselijke expertise en proactieve beveiligingsmaatregelen. Door prioriteit te geven aan security en compliance in de cloud en door passende maatregelen te nemen, kunnen cloudgebruikers hun risico's beperken, hun data beschermen en de voordelen van cloudcomputing optimaal benutten zonder dat de naleving van regelgeving in het geding komt.

Over de auteurs:

Yagmur Bozcuk

Yagmur werkt als Senior Consultant op het gebied van cybersecurity. Ze heeft een sterke achtergrond op het gebied van IT en audits van bedrijfsprocessen binnen uiteenlopende sectoren en met verschillende auditmethodes en kaders. Daarnaast heeft ze veel ervaring op het gebied van IT & cybersecurity en naleving.

Mail: yagmur.bozcuk@capgemini.com

LinkedIn: https://www.linkedin.com/in/yagmurbozcuk/

Rahul Mishra

Rahul is een zeer ervaren Managing Consultant met ruim tien jaar ervaring in toonaangevende adviesfuncties met betrekking tot audits, risico- en nalevingsbeheer op het gebied van cybersecurity. Rahul is gecertificeerd als ISO 27001 Lead Auditor, als Qualys Vulnerability Assessment Expert en heeft daarnaast verscheidene andere productcertificeringen op het gebied van cybersecurity.

Mail: rahul.f.mishra@capgemini.com

LinkedIn: https://www.linkedin.com/in/rahul-mishra-64990052/

Bronnen:

1. https://www.lucidchart.com/blog/hybrid-cloud-benefits

2. https://website.xebia.com/eu/digital-transformation/cloud/cloud-first-workplace/google-workspace?hsLang=en-us

3. https://dl.acm.org/doi/fullHtml/10.1145/3546068

4. https://www.linkedin.com/pulse/why-airbnb-using-aws-cloud-services-what-benefits-provides-saxena

5. https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/

6. https://www.edx.org/school/googlecloud

7. https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model

DIGITALE WEERBAARHEID EN BEVEILIGINGS BASELINES

Is een baseline zoals de BIO voldoende om digitaal weerbaar te zijn?

De Baseline Informatiebeveiliging Overheid (BIO) heeft tot doel om de informatiebeveiliging voor de overheid en haar diensten op een bepaald minimum niveau te krijgen. De BIO is gebaseerd op beheersmaatregelen uit de ISO 27002, aangevuld met overheid specifieke detailmaatregelen en een aantal maatregelen uit het VIR-BI (Voorschrift Informatiebeveiliging Rijksdienst- Bijzondere informatie) op het niveau Dep. V (Departementaal Vertrouwelijk). Baselines zijn doorgaans op compliancy gebaseerd en dat zegt nog niks over feitelijke weerbaarheid.

Digitale weerbaarheid omvat het voorbereiden op en het weerstaan van cyberaanvallen, terwijl tegelijkertijd de informatiesystemen operationeel blijven tijdens dergelijke aanvallen. Cyberweerbaarheid is door National Institute of Standards and Technology (NIST) gedefinieerd als:

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Cybersecurity resilience should be expressed as the amount of disruption your organization can avoid in its regular operations when a cybersecurity event occurs. Cybersecurity resilience is reinforced by protective security controls and reactive security controls[1].

Volgens deze definitie wordt gekeken naar de volgende onderdelen:

- **Anticipate:** het anticiperen wat er op je af komt, dit vertaalt zich door het opstellen van een dreigingsbeeld dat aangeeft welke actoren het op de organisatie voorzien hebben, op welke informatie of systemen ze uit zijn en hoe relevant de actuele dreiging is. Weten wat je kwetsbaarheden zijn en deze managen door te beginnen met de implementatie van basisprocessen en basismaatregelen.
- **Withstand:** in hoeverre kan de organisatie de aanvallen voorkomen en voldoende weerstand bieden, dit heeft met name de focus op preventieve maatregelen zoals firewalls, inbraak detectie, antivirus, toegangsbeheer en versleuteling van “belangrijke” informatie.
- **Recover from:** dit houdt in dat bij een ernstige verstoring de dienstverlening hersteld kan worden, hierbij ligt de focus op security incident response, business continuity, disaster recovery en het managen van de crisis die ontstaan is.
- **Adapt to adverse conditions:** betekent reageren op aanvallen en gecompromitteerde systemen, dit vraagt om detectie van aanvallen en het kunnen vaststellen van aangetaste systemen.

Highlights

- Digitale weerbaarheid is eenduidig te definiëren.
- De BIO alleen is niet voldoende voor het bereiken van digitale weerbaarheid.
- Een Security Operating Model draagt direct bij aan het structureren van security capabilities in de organisatie.
- De security capabilities die nog moeten worden aangevuld op de BIO zijn duidelijk aanwijsbaar en gedefinieerd.
- Digitale weerbaarheid is sterk gebaat bij een benadering vanuit dreigingen in plaats van compliance.

De vraag die rijst is of men aan de BIO voldoende heeft om deze bovengenoemde security capabilities in te vullen. Alle beheersmaatregelen staan erin, maar is dat genoeg om de business doelstellingen van de organisatie te waarborgen? Het structureren van security capabilities kan door middel van een Security Operating Model (SOM). Het SOM beschrijft de benodigde security capabilities en de governance daarvoor. Het BIO beschrijft security doelstellingen en maatregelen maar geen security capabilities op zich.

Een Security Operating Model (SOM) is een raamwerk dat wordt gebruikt om de beveiligingsmaatregelen en -processen van een organisatie te organiseren en te structureren. Het is een gestructureerde benadering die helpt bij het ontwerpen, implementeren en beheren van de beveiligingsfunctie van een organisatie.

Security Operating Model bewaakt samenhang

De samenhang tussen security capabilities wordt opgenomen in een SOM, dit SOM kent een twee sporen benadering: 1. beveiligen van de bestaande (legacy) systemen en 2. (innovatieve) beveiliging bieden aan nieuwe informatiesystemen. Het SOM kent een viertal domeinen, zoals weergegeven is in figuur 1.

- Strategie en Governance
- Beveilig en Transformeer
- Dynamische verdediging
- Innovatie en Beveiliging

Figuur 1: Standaard Security Operating Model (SOM).

Strategie en Governance

Dit domein bevat de kaderstellende security capabilities zoals:

- **Risicomanagement en compliancy-management**, voor het beheersen van de risico's (risico identificatie, risicoanalyse, risicobehandeling, risico monitoring en rapportages) en het aantoonbaar voldoen aan compliacy eisen.
- **Enterprise security architectuur** voor het in samenhang ontwerpen en inrichten van alle security capabilities.
- **Security awareness**, voor het beveiligingsbewustzijn van alle medewerkers in de organisatie die weten wat ze moeten doen als ze slachtoffer dreigen te worden van een cyberaanval.
- **Beleid, standaarden** en **richtlijnen** waarin de beleidsuitgangspunten voor security zijn opgenomen en doorvertaald zijn naar beleid op specifieke security gebieden (zoals Incident management, Vulnerability management en IAM- Identity and Access Management). Zij worden ondersteund door standaarden en richtlijnen voor implementatie.

Beveilig en Transformeer

- Dit zijn security capabilities die nodig zijn om de bestaande informatiesystemen en of operationele assets te beveiligen, hierbij kan gedacht worden aan IAM, Vulnerability management, Antivirus, Cryptografie, Netwerkbeveiliging et cetera.

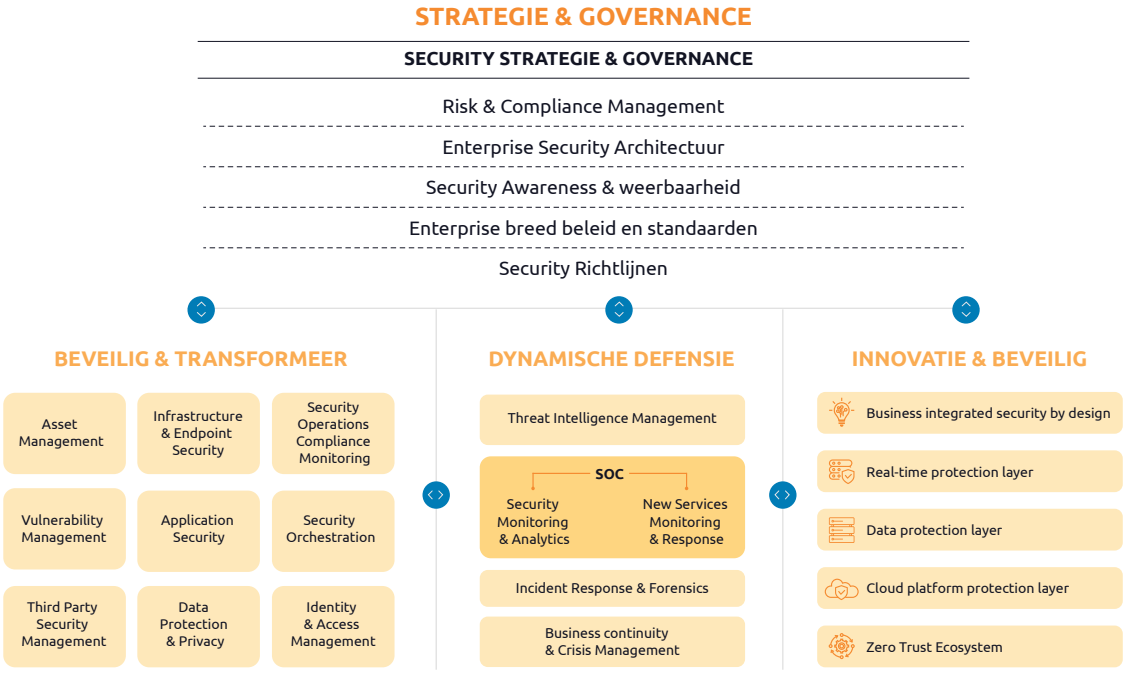
Dynamische verdediging

- Dit zijn security capabilities die gebruikt worden voor het tijdig detecteren van (pogingen tot) aanvallen (inbraakdetectie), dit te monitoren (Security monitoring, Threat modelling) en bij security incidenten adequate incident response, crisismanagement en indien nodig business continuity management op te schalen.
- Deze capabilities ondersteunen zowel de Beveilig en Transformeer als de Innovatie & Beveiliging SOM domeinen.

Innovatie en beveiliging

- Dit zijn security capabilities die bedoeld zijn om nieuwe diensten sneller te ondersteunen. Hierbij kan gedacht worden aan gebruik van cryptografie om gegevens overal te versleutelen, federatieve IAM om ketensamenwerking te bevorderen en cloud security om nieuwe diensten veilig in een cloud omgeving te laten landen.
- Naast security capabilities zal ook DevSecOps een belangrijke capability zijn om security in agile ontwikkelingen te waarborgen.

Een SOM voor een organisatie kan er uitzien zoals weergegeven is in figuur 2



Figuur 2: Voorbeeld SOM

Een SOM voor Cyberweerbaarheid

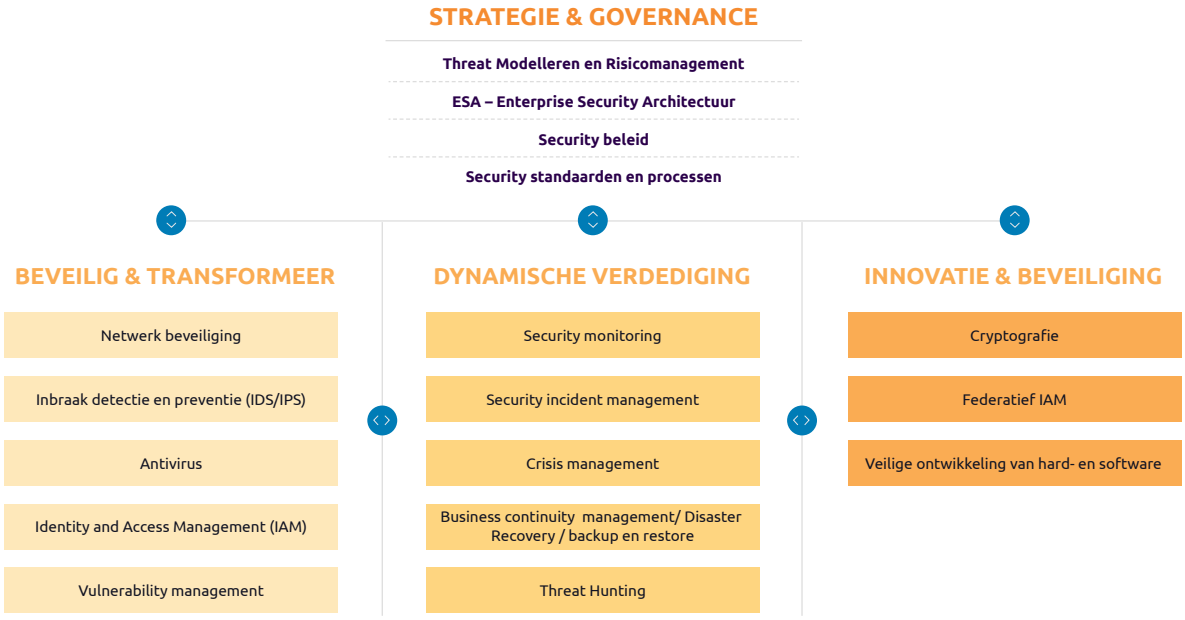
Als een organisatie cyber weerbaar wil zijn dan zijn de volgende security capabilities nodig, weergegeven in tabel 1, op basis van de invulling van de definitie van NIST.

Cyber weerbaarheid vraagt dus om veel security capabilities die in samenhang ontwikkeld en geïmplementeerd moeten worden, dit komt tot uiting in een securityprogramma die onder Enterprise security architectuur (ESA) wordt aangestuurd. Deze ESA zorgt voor inzicht, overzicht en samenhang van alle security capabilities.

Wanneer we dit presenteren als een SOM, ziet het eruit zoals afgebeeld in figuur 3.

ONDERDEEL	SECURITY CAPABILITY
Anticipate	• Threat modelleren en dreigingsbeeld. • Risicomanagement. • Security Standaarden. • Trainen en oefenen. • Classificatie van informatie. • Securitybeleid, plannen en procedures voor managen van dreigingen, Security incident management, IAM, Netwerkbeveiliging, Security Monitoring, Business continuity, Versleuteling, Scanning van systemen en bedienprocedures.
Withstand	• Netwerkbeveiliging. • Inbraakdetectie en inbraak preventie. • Antivirus. • Versleuteling. • Vulnerability management en patch management. • Veilige ontwikkeling van hardware en software.
Recover from	• Security incident management, crisismanagement. • Business continuity en Disaster recovery. • Change management (know to manage changes in a secure way). • Backup en restore.
Adapt to adverse condition	• Security Monitoring. • Threat Hunting.
Overview and insights	• Enterprise Security Architectuur (ESA). • Internal reporting en compliance. • Asset & configuration management (know what you have).

Tabel 1: Cyberweerbaarheid security capabilities



Figuur 3: Cyberweerbaarheid security capabilities

Het SOM en de BIO

Het BIO beschrijft security doelstellingen en maatregelen en geen security capabilities op zich. Kijkend naar de BIO dan is hieruit een SOM af te leiden zoals weergegeven is in figuur 4. De nummering van de onderstaande blokken komt overeen met de hoofdstukindeling van de BIO.

Dit SOM van de BIO lijkt grotendeels op het SOM die nodig is voor cyberweerbaarheid, wat we echter missen zijn de volgende security capabilities:

- **Dreigingen modelleren:** voor het opstellen van het dreigingsbeeld. Het dreigingsbeeld bevat een overzicht van de soort actoren (Statelijke actoren, Georganiseerde misdaad, Hacktivisme, Script kiddies, Insiders en Onderzoekers), bij voorkeur benoemd naar daadwerkelijke namen van de actor groepen. De informatiesystemen (IT) op de operationele assets (OT) waar zij het op gemunt hebben, de motivatie, mogelijkheden en de wil om het te doen. Het opgestelde dreigingsbeeld kan gebruikt worden om de Tactieken, Technieken en Procedures (TTP) van de actoren te monitoren.
- **Enterprise Security Architectuur (ESA):** voor het inzicht, overzicht en samenhang. De ESA beschrijft de samenhang van alle security capabilities, de onderlinge relaties en de wijze waarop dit in de tijd gezien (roadmap) geïmplementeerd moeten worden. De ESA is daarom een stuurinstrument voor verandering.
- **Threat Hunting (TH):** proactief zoeken naar compromittaties in de IT-en OT-omgevingen. Bij TH worden hypothesen opgesteld dat specifieke actor groepen reeds informatiesystemen of operationele asset hebben geïnfecteerd, met andere woorden zij zitten al in de systemen. Op basis van de hypotheses wordt onderzoek gedaan naar de mogelijke compromittatie.

De BIO vereist wel monitoring, maar voor cyberweerbaarheid zal er veel meer security monitoring ingericht moeten worden op cyber actoren en hun gedrag. Deze actoren en TTP's kunnen afgeleid worden van het opgestelde dreigingsbeeld.

Figuur 4: SOM van de BIO

Daarnaast beschrijft de BIO security incident management, in kader van cyberweerbaarheid zullen specifieke incident response playbooks opgesteld moeten worden in lijn met het dreigingsbeeld en hetgeen gemonitord kan en moet worden.

BIO compliancy alleen is niet voldoende om cyberweerbaar te zijn. De extra benodigde security capabilities kunnen worden gevonden in de SOM cyberweerbaarheid.

We bevelen aan om: focus te hebben op het opstellen van het dreigingsbeeld, ontwerp een security architectuur voor sturing op de security capabilities, ga ervanuit dat je gecompromitteerd bent en richt threat hunting in om dit vast te kunnen stellen.

Bronnen:

1. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf*

Over de auteurs:

Renato Kuiper

Renato Kuiper heeft meer dan 25 jaar ervaring in securityarchitectuur, cloud security, riskmanagement en IAM. Renato was gastdocent aan de executive master cybersecurity van de CSA (cybersecurity Academy). Hij is bestuurslid van de CSA (Cloud Security Alliance Nederland) en presenteert en publiceert regelmatig op het vakgebied van security Ten tijde van het schrijven van dit rapport was Renato Security Architact bij Capgemini.

LinkedIn: https://www.linkedin.com/in/renato-kuiper-3246733/

Jule Hintzbergen

Jule is een expert op het gebied van cybersecurity, met een focus op strategie, governance en implementatie. Hij brengt zijn kennis over als trainer voor Capgemini Academy. Jule is gepassioneerd over identiteits- en grensbeheer, en wijdt daar zijn tijd aan.

Mail: jule.hintzbergen@capgemini.com

LinkedIn: https://www.linkedin.com/in/jule-hintzbergen-17b486/

DE ONMISBARE ROL VAN HET BESTUUR IN THIRD-PARTY RISK MANAGEMENT

Hoe kunnen organisaties hun risicomanagement effectiever organiseren en ervoor zorgen dat het bestuur van de organisatie Third-Party Risk Management prioriteert (TPRM)?

ORGANISATORISCHE ASPECTEN VAN VEILIGHEID

Highlights

- Betrek het bestuur bij het vaststellen van rollen en verantwoordelijkheden.
- Geef het bestuur inzicht in het risicolandschap.
- Stel het bestuur op de hoogte van nieuwe inzichten.
- Creëer cyberbewustzijn bij het bestuur.
- Stel als bestuur de juiste vragen.

Steeds meer organisaties ondernemen stappen om hun cyberweerbaarheid te vergroten. Maar hoe zorg je ervoor dat je daarbij geen risico's uit het oog verliest? Een zeer groot deel van de cyberrisico's kan namelijk ook veroorzaakt worden door de derde partijen waar een organisatie op vertrouwt. Zo zag de Autoriteit Persoonsgegevens in 2021 een toename van 88% in datalekken waarvan een zeer groot deel ontstond bij derde partijen, met name IT-leveranciers[1]. Steeds vaker besteden organisaties veel van hun ondersteunende diensten uit, waardoor derde partijen steeds meer persoonsgegevens van klanten en van personeel verwerken. Denk bijvoorbeeld aan het recente datalek bij softwareleverancier Nebu, die haar diensten aan veel verschillende organisaties aanbiedt. Het datalek bij deze partij heeft zeker twee miljoen mensen getroffen, en onderstreept het belang van het beveiligen van de hele digitale keten[2]. Naast persoonsgegevens verwerken derde partijen ook interne informatie die als bedrijfskritisch kunnen worden beschouwd. Bovendien hebben derden soms zelfs directe toegang tot organisatie-systemen in het kader van samenwerkingsconstructies.

Het managen van risico's ten aanzien van derde partijen - ofwel Third-Party Risk Management (TPRM) - is dan ook een belangrijke trend binnen het cybersecurity domein en is een significante factor in het meten van de cyberweerbaarheid van een organisatie. Door de relatieve nieuwheid van het concept hebben veel organisaties het vaak nog niet op de radar. Een succesvol TPRM-programma valt of staat met het onderkennen van het belang van TPRM door het bestuur. Dit artikel gaat in op de manier waarop een TPRM-programma kan slagen en wat de rol is van het bestuur - het orgaan van een organisatie dat belast is met het dagelijks leiding geven aan een organisatie en het uitzetten van de koers.

Het vaststellen van rollen en verantwoordelijkheden

Het beschrijven en communiceren van rollen en verantwoordelijkheden is van belang in een succesvol TPRM-programma. Zonder een vastgesteld eigenaarschap van het TPRM-programma blijft het ad-hoc, stuurloos en onvoldoende ingebed in bestaande bedrijfsprocessen. Het bestuur van een organisatie zou hierin een belangrijke rol moeten spelen door het eigenaarschap voor TPRM te beleggen en het belang voor de organisatie uit te dragen naar de belangrijkste stakeholders.

Duidelijk gedefinieerde rollen en verantwoordelijkheden zorgen ervoor dat iedereen die betrokken is bij het TPRM-programma verantwoordelijk wordt gehouden voor zijn of haar acties. Dit helpt ervoor te zorgen dat risico's correct worden geïdentificeerd, beoordeeld en gemanaged.

Wanneer de belangrijkste stakeholders zijn geïdentificeerd, zoals de security- en privacyafdeling, het senior management, inkoop en andere proceseigenaren, is het belangrijk om te bepalen en te communiceren wat hun verantwoordelijkheden zijn in relatie tot TPRM.

Een belangrijk kenmerk van een succesvol TPRM-programma is dat het bestuur van een organisatie betrokken is bij het vaststellen van de rollen en verantwoordelijkheden. Daarmee onderschrijft het bestuur het belang van TPRM voor de organisatie en is het beter in staat om goed toezicht te houden op de uitvoering van het programma. Als eindverantwoordelijke van de organisatie is het de taak en verantwoordelijkheid om goed geïnformeerd te worden over TPRM-risico's die de continuïteit van de organisatie kunnen aantasten. Met behulp van deze informatie kunnen de juiste keuzes worden gemaakt, om grote incidenten, zoals datalekken of ransomware te voorkomen.

Begrijpen van het risicolandschap

Inzicht in het risicolandschap is essentieel voor iedere organisatie en als bestuurder ben je hoofdelijk aansprakelijk op het moment dat kritieke cybersecurity of privacy risico's worden genegeerd. Risico's ten aanzien van derde partijen vormen een belangrijk onderdeel van het risicolandschap van iedere organisatie. Zo hebben veel derde partijen toegang tot bedrijfs- en privacygevoelige gegevens en wisselen zij deze op hun beurt ook weer uit met andere organisaties. Zicht hebben op welke gegevens in beheer zijn van derde partijen is een belangrijke basis en randvoorwaarde in ieder TPRM-programma. Deze kennis helpt organisaties om risico's effectief te beheren en te mitigeren, zodat ze geen negatieve invloed hebben op de activiteiten of reputatie van de organisatie. Het inzichtelijk maken en houden van welke gegevens in het beheer zijn van derde partijen is veelal een gezamenlijke inspanning van de business stakeholders samen met de IT, privacy, security & risk afdelingen.

Begrip van het risicolandschap begint met het identificeren van derde partijen en het beoordelen van de negatieve impact die zij kunnen hebben op cybersecurity en privacy. Dit moet worden gedaan als onderdeel van de "due diligence" nog voordat er zaken worden gedaan met een derde partij, maar ook herhaald worden bij bestaande relaties, omdat het risicolandschap niet stilstaat.

Voor de derde partijen die een significante impact hebben op privacy en cybersecurity dient een risicoanalyse uitgevoerd te worden in overeenstemming met de belangrijkste stakeholders. Op basis van deze risico's kan een risico mitigatieplan worden opgesteld dat zich richt op het behalen van de beste resultaten tegenover de minste inspanning.

Het risicolandschap begrijpen is één , ervan op de hoogte blijven is weer een andere uitdaging.

Op de hoogte blijven van nieuwe inzichten

Het risicolandschap is constant in ontwikkeling. Iedere dag doen zich nieuwe dreigingen voor in de vorm van zero day vulnerabilities, virussen en ransomware. Het is de verantwoordelijkheid van het bestuur om op hoofdlijnen op de hoogte te zijn van de belangrijkste ontwikkelingen in het risicolandschap. Dit stelt hen in staat de juiste vragen te stellen aan de security en privacy experts die zich bezighouden met het beschermen tegen deze risico's.

In een recent onderzoek van Adaptive Shield blijkt dat organisaties met 10.000 SaaS-gebruikers die Microsoft 365 en Google Workspace gebruiken gemiddeld ruim 4.371 extra connected apps hebben[3]. Deze verbonden apps hebben allemaal een soort autorisatie voor bedrijfsgegevens, en in sommige gevallen zelfs het recht om alle bestanden te verwijderen van de apps waarmee ze verbonden zijn. Deze risico's zijn voor een aanzienlijk aantal organisaties niet of niet geheel bekend.

Derde partijen zoals leveranciers en ketenpartners kunnen daarnaast in de loop van de tijd de dienstverlening aanpassen, wat invloed heeft op de risico's die aan deze dienstverlening zijn verbonden. Door deze risico's periodiek in kaart te brengen, zijn organisaties ook beter in staat deze te managen.

TPRM is een doorlopend proces, gezien de context waarin het opereert continu verandert en daarmee dus ook de risico's. Het gebruik van een geautomatiseerd platform dat continu de aanvalsoppervlakte van derde partijen scant, in combinatie met auditing op gestructureerde basis zijn de sleutels tot het succesvol monitoren van risico's van derde partijen.

De juiste vragen stellen

Veel organisaties bevinden zich in de beginfase van hun TPRM-programma[4]. Als onderdeel van de organisatie brede dialoog over TPRM, heeft het meerwaarde als het bestuur het managementteam actief vragen stelt over welke elementen het TPRM-programma van de organisatie bevat. En daarnaast welke belangrijke elementen mogelijk nog missen. Door onder andere de volgende vragen te stellen, krijgen bestuursleden meer inzicht in de status en mogelijke uitdagingen van het TPRM-programma van hun organisatie:

- Zijn rollen en verantwoordelijkheden effectief gedefinieerd in het TPRM-programma van de organisatie?
- Betrekt de organisatie ook vierde, vijfde en zesde partijen in het TPRM-programma?
- Welke informatie krijgt het bestuur van het management met betrekking tot risico's van derden?
- Op welke niveaus, en met welke frequentie en relevantie wordt de informatie gepresenteerd?
- Worden interne audit en risicomanagement betrokken bij de beoordeling van het TPRM-programma? En zo ja, hoe?
- Welke tools gebruikt de organisatie om TPRM te meten en te beheren, en hoe effectief zijn ze? Hoe en naar wie worden risico's van derden geëscaleerd? Hoe effectief zijn mitigatiemaatregelen?
- Welke investeringen zou de organisatie kunnen overwegen om het TPRM-programma te verbeteren en te integreren in de hele organisatie?

Bewustzijn creëren

De hierboven beschreven aspecten leiden gezamenlijk tot meer bekendheid over TPRM op directieniveau. Om het doel van het ondersteunen van een TPRM-programma echter volledig te begrijpen, is het essentieel om ook op directieniveau bewustzijn te creëren over privacy en security in bredere zin.

Activiteiten om dit bewustzijn te vergroten kunnen bestaan uit het geven van inzicht in de specifieke risico's die kritieke derde partijen vormen voor de organisatie, hun profiel en impact waarmee de organisatie wordt geconfronteerd. Deze aspecten maken meestal deel uit van algemene bewustzijnsactiviteiten voor gegevensbescherming. De focus op TPRM-risico's zouop die manier eenvoudig kunnen worden afgestemd op bestaande activiteiten.

Bovendien kan het vertellen van informatie in verhalende vorm het bestuur helpen de TPRM-uitdagingen in bredere context te begrijpen. Bestuursleden lezen het nieuws, praten met vakgenoten en zijn doorgaans op de hoogte van grote cybersecurity-incidenten met betrekking tot derde partijen. Zo zijn incidenten in het supply chain-domein meestal een veelbesproken onderwerp. Het is nuttig om op de hoogte te zijn van verhalen over die incidenten en met name vergelijkingen te kunnen maken met de eigen organisatie. Op directieniveau gaat het vooral om herkenbaarheid: waarom kan een incident wel of niet bij onze organisatie plaatsvinden?

Tot slot betrekken sommige organisaties hun bestuursleden bij interne awareness trainingen. Een sterk voorbeeld is het betrekken van het bestuur bij incident-response trainingen samen met kritieke leveranciers. Door samen met elkaar een cyber incident, zoals een ransomware virus uitbraak te simuleren, wordt awareness gecreëerd over de impact van een incident op de organisatie. Door dergelijke simulaties is de organisatie in staat om te toetsen of de noodzakelijke maatregelen zijn genomen om zo bedrijfscontinuïteit te borgen.

Conclusie

Om antwoord te geven op de vraag hoe organisaties risicomanagement effectiever kunnen organiseren door TPRM op de kaart te zetten, is allereerst een vastgesteld eigenaarschap van Third-Party Risk Management (TPRM) essentieel. Dit is nodig zodat een duidelijke koers uitgezet kan worden en zodat het programma op een correcte manier ingebed kan worden in de bestaande bedrijfsprocessen. Het bestuur van een organisatie speelt een essentiële rol in het uitdragen van de verantwoordelijkheden van de stakeholders binnen de organisatie.

Daarnaast is inzicht krijgen in het risicolandschap essentieel voor het bestuur. Op basis van 'de vastgestelde' risico's kunnen mitigatiemaatregelen worden opgesteld om de risico's te vermijden of te verkleinen. Het is daarbij belangrijk om TPRM als een doorlopend proces te zien. Risico's veranderen continu. Om die reden zou het gebruik van een geautomatiseerd platform kunnen worden overwogen om de druk op de organisatie te ontlasten.

Door onder andere actief vragen te stellen met betrekking tot het TPRM-programma van de organisatie, krijgen bestuursleden meer inzicht in de status en mogelijke uitdagingen van het TPRM-programma van hun organisatie. Deze vragen gaan o.a. over rollen en verantwoordelijkheden, de scope van het TPRM-programma, rapporteren, betrokken actoren, tooling die gebruikt kan worden en vragen over verdere investeringen die het programma kunnen verbeteren.

Bronnen:

1. *https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken*
2. *https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen*
3. *https://www.adaptive-shield.com/saas-to-saas-3rd-party-app-risk-report-2023*
4. *https://www.gartner.com/en/newsroom/press-releases/2023-02-21-gartner-survey-shows-third-party-risk-management-misses-are-hurting-ororganizations.*

Over de auteurs:

Britt Huveneers

Als Senior Privacy Consultant bij Capgemini zorgt Britt voor het borgen van privacy compliance binnen publieke en private organisaties. Haar expertise ligt met name op het legitiem gebruik van (gevoelige) data, het gebruik van nieuwe technologieën en data ethiek.

Mail: ***britt.huveneers@capgemini.com***

LinkedIn: ***https://www.linkedin.com/in/britt-huveneers-b8b186114/***

Christiaan Koopman

Christiaan Koopman geeft Christiaan advies over de wijze waarop cybersecurity geborgen kan worden binnen bestaande en nieuwe bedrijfsprocessen. Zijn expertise ligt bij het implementeren van cybersecurity Strategie, IT-Risk Management en Governance & Compliance aan de hand van diverse normenkaders waaronder ISO 27001, BIO & ISAE 3402.

Mail: ***christiaan.koopman@capgemini.com***

LinkedIn: ***https://www.linkedin.com/in/christiaan-koopman/***

Manisha Ramsaran

Manisha adviseert organisaties over vraagstukken op het gebied van privacy en gegevensbescherming. Haar expertise ligt bij het implementeren van privacy by design principes, het adviseren over privacy risico's bij nieuwe processen/technologieën en het verhogen van bewustzijn over gegevensbescherming. Ten tijde van het schrijven van dit rapport was Manisha Privacy Consultant bij Capgemini.

LinkedIn: ***https://www.linkedin.com/in/manisha-ramsaran-91aa1b140/***

WAAROM BEDRIJFSCONTINUÏTEIT CRUCIAAL IS IN TIJDEN VAN MAATSCHAPPELIJKE ONRUST

Wat kunnen we leren van de omgang met business continuity management ten tijde van maatschappelijke onrust?

Highlights

- Organisaties richten zich met name op het reageren op en oplossen van een crisis of incident, maar verliezen vaak de focus op het voorzetten van de normale operatie.
- Organisaties zien crisismanagement, incident response en business continuity vaak als losse domeinen, terwijl er een essentiële samenhang van weerbaarheid bestaat tussen deze domeinen.
- Grote maatschappelijke gebeurtenissen kunnen een geduchte invloed hebben op business continuity, wat vaak over het hoofd wordt gezien in plannen.
- De migratie van de infrastructuur van een organisatie naar de cloud is van groot belang.
- Door als organisatie regelmatig de business continuity plannen te testen, kunnen verbeterpunten worden geïdentificeerd.

Sinds COVID-19 hebben landen meer te maken met maatschappelijke onrust[1]. Deze onrust wordt vaak gedreven door protesten over kwesties als economische tegenspoed, mogelijke klimaatzorgen, politiegeweld, etc. Dit zorgt voor onrust en problemen in de samenleving, iets wat invloed heeft op de normale gang van zaken. De acties tegen de pensioenhervormingen in Frankrijk zorgen er bijvoorbeeld voor dat wegen of sporen moeten worden afgesloten of zijn geblokkeerd, daarnaast is er sprake van een tekort aan benzine door acties bij raffinaderijen. Voor een land is het van belang om effectief te reageren op deze acties om de dagelijkse gang van zaken door te laten gaan. Dit geldt ook voor de digitale wereld. Dit artikel gaat in op het verband tussen maatschappelijke onrust en business continuity en biedt daarmee inzicht voor organisaties om hun veerkracht te verbeteren. Politieke en maatschappelijke onrust brengen namelijk ook risico's en dreigingen met zich mee zoals het hacken van kritieke systemen van een land of stad. Dit betekent concreet dat ook voor de cyberweerbaarheid van een samenleving het van groot belang is om aandacht te hebben voor business continuity.

Wat is business continuity?

Om het belang van business continuity tijdens maatschappelijke onrust duidelijk te maken is het essentieel om te begrijpen wat precies onder business continuity wordt verstaan. Hoewel er verschillende definities bestaan in het veiligheidsdomein, hanteren wij in dit de volgende definitie: business continuity is het vermogen van een organisatie om essentiële functies te handhaven tijdens en na een ramp. Het voorziet in risicobeheersingsprocessen- en procedures die als doel hebben onderbrekingen van bedrijf kritische diensten te voorkomen en te verhelpen en de organisatie zo snel en soepel mogelijk weer volledig te laten functioneren.

VOORDELEN VAN CERTIFICERING

Certificering helpt de veerkracht van een organisatie te vergroten, waarbij meer dan een kwart aangeeft dat het helpt om verzekeringskosten te verlagen

De voordelen van certificering voor organisaties

Figuur 1: Voordelen van certificering[2]

Gebrek aan focus

Ten tijde van demonstraties en protesten ligt de focus van een samenleving voornamelijk op het reageren op deze onrust, de normale gang van zaken in een samenleving wordt hierbij vaak overschaduwd. We zijn als samenleving immers getraind om op acute problemen te reageren en alles uit onze handen te laten vallen om een probleem op te lossen. Hierdoor raakt het gewone leven op de achtergrond bij een ramp of crisis. Ook in het bedrijfsleven ligt de focus binnen de weerbaarheid van een organisatie ten tijde van een cyberincident vaak op het reageren op crises of het oplossen van een incident. Veel aandacht gaat uit naar de principes van de crisismanagement cyclus (response, recovery, mitigation, preparedness). Hoewel er plannen zijn voor verschillende scenario's, wordt er minder nagedacht over het feit dat de normale bedrijfsvoering van essentieel belang is, niet alleen na een crisis maar, ook tijdens een crisis. Dit is van belang om de gezondheid en continuïteit van de organisatie te waarborgen. Voor bedrijfscontinuïteit bestaan er International Standardization Organizations (ISOs), waarin best practices en normen samengesteld zijn. Deze worden vaak over het hoofd gezien of ze vallen buiten de focus van de business continuity management of crisis management afdeling van een organisatie. Business ccontinuity activiteiten zijn essentieel omdat ze een organisatie in staat stellen om tijdens de crisis tenminste op een minimaal niveau te blijven draaien. Business continuity activiteiten helpen de organisatie veerkracht te behouden door snel te reageren op een onderbreking. Een effectieve aanpak van de business continuity bespaart geld, tijd en de reputatie van de organisatie. Een langdurige uitval kan namelijk leiden tot onder andere financiële en reputatieschade. In figuur 2 staat een overzicht van ISO-normen die verband houden met bedrijfscontinuïteit en maatschappelijke onrust.

Domeinen en de overlap

Binnen ons werkveld zien we vaak dat organisaties hun weerbaarheidsafdeling splitsen in een aantal onderdelen, zoals incident response, crisismanagement en business continuity, met elk aparte rapportagelijnen. De onderdelen vallen geregeld onder dezelfde afdeling, maar de samenwerking tussen deze onderdelen is niet altijd goed zichtbaar. Hierin kunnen organisaties verbeteren, want juist met samenwerking wordt een organisatie weerbaarder. In organisaties met gesplitste disciplines is het een uitdaging als er echt een crisis gaande is, omdat de gebeurtenis vanuit verschillende lenzen wordt bekeken. Als het gaat om technische incidenten, speelt business continuity vaak een kleine of geen rol bij de afhandeling. Hierbij ontbreekt af en toe een gevoel van de ernst van de impact op de organisatie en de passende acties die nodig zijn vanuit management worden pas later duidelijk. Dit gebrek aan integratie en samenwerking kan leiden tot een vertraagde respons van de organisatie en reputatieschade. Meer integratie tussen crisismanagement, business continuity management en incident response kan dus het vermogen van een organisatie om te reageren op een verstorende gebeurtenis verbeteren door het risico van vertragingen, tegenstrijdige prioriteiten en miscommunicatie te verminderen.

THE ISO 223XX SERIES – SOCIETAL SECURITY

INCREASE ORGANIZATION'S	WHAT IT ADDRESSES
ISO 22300:2012	Societal Security-- Vocabulary
ISO 22301:2012	Business Continuity Management Systems -- Requirements
ISO 22311:2012	Video Surveillance
ISO 22313:2012	Business Continuity Management Systems - Guidance
ISO 22315:2014	Mass Evacuation - Guidelines
ISO 22320:2011	Emergency Management – Requirements for Incident Response
ISO 22322:2015	Emergency Management – Guidelines for Public Warning
ISO 22324:2015	Emergency Management – Guidelines for Color-Coded Alert
ISO 22351:2015	Emergency Management – Message Structure for Interoperability
ISO 22397:2014	Guidelines for Establishing Partnering Arrangements
ISO 22398:2013	Guidelines for Excersises
ISO 22399:2007	Guidelines for Incident Preparedness and Operational Continuity Management

Figuur 2: ISO normen rondom business continuitiy en maatschappelijke onrust[3]

Onrust zorgt voor gebrekkige business continuity

In het licht van diverse maatschappelijke gebeurtenissen zoals natuurrampen, terroristische aanslagen en pandemieën, is de focus op bedrijfscontinuïteit toegenomen. Hoewel de focus tijdens de coronapandemie al aan het verschuiven was, blijkt uit verschillende studies[4] dat er nu een verschuiving plaatsvindt naar onderwerpen als geopolitieke veranderingen en natie-tot-natie conflict. Bij geopolitieke veranderingen wordt er vooral gekeken naar de strategische gevolgen hiervan, zoals veranderende bondgenootschappen en afhankelijkheden, strategische kracht van buitenlandse hulp en oplegging van sancties, maar ook de commerciële vergeldingsmaatregelen tegen landen en bedrijven. Bij vijandige acties van natie tot natie moet men denken aan oorlog, andere gewapende conflicten, staatterrorisme, pogingen om verkiezingsuitslagen te beïnvloeden en het aanwakkeren van politiek protest.

Invloed op het voortbestaan van organisaties

Al deze zaken kunnen een grote invloed hebben op een organisatie en op het voortbestaan hiervan. Bedrijven kunnen namelijk beslissen om niet meer te opereren voor- of in een bepaald land vanwege de onrust die hier heerst. Het is bijvoorbeeld vaak niet meer haalbaar vanwege supply chain problemen. Deze problemen kunnen bij bepaalde organisaties van desbetreffende omvang zijn dat het een te groot gedeelte van de totale operatie van de organisatie beïnvloeden. Het is belangrijk om dergelijke uitdagingen aan te pakken door te kijken naar onderwerpen met betrekking tot bedrijfscontinuïteit bij het opstellen en bijwerken van de bedrijfscontinuïteitsplannen. Een voorbeeld van een ondersteunende tool voor organisaties is threat intelligence-analyse.

Cloud zorgt voor een verbeterde business continuity

Een aanval op maatschappelijk relevante IT-systemen kan grote impact hebben. In 2021 werd het zorgsysteem in Ierland getroffen door ransomware[5]. Dit had een grote invloed op de bedrijfsvoering van het zorgsysteem in het land. Patiëntgegevens waren niet beschikbaar voor zorgmedewerkers en patiënten, afspraken werden afgezegd en het terugzetten van alle servers en applicaties duurde vier en een halve maand. Toegang tot kritieke gegevens, processen en systemen is van belang om de continuïteit van de zorg te waarborgen. Gebruik maken van de cloud, wat inhoudt dat data online wordt opgeslagen en kan worden opgevraagd, kan een positief effect hebben op de business continuity.

Voordelen van cloudgebruik

Een goed doordachte implementatie van cloud-gebaseerde software in een organisatie kan de business continuity vergroten met gemakkelijk toegankelijke back-ups en vrijwel onbeperkte schaalbaarheid. Veel organisaties zijn nog erg afhankelijk van interne netwerken, datacenters en inefficiënte verouderde technologie, waardoor zelfs een plaatselijk stroom- of internetstoring al voor veel ongeplande downtime kan zorgen. Door het gebruik van de cloud kan de downtime van een organisatie aanzienlijk worden verminderd. Bedrijfskritische processen en applicaties kunnen nog steeds worden uitgevoerd zonder vaak terug te hoeven vallen op fysieke alternatieven. De cloud biedt onbeperkte mogelijkheden voor gegevensopslag in ruil voor betaling. Dit maakt de business continuity sneller haalbaar aangezien eindgebruikers vanaf elk apparaat met internetverbinding toegang hebben tot de gegevens. Een voorbeeld van de effectiviteit is zichtbaar geworden tijdens de mogelijkheid tot thuiswerken tijdens COVID-19. Organisaties konden door het gebruik van de cloud het personeel dezelfde werkzaamheden laten uitvoeren die normaliter op locatie werd gedaan.

Hoe ziet die positieve invloed van de cloud eruit?

De cloud zorgt ook voor een effectieve disaster recovery, waarbij continu een back-up naar de cloud wordt geschreven zodat kritieke gegevens worden beschermd tegen rampen en/of aanvallen. De cloud kan het effect van bepaalde cyberaanvallen zoals een DoS-aanval verminderen. Een DoS-aanval is erop gericht de IT-systemen te overweldigen zodat de normale werklast niet meer gedragen kan worden. Cloud services kunnen worden geschaald om aan een bepaalde vraag te voldoen, waardoor het effect van bijvoorbeeld een DoS-aanval minder is en dus bescherming biedt. Het toepassen van multi-cloudstrategieën waarbij back-ups staan opgeslagen bij meerdere cloudleveranciers, voorkomt dat een organisatie afhankelijk is van een enkele back-up.

Oefenen en trainen zorgt voor effectieve werking

Het succes van de business continuity plannen is afhankelijk van het vermogen van het personeel om plannen effectief te ontwikkelen, te documenteren en vooral uit te voeren. Dit betekent dat om de plannen effectief te laten werken, het personeel getraind moet zijn door middel van opleiding en oefening. Wanneer het personeel traint en oefent met het volgen van business continuity plannen, kan een organisatie doeltreffender reageren. Personeel moet ook vertrouwd zijn met de communicatiemiddelen en de middelen waarmee zij zullen worden ingelicht door bijvoorbeeld technische medewerkers omtrent business continuity problemen. Senior managers die betrokken zijn bij de reactie van het bedrijf moeten bekend zijn met de beschikbare instrumenten en hun verantwoordelijkheden tijdens een incident. Dit helpt om de strategieën te valideren en de reactietijd te verkorten. Een voorbeeld van het oefenen is het uitvoeren van een table-top oefening die in real time wordt uitvoert tijdens een gesimuleerd incident.

Business continuity is cruciaal ten tijde van maatschappelijke onrust

Tijdens de protesten in Frankrijk werd met name gefocust op de chaos die door bepaalde ontwikkelingen werd gecreëerd. Organisaties zouden zich ten tijde van maatschappelijke onrust bewust moeten zijn dat niet alleen de onrust moet worden aangepakt, maar ook de dagelijkse gang van zaken niet uit het oog verloren moet worden. Uit het artikel blijkt dat business continuity een belangrijk onderwerp is voor organisaties. Het is van belang om als organisatie duidelijke plannen en richtlijnen op te stellen of bestaande plannen en richtlijnen te beoordelen waarbij de link tussen de verschillende onderdelen zoals crisismanagement en incident response in acht wordt genomen. Door te richten op vernieuwde strategieën, zoals het combineren van cloudgebruik met oefening en training in het beheer van bedrijfscontinuïteitsactiviteiten, kan een effectievere benadering van continuïteit tijdens maatschappelijke onrust worden bewerkstelligd. Door op deze wijze om te gaan met business continuity management ten tijde van maatschappelijke onrust wordt het de normaalste zaak van de wereld.

Over de auteurs:

Manouck Schotvanger

Manouck is een cybersecurity Consultant en is gespecialiseerd in crisis- en beveiligingsmanagement binnen het cyberbeveiligingsdomein. Ten tijde van het schrijven van dit rapport richtte ze zich op bedrijfscontinuïteit en crisismanagement met betrekking tot de publieke en private sector.

LinkedIn: https://www.linkedin.com/in/manouck-schotvanger/

Rachel Splinters

Rachel is cybersecurityconsultant met een specialisatie in crisis- en beveiligingsmanagement binnen het cyberdomein en richt zich op het ontwikkelen van cybercrisisoefeningen voor de publieke en private sector.

Mail: rachel.splinters@capgemini.com

LinkedIn: https://www.linkedin.com/in/rachel-splinters-6825b7137/

Bronnen:

1. *https://drive.drii.org/2022/12/08/8th-trends-report/*
2. *https://www.globenewswire.com/news-release/2023/06/14/2688019/0/en/ACT-Achieves-HITRUST-Certification-for-Healthcare-Services.html*
3. *https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity*
4. *https://drive.drii.org/2022/12/08/8th-trends-report/*
5. *https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf*

DE PERFECTE MATCH: HOE KIES JE DE IDEALE SECURITY SERVICE PROVIDER VOOR JOUW ORGANISATIE?

Technische eisen zijn goed te bepalen, maar wat verwacht je aan service-ervaring?

Highlights

- Een goede Managed Security Service Provider (MSSP) richt zich op de 'service-experience'.
- Service-experience kent drie type kenmerken: people, process en business.
- Bij processen tussen organisatie en een MSSP is de regievorm belangrijk.
- De drie meest voorkomende regievormen zijn: een leverings-, directie- of een vraagorganisatie.
- Jouw organisatie zoekt specialisten, die een MSSP standaard al heeft.

Bij de gemiddelde aanbesteding wordt de meeste aandacht besteed een de functionele eisen. Helaas komt men er vaak na afloop achter dat de verkregen dienstverlening niet helemaal bevalt. Gelukkig is dit een bekend probleem, waarvoor een oplossing al bestaat.

Functionele eisen zijn een onmisbaar onderdeel. De meeste serviceproviders kunnen, op verschillende manieren, hieraan voldoen. Wanneer ze dat niet kunnen, wordt dat vroegtijdig duidelijk. Om die reden gaan we voor dit artikel de functionele eisen overboord gooien en ons richten op de niet functionele eisen, oftewel: de 'service-experience'.

Service-experience kent veel varianten, maar het moet vooral aansluiten op jouw wensen. Zaken zoals bedrijfscultuur, niveau aan formaliteit, volgen we de letter- of de intentie van het contract etc. Dezelfde service-experience die ervoor zorgt dat jouw medewerkers effectief en prettig samen kunnen werken met jouw gekozen Managed Security Service Provider (MSSP) zal daarom ook de meest effectieve security service met zich mee brengen.

De kenmerken van service-experience kunnen we in drie primaire categorieën indelen:

1. People
2. Process
3. Business

Security is mensenwerk

Wanneer we het over mensen hebben kunnen we er niet meer omheen: het nieuwe werken en het tekort aan technisch specialisten. Met een wereldwijde vraag naar 3.5 miljoen cyberspecialisten[1] en een veranderende norm naar meer flexibiliteit[2] voor de werknemer is de arbeidsmarkt enorm competitief.

De arbeidsmarkt is zelfs zo competitief, dat jouw organisatie dezelfde 'skill-shortage' ervaart als een MSSP. Dit hoeft geen probleem te zijn, tenzij beide organisaties hetzelfde bedrijfs-culturele profiel zoeken. Indien je een complementair profiel zoekt wordt het juist een voordeel. Jouw MSSP zal namelijk aantrekkerlijker zijn voor ander personeel dan jouw organisatie.

In hoofdlijnen zijn er vier factoren die de cultuur bepalen;

- Globalisering: ben je een globale organisatie of juist een lokale?
- Prestaties: hoe ziet succes eruit en hoe wordt dit behandeld?
- Demografie: wat is de gemiddelde leeftijd en culturele achtergrond van jouw personeel?
- Hiërarchie: hoe wordt er omgegaan met hiërarchie?

Nu is het interessante dat wanneer we jouw waardes van prestatie, demografie en hiërarchie uitlijnen op die van jouw MSSP, we in de praktijk zien dat de zakelijke relatie gemakkelijker tot stand komt. Wat op den duur weer resulteert in een efficiënter opererende organisatie tussen klant en leverancier.

Globalisering is de vreemde eend in de bijt. Waar we zien dat sommige mensen geen interesse hebben in een internationale werkomgeving, is dit voor andere juist een must. Hierin kan jouw MSSP een interessante rol spelen. Wanneer een MSSP namelijk een tegenovergestelde waarde heeft dan die van jou, kunnen zij specialisten aantrekken die je als organisatie mis zou lopen.

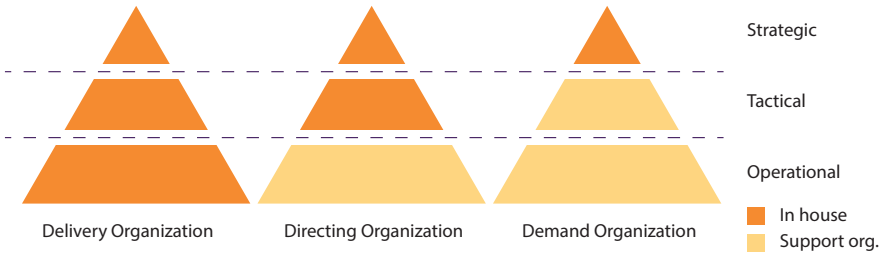
Uiteindelijk zijn de interacties tussen mensen te complex om samen te vatten in een enkel artikel. Zeker is wel dat het personeel dat je MSSP aanwijst om een dienst te leveren een goede relatie moet kunnen opbouwen met het personeel dat de geleverde dienst benut. Als dit niet werkt, zullen zowel de processen als de techniek niet kunnen helpen.

Processen maken de dienst, maar jij neemt de beslissing

Verschillende diensten hebben verschillende processen. Een auto wassen is namelijk niet hetzelfde als een cloud migratie. Maar wanneer we het hebben over processen tussen je organisatie en je MSSP is het vooral belangrijk om na te denken over de

regievorm. Het verschil in regie bepaalt namelijk de mate van inspraak die je hebt op operationeel, tactisch of strategisch niveau.

Wij benoemen drie primaire regievormen: Een leverings-, directie- of een vraagorganisatie (figuur 1).



Figuur 1: Regievormen

Bij een leveringsorganisatie worden zowel de operationele, tactische en strategische zaken door de eigen organisatie beheerd. Er kan uiteraard wel sprake zijn van detachering vanuit een MSSP maar de regie blijft compleet bij jou.

Wanneer de operationele activiteiten uitbesteed worden, maar de tactische en strategische regie behouden blijft, spreken wij over een directieorganisatie. Hierbij is de MSSP uitvoerend betrokken maar verricht werkzaamheden uitsluitend op verzoek. Een service desk is hier een klassiek voorbeeld van: geen ticket, geen service.

Mag de MSSP ook tactische beslissingen nemen om de organisatie te ondersteunen? Dan spreken wij van een vraagorganisatie. Hierbij bepaal je nog wel de strategie maar laat je de invulling over aan de MSSP. Hierbij moet je denken aan een dienst voor werkplekbeheer. Je geeft aan een beveiligde werkplek te willen voor jouw personeel, de MSSP bepaalt vervolgens om een combinatie van antivirus en configuratie hardening toe te passen.

Natuurlijk kan je verschillende regie vormen hanteren bij verschillende diensten. Uiteindelijk kan je de keuze het beste baseren op je inhoudelijke kennis. Heb je de expertise in huis om tactische of operationele beslissingen te nemen?

Business enablement door security services

Tot slot komen we tot het onderwerp de business. Zoals de IT ondersteunend is aan de business, zo moet security ook als een enabler gezien worden. Denk hierbij aan zaken zoals wet- en regelgeving, maar ook aan de bedrijfscontext en groei ambitie.

Wet- en regelgeving hebben een duidelijke link met een MSSP, er zijn immers zaken waar je aan moet voldoen. Hier kan een MSSP bij helpen en een ervaren partij zal hier zelfs al mee bekend zijn. Simpelweg omdat deze wetten en regels ook voor andere organisaties gelden.

Maar wanneer we kijken naar de bedrijfscontext en ambitie om te groeien ontstaat een uniek beeld. De ene organisatie is immers de andere niet. Een MSSP vinden die jou begrijpt en jouw belangen kan behartigen is daarom gewenst.

Jouw groeiambitie is hier een goed voorbeeld van. Een MSSP zal vaak ‘optionele’ diensten aanbieden. Dit zijn activiteiten die pas in rekening gebracht worden wanneer je hier om vraagt. Dit geeft zowel flexibiliteit als transparantie, maar kan onwenselijk zijn indien je van plan bent hier vaak gebruik van te maken. Neem bijvoorbeeld een personeelsscreening; hiervoor zou een MSSP een vast bedrag per screening kunnen rekenen. Maar als je de ambitie hebt je personeelsbestand significant uit te breiden over de komende jaren, is dit wellicht niet optimaal. Een structuur waarbij de dienst meegroeit is wellicht wenselijker.

Hier vinden we een bruggetje naar de bedrijfscontext. De organisatie heeft een primaire taak, wat niet het beveiligen van de IT is, want daar valt geen bestaansrecht uit te ontlenen. Maar wanneer de MSSP een goed begrip heeft van waar jij jouw bestaansrecht wel aan ontleent kunnen zij beter ondersteunen. Neem weer het voorbeeld van het groeiende personeelsbestand en de screening service. Is jouw primaire taak gebaat bij het hebben voor een groot personeelsbestand, of is er sprake van seizoensarbeid?

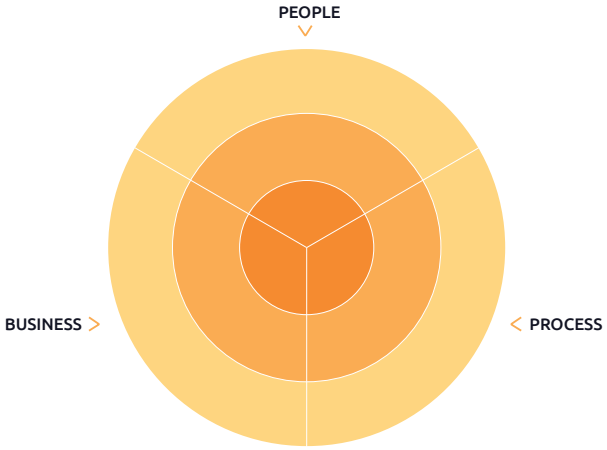
In het laatste geval is het wel zo prettig als de MSSP begrijpt dat er sprake zal zijn van piekbelasting en er geen werk blijft liggen.

De drie overwegingen die jij moet maken

Om tot een gedegen MSSP selectie te komen zijn er diverse overwegingen te maken. Hiervoor is het belangrijk om eerst jouw eigen wensen scherp te krijgen. Wil je een strategische, tactische of operationele focus van je MSSP. Deze focus zal overwogen moeten worden over de assen van people, process en business (figuur 2).

Alles overziend kunnen alle opties van waarde zijn. Ons advies is om daarom stil te staan bij de volgende overwegingen:

- Hoe wil ik onze mensen zien samenwerken?
- Hoe wil ik interactie hebben met onze MSSP
- Hoe wil ik richting geven aan onze MSSP



	PEOPLE	PROCESS	BUSINESS
Strategic	Demographic	Demand	Bus. Strategy
Tactical	Hierarchy	Direct	Bus. Tactics
Operational	Performance	Delivery	Bus. Operations

Figuur 2: MSSP selectieoverwegingen

Bronnen:

1. *https://fortune.com/education/articles/the-3-cybersecurity-hiring-trends-experts-predict-for-2023/*
2. *https://www.dbxuk.com/statistics/cyber-security-risks-wfh*

Over de auteurs:

Arjen van der Post

Arjen is een Senior Delivery Manager met uitgebreide ervaring in transities en transformaties en het leveren van nieuwe diensten aan een verscheidenheid van klanten binnen de Capgemini Infrastructure Services en cybersecurity unit.

Mail: arjen.vander.post@capgemini.com

LinkedIn: https://www.linkedin.com/in/arjen-van-der-post-75627714/

Dick Bruines

Dick heeft al meer dan twintig jaar ervaring binnen service management. Hij levert IT- en beveiligingsdiensten aan klanten door een balans te vinden tussen contractuele overeenkomsten en wat klanten daadwerkelijk nodig hebben. Dick heeft gewerkt met zowel kleine als grote teams, altijd met de focus op het succes en het partnerschap met de klant.

Mail: dick.bruines@capgemini.com

LinkedIn: https://www.linkedin.com/in/dick-bruines-a1619a2/

Sebastiaan de Vries

Sebastiaan de Vries is een ervaren Security expert die naast zijn technische kennis ook op de hoogte is van de laatse compliance standaarden. Hij houdt zich bezig met het helpen van klanten door security te veranderen van een noodzaak naar een voordeel.

Mail: sebastiaan.de.vries@capgemini.com

LinkedIn: https://www.linkedin.com/in/gsdevries/

NAVIGEREN DOOR NIS2: ORGANISATORISCHE STRUIKELBLOKKEN EN OPLOSSINGEN

Wat zijn de drie grootste uitdagingen voor organisaties bij het implementeren van de NIS2-richtlijn?

Op 16 januari 2023 trad de Network and Information Security Directive 2 (NIS2-richtlijn) in werking als opvolger van NIS1, de voorgaande richtlijn uit 2016. De NIS2-richtlijn vereist dat essentiële en belangrijke entiteiten maatregelen nemen om cyberbeveiligingsrisico's en incidenten adequaat te beheren. De herziene richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties. De Europese lidstaten zijn verplicht om deze richtlijn om te zetten naar landelijke wet- en regelgeving. Uiteindelijk moeten alle lidstaten per 18 oktober 2024 de NIS2-richtlijn om hebben gezet naar landelijke wet- en regelgeving.

Gezien het toenemende aantal cyberaanvallen overal ter wereld en de snelgroeiende afhankelijkheid van (digitale) infrastructuren lijkt de vervanging van de NIS1- door de NIS2-richtlijn op het juiste moment te komen. NIS2 introduceert een aantal welkome veranderingen. Het omvat strengere en explicietere cyberveiligheidsvereisten die kansen bieden om de beveiliging in organisaties te verbeteren en hun risico's te verminderen. Desalniettemin brengt de naleving van NIS2 ook kosten met zich mee en plaatst de implementatie ervan organisaties onvermijdelijk voor de nodige uitdagingen.

Highlights

- De drie grootste uitdagingen met betrekking tot de implementatie van de NIS2-richtlijn zijn (1) het toepassingsbereik, (2) SCRM (risicobeheer in de supply chain) en (3) de meldplicht over het beheer van beveiligingsincidenten (SIM).
- De NIS2-richtlijn is van toepassing op een groter deel van de economie en samenleving.
- De NIS2-richtlijn omvat strengere en explicietere vereisten voor cybersecurity.
- De NIS2-richtlijn stelt strengere eisen aan toezicht en naleving van de regelgeving.
- Elke uitdaging met betrekking tot de NIS2-richtlijn biedt ook kansen voor een betere beveiliging en minder risico's in essentiële en belangrijke organisaties.

NIS2 en de veranderingen voor het cybersecuritylandschap

Zoals we in de introductie al stelden, is NIS2 eerder dit jaar van kracht geworden en bevat de richtlijn behoorlijk wat veranderingen vergeleken met zijn voorganger, NIS1. Maar wat zijn deze veranderingen? Hoe verandert NIS2 het cybersecuritylandschap en wat betekent dit precies voor organisaties? We zetten de belangrijkste veranderingen op een rij.

1. Grotere reikwijdte

Onder NIS2 wordt de identificatie van entiteiten die binnen de reikwijdte vallen niet meer uitgevoerd door sectorspecifieke landelijk bevoegde autoriteiten (zoals De Nederlandsche Bank). In plaats daarvan vallen alle middelgrote of grote ondernemingen die in een van de onderstaande (sub) sectoren actief zijn en die een van de hierna genoemde type diensten leveren onder de reikwijdte van NIS2. NIS2 is ook van toepassing op sommige entiteiten die, ongeacht hun omvang, aan bepaalde voorwaarden voldoen. Als zodanig omvat NIS2 alle sectoren die al onder NIS1 vielen, maar dan aangevuld met een aantal nieuwe sectoren. Hierdoor beslaat de tweede richtlijn duidelijk een groter deel van de economie en samenleving dan zijn voorganger, NIS1, zoals te zien is in figuur 1.

Verder maakt de NIS2-richtlijn geen onderscheid meer tussen aanbieders van essentiële diensten (OES) en digitale dienstverleners (DSP), maar is er voortaan sprake van 'essentiële' en 'belangrijke' entiteiten, waarbij het onderscheid wordt gemaakt afhankelijk van het kritieke karakter van de betreffende sector[2].

Ook is de NIS2-richtlijn straks niet alleen van toepassing op belangrijke of essentiële entiteiten die in de EU-lidstaten zijn gevestigd, maar ook op belangrijke of essentiële entiteiten die hun diensten aan de respectievelijke lidstaten aanbieden[3]. Als zodanig wordt de NIS2-richtlijn een richtlijn met een

*Sectoren uitgebreid in NIS2

Figuur 1: Verschillen in de reikwijdte tussen NIS1 en NIS2

extraterritoriale werking, vergelijkbaar met de Algemene Verordening Gegevensbescherming (AVG).

2. Expliciete en strengere vereisten op het gebied van cybersecurity

NIS1 stelde dat aanbieders van essentiële diensten en digitale dienstverleners passende en evenredige technische en organisatorische beveiligingsmaatregelen moesten nemen om de risico's van de netwerk- en informatiesystemen die ze gebruiken voor de uitvoering van hun activiteiten te beheersen. Aanbieders van essentiële diensten onder NIS1 moesten passende maatregelen nemen om incidenten te voorkomen. Als zich toch incidenten voordeden, moesten ze de gevolgen ervan voor hun netwerk- en informatiesystemen beperken om de continuïteit van essentiële diensten te waarborgen. Tot slot stelde de NIS1-richtlijn dat aanbieders van essentiële diensten, in geval van een incident met aanzienlijke gevolgen voor de continuïteit van de essentiële dienstverlening, daarvan onverwijld melding moesten maken bij de bevoegde autoriteit of bij het landelijke Computer Security Incident Response Team (CSIRT). Deze meldingen moesten alle informatie bevatten waarmee de bevoegde autoriteit of het landelijke CSIRT eventuele grensoverschrijdende gevolgen van het incident kon vaststellen[4].

De NIS2-richtlijn maakt deze vereisten nog explicieter. Allereerst omvat de NIS2-richtlijn een opsomming van veiligheidsmaatregelen die alle entiteiten moeten implementeren om de beveiligingsrisico's voor hun netwerken en informatiesystemen te beheersen. Hiermee moeten incidenten worden voorkomen en, indien deze zich toch voordoen, de gevolgen ervan voor de afnemers van hun diensten worden beperkt (zie figuur 2).

Ten tweede vereist de NIS2-richtlijn expliciet dat entiteiten risico's in de supply chain beheren en beperken door het uitvoeren van due diligence-onderzoeken op het gebied van cybersecurity. Dit betekent dat organisaties die oorspronkelijk niet binnen de reikwijdte van NIS2 vielen nu ook cyberveilig moeten zijn. Een logische stap, aangezien het aantal cyberaanvallen in de supply chain de afgelopen drie jaar met 742% is toegenomen[6].

Ten derde voorziet NIS2 in een verbetering van de bestaande rapportageverplichtingen die onder NIS1 van kracht waren. Voortaan moeten alle significante incidenten of grote cyberdreigingen die een significant incident tot gevolg zouden kunnen hebben, binnen 24 uur gemeld worden bij het landelijke CSIRT of bij de relevante toezichthoudende instantie. Daarnaast moet binnen 72 uur melding worden gedaan van het incident en moet er binnen uiterlijk een maand na het incident een eindrapport worden ingediend. De NIS2-richtlijn voert ook een meldplicht in naar alle afnemers van de dienst die door het significante incident zijn geraakt, net als bij de bestaande verplichtingen onder de AVG.

3. Toezicht en consequenties in geval van niet-naleving

NIS1 bevatte geen uitgesproken toezicht en handhavingsmechanismen. Dit staat in scherp contrast met de NIS2-richtlijn. Deze staat toezichthoudende autoriteiten toe om inspecties uit te voeren of bewijs op te vragen en kan de bestuurder (algemeen directeur) in geval van wanprestaties een tijdelijk verbod voor het uitvoeren van diens taken opleggen (mits daarvoor een gerechtelijk bevel is verkregen). De nieuwe richtlijn introduceert ook een mechanisme voor niet-naleving waarmee toezichthoudende instanties boetes tot 10 miljoen euro of 2% van de totale wereldwijde jaaromzet kunnen opleggen. Tot slot introduceert NIS2 verplichtingen op het gebied van bestuur en aansprakelijkheid van het management. Deze verplichtingen vereisen dat het management risicomaatregelen goedkeurt en toezicht houdt op de implementatie ervan[11].

4. Herziening taken en bevoegdheden van het CSIRT

Naast de bovengenoemde veranderingen zijn onder de NIS2-richtlijn ook de taken en bevoegdheden van de CSIRT's van de lidstaten aanzienlijk herzien. Naast het monitoren en analyseren van standaardtaken, is het CSIRT nu ook verantwoordelijk voor het assisteren van entiteiten wanneer zich een incident voordoet, het gecoördineerd bekendmaken van kwetsbaarheden, het verzamelen en analyseren van forensische gegevens, en het uitvoeren van risico- en incidentanalyses. Dit geeft entiteiten het recht om gebruik te maken van de ondersteuning en informatie over dreigingen van het landelijke CSIRT[12].

BEVEILIGINGSEISEN IN NIS2

- Beleid inzake risicoanalyses en beveiliging van informatiesystemen
- Incidentenbehandeling
- Bedrijfscontinuïteit
- Beveiliging van de toeleveringsketen
- Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen
- Beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen
- Basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging
- Beleid en procedures voor het gebruik van cryptografie en encryptie
- Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa
- Het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen

Bekijk voor meer informatie artikel 21 van de NIS2-richtlijn

Figuur 2: Beveiligingseisen in NIS2

De uitdagingen die komen kijken bij de implementatie van de NIS2-richtlijn ontrafeld

In het voorgaande deel zijn de belangrijkste veranderingen van de NIS2-richtlijn in vergelijking met de NIS1-richtlijn besproken. Deze veranderingen bieden organisaties mogelijkheden om hun beveiliging te versterken en hun risico's te verminderen. Hieronder gaan we in op de belangrijkste uitdagingen die organisaties bij de implementatie het hoofd moeten bieden, waarbij we ons gebaseerd hebben op onze eigen ervaringen met klanten die we hebben geholpen met het implementeren van de NIS-richtlijn.

Uitdaging 1: Het bepalen van de reikwijdte van NIS2 voor je organisatie

Bepalen of een organisatie binnen de reikwijdte van de NIS2-richtlijn valt is voor veel organisaties een uitdagende en tijdrovende taak. Het vereist experts met diepgaande kennis van het bedrijf, IT en beveiliging. Nochtans is het de meest cruciale stap om NIS2-compliant te worden. Het toepassingsbereik bepaalt tenslotte welke diensten, middelen en bedrijfsprocessen aan de NIS2-richtlijn moeten voldoen. Op basis van onze eigen ervaringen met klanten die we hebben geholpen met het bepalen van het toepassingsbereik van NIS2 hebben we hieronder de belangrijkste uitdagingen op een rij gezet.

De juiste balans vinden tussen de vereiste weerbaarheid van het bedrijf en kostenefficiëntie

De digitale weerbaarheid van bedrijven (ofwel je snel kunnen aanpassen aan verstoringen) en kostenefficiëntie (het vermogen om projecten en diensten zo voordelig mogelijk te leveren zonder dat dit ten koste gaat van de kwaliteit) spelen elkaar vaak parten. Nochtans zijn beide aspecten essentieel voor het voortbestaan van de organisatie. De juiste dynamische balans vinden is belangrijk, maar meestal weegt kostenefficiëntie zwaarder dan weerbaarheid. De NIS2-richtlijn dwingt organisaties om dit evenwicht te herzien, aangezien ze nu wettelijk verplicht zijn om hun digitale weerbaarheid te vergroten. Tijdens het bepalen van het toepassingsbereik moet er een nieuwe balans worden gevonden die overeenstemt met de NIS2-richtlijn. Maar stakeholders zoals de IT-afdeling, beveiligingsmedewerkers en het bedrijf kunnen verschillende belangen en ideeën hebben over hoe ze hiermee moeten gaan.

Interpreteren van de selectiecriteria voor de reikwijdte

Niet alle bedrijfsservices en onderliggende bedrijfsprocessen en activa voor de levering van een bedrijfsservice worden door NIS2 als belangrijk of essentieel beschouwd. De uitdaging waar veel organisaties vaak tegenaan lopen, is het gebrek aan kennis en expertise op het gebied van NIS2 om te bepalen welke bedrijfsservices en onderliggende processen en activa essentieel of belangrijk zijn onder de NIS2-richtlijn. Hierdoor vinden organisaties het moeilijk om de betekenis van NIS2 te vertalen naar vastomlijnde selectiecriteria die de organisatie kunnen helpen bij het bepalen van de vervolgstappen. En dat terwijl vastomlijnde selectiecriteria essentieel zijn om de juiste balans te vinden tussen de weerbaarheid van het bedrijf en kostenefficiëntie. Alleen zo kunnen bedrijven hun koers bepalen.

Bedrijfsmiddelen en processen

Vaak hebben organisaties beperkt inzicht in hun bedrijfsmiddelen en processen, omdat ze de documentatie van hun activabeheer en bedrijfsprocessen slechts gedeeltelijk op orde hebben. Ook komt het voor dat organisaties hun bedrijfsprocessen helemaal niet hebben vastgelegd. Dergelijke inzichten moeten er wel komen. Maar organisaties kunnen te maken hebben met de situatie dat de kennis en expertise over deze activa en processen verspreid is tussen verschillende zakelijke stakeholders en verantwoordelijken voor de informatietechnologie, operationele technologie en cybersecurity. Zelfs als de organisatie over de juiste NIS2-expertise beschikt en de selectiecriteria voor het toepassingsbereik succesvol zijn vastgesteld, wordt het bepalen van het toepassingsbereik buitengewoon lastig wanneer duidelijk inzicht in de activa, processen en precieze stakeholders ontbreekt.

Uitdaging 2: Risicobeheer in de supply chain onder NIS2

De NIS2-richtlijn vereist dat organisaties robuuste beoordelingen en beheerprocessen voor de risico's in de toeleveringsketen (Supply Chain Risk Management ofwel SCRM) implementeren om de beveiliging van hun kritieke infrastructuur te waarborgen. Dit betekent dat zowel technische als niet-technische risico's als gevolg van de verspreide en onderling verbonden aard van IT/OT-producten en -diensten in de supply chains moeten worden geïdentificeerd, beoordeeld en beheerd. Het doel is om ervoor te zorgen dat organisaties een compleet beeld hebben van de risico's van hun supply chain en passende maatregelen nemen om deze risico's te beperken. Het opzetten en implementeren van effectieve SCRM-processen kan echter een behoorlijke uitdaging zijn, met name voor organisaties die van veel leveranciers afhankelijk zijn. Op basis van onze eigen ervaringen met klanten die we hebben geholpen met het SCRM-proces voor NIS2 hebben we hieronder de belangrijkste uitdagingen op een rij gezet.

Identificeren van stakeholders en afhankelijkheden van stakeholders

Een helder beeld van de supply chain is essentieel voor een effectief beheer van de risico's in de supply chain. Een goed overzicht krijgen kan echter lastig zijn, omdat de informatie niet altijd direct voorhanden is of zich verspreid binnen de organisatie bevindt. Bovendien vereist de NIS2-richtlijn niet alleen dat de belangrijkste externe stakeholders in kaart worden gebracht, maar ook dat de afhankelijkheden van deze stakeholders vanuit het oogpunt van NIS2 worden geïdentificeerd. Daartoe moet bepaald worden of het gebruik van de externe dienst of bedrijfsmiddelen gevolgen kan hebben voor de vertrouwelijkheid, integriteit en beschikbaarheid, en zodoende de bedrijfscontinuïteit in gevaar kan brengen. Het vaststellen van criteria en het bepalen van deze gevolgen kan uitdagend zijn, aangezien

het een gestructureerde aanpak en samenwerking van alle stakeholders vereist.

Het integreren van SCRM in bestaande processen voor inkoop- en contractbeheer

Bij het integreren van risicobeheer in de supply chain moet met meerdere aspecten rekening worden gehouden. Voor organisaties die reeds beschikken over inkoop- en contractbeheerprocessen is het belangrijk om te beoordelen of cybersecurity daar al in is opgenomen. Is dit het geval, dan moet geverifieerd worden of de gehele supply chain expliciet in de contracten is gedekt. Ontbreekt cybersecurity nog in de processen, dan moeten de contractvoorwaarden worden uitgebreid of veranderd om aan de NIS2-richtlijn te voldoen. Het kan ook zijn dat organisaties de cybersecurityregels van NIS2 al in de inkoopprocessen hebben opgenomen, maar dat het schort aan implementatie ervan. Inzicht verkrijgen in de status van SCRM is dus belangrijk. Hoewel dit uitdagend is, is het essentieel voor het handhaven van het SCRM en het naleven van de NIS2-richtlijn.

De naleving monitoren en aan alle vereisten voldoen

Organisaties versturen NIS2- of SCRM-beoordelingen om het huidige niveau van beveiliging, naleving en leveranciersrisico te controleren. Zonder contractuele verplichtingen is het echter mogelijk dat niet alle leveranciers bereid zijn om mee te werken. Ze kunnen deze monitoring opdringerig of te veel gedoe vinden. Een ander ingewikkeld aspect is risicobereidheid: een organisatie moet beslissen welke risico's ze bereid zijn om te nemen wanneer toekomstige of bestaande leveranciers die essentieel zijn voor hun bedrijfsvoering, niet aan de vereisten voldoen.

Uitdaging 3: Beheer van beveiligingsincidenten en rapportageverplichtingen

De NIS2-richtlijn bevat een herziening van de bestaande rapportageverplichtingen en stelt expliciet wat er van organisaties wordt verwacht. Het voldoen aan deze vereisten resulteert in meedere implementatieuitdagingen.

Het opzetten en integreren van de NIS2-richtlijn in het proces voor het beheer van beveiligingsincidenten

Om aan de meldplicht van de NIS2-richtlijn te kunnen voldoen, moet het beheer van beveiligingsincidenten in orde zijn.

Het optuigen van een dergelijke procedure kan best uitdagend zijn. Het vereist duidelijke governance en idealiter de implementatie van gecentraliseerd beheer van logboeken met beveiligingsanalyses om alle activiteiten binnen de IT/OT-omgeving te verzamelen, naast elkaar te leggen en te analyseren. Niet alle bedrijven zullen over het budget, de expertise of zelfs de volwassenheid beschikken om dit te doen, waardoor organisaties het risico lopen om niet aan de strenge verplichtingen voor het beheer van beveiligingsincidenten en rapportages te voldoen. Daarnaast verschilt de volwassenheid per organisatie. Hierdoor bestaat er nog een grijs gebied en is het de vraag wanneer de detectiemogelijkheden volstaan om aan de door NIS2 gestelde rapportageverplichtingen te voldoen. Een andere complicerende factor kan zijn dat organisaties het beheer van hun beveiligingsincidenten hebben uitbesteed. Dit betekent dat de NIS2-rapportageverplichtingen niet in de service level agreements (SLA's) kunnen worden opgenomen, omdat dat nieuwe contractonderhandelingen zou vereisen.

Het definiëren van een 'significant incident' en 'verdachte activiteit'

Een significant incident of een grote cyberdreiging die tot een significant incident kan leiden moet gemeld worden aan het landelijke CSIRT. Maar interpreteren of een verdachte activiteit een incident is of mogelijk tot een significant incident kan leiden, en dus gemeld moet worden, blijkt nog wel eens lastig en is voor elke organisatie anders. Het kan bovendien meer tijd in beslag nemen dan het tijdsbestek waarin de melding gedaan moet zijn. Zonder duidelijke afstemming binnen organisaties over wat wordt beschouwd als een significant incident en welke strenge tijdslijnen moeten worden aangehouden, riskeren organisaties uit angst voor niet-naleving een aanzienlijke overbelasting van hun beheerteams voor beveiligingsincidenten.

Over de auteurs:

Florianne Kortmann

Florianne is een Senior cybersecurityconsultant gespecialiseerd in IT-strategie, governance, risicobeheer (in de supply chain) en compliance. Ze heeft veel ervaring met het uitvoeren van advies en implementatietrajecten met betrekking tot NIS2 en ISO27001 en houdt zich daarnaast bezig met business development op het gebied van NIS2. Florianne pakt uitdagingen met beide handen aan en ziet deze als een kans om security naar een hoger niveau te tillen.

Mail: florianne.kortmann@capgemini.com

LinkedIn: https://www.linkedin.com/in/florianne-kortmann/

Sasha Brouwer

Sasha is een cybersecurityconsultant met een focus op strategie, risk en compliance. Zij heeft ervaring met NIS2 business development, risicobeheer van derden en ISO27001-implementaties bij zowel de private als publieke sector.

Mail: sasha.brouwer@capgemini.com

LinkedIn: https://www.linkedin.com/in/sashabrouwer/

Bronnen:

1. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
2. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 2 NIS2-richtlijn)
3. https://doi.org/10.1007/978-981-19-6414-5_18
4. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 26 NIS2-richtlijn)
5. https://eur-lex.europa.eu/eli/dir/2016/1148/oj (Artikel 14 NIS1-richtlijn)
6. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 21 NIS2-richtlijn)
7. https://securityboulevard.com/2023/05/how-software-supply-chain-vulnerabilities-lead-to-attacks
8. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 23 NIS2-richtlijn)
9. https://www.stibbe.com/publications-and-insights/the-revised-network-and-information-security-directive-enhancing-eu
10. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 32 NIS2-richtlijn)
11. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 34 NIS2-richtlijn)
12. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 20 NIS2-richtlijn)
13. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 10,11,12 NIS2-richtlijn)
14. https://eur-lex.europa.eu/eli/dir/2022/2555 (Artikel 23 NIS2-richtlijn)

VEILIGHEID IN OPKOMENDE (OF UITBREIDENDE) TECHNOLOGIEGEBIEDEN

02

Trends in Cybersecurity 2023

GEGEVENS IN DE METAVERSE: WIE IS DE EIGENAAR?

Hoe beschermen we persoonsgegevens in de metaverse waarbij gebruikers zeggenschap en controle behouden over hun gegevens en hun identiteit?

Highlights

- Door de manier waarop interacties plaatsvinden in de metaverse zullen er nieuwe soorten gevoelige persoonsgegevens verwerkt worden die onder privacyregelgeving kunnen vallen.
- Bedrijven kunnen hierop inspelen door proactief na te denken over hun privacy beleid voor het Web 3.0.
- De metaverse zal zorgen voor levensechte ervaringen in de digitale wereld, wat zal resulteren in een ongekende stroom van gegevens.
- Pseudonimisering van gegevens wordt de prioriteit in Web 3.0.
- In Web 3.0 zal jouw identiteit niet langer in handen zijn van één grote speler. In plaats daarvan heeft de gebruiker de controle met *decentralized identities* die worden beschermd dankzij veilige en betrouwbare distributed ledgers.
- *Decentralized identities* vereenvoudigen het proces van identiteitsvalidatie bij interacties in de metaverse en zorgen zo voor een betere gebruikerservaring.

"Privacy is not an option, and it should not be the price we accept for just getting on the internet". Dit benadrukte Gary Kovacs al in 2012 toen hij de privacyoplossing Collusion voor Firefox introduceerde[1]. Gezien het feit dat tegenwoordig miljarden internetgebruikers meer dan ooit hun persoonlijke informatie delen, blijven Gary's woorden vandaag de dag nog altijd relevant.

De ontwikkeling van Web 3.0 heeft een nieuw bewustzijn met zich meegebracht over de handel in persoonsgegevens. In de metaverse, waar de grenzen tussen online en offline vervagen en waar onze digitale identiteit even belangrijk wordt als onze fysieke identiteit, willen mensen steeds vaker de controle houden over hun gegevens. Het biedt een wereld vol mogelijkheden, maar gaat gepaard met de uitdaging om persoonsgegevens des te meer te beschermen. In dit artikel worden de kwesties rondom data eigenaarschap in de metaverse belicht en wordt een oplossing gepresenteerd waarmee gebruikers meer zeggenschap over hun gegevens en identiteit krijgen.

De uitdagingen van de nieuwe digitale wereld

In de afgelopen 32 jaar heeft het internet een evolutie meegemaakt: van een eenvoudige leeservaring (Web 1.0) naar een interactief medium waarin we zowel lezen als schrijven (Web 2.0). Nu staan we op de drempel van het zogenaamde semantische web of Web 3.0, wat decentralisatie van informatie mogelijk maakt en waarin individueel eigenaarschap van je eigen informatie centraal staat. De nieuwe generatie internetgebruikers verkent het enorme potentieel van deze nieuwe onlinewereld en omarmt volop de nieuwe mogelijkheden zoals blockchain en de metaverse. Deze nieuwe mogelijkheden hebben de potentie om ons gebruik van het internet te veranderen in een compleet nieuwe ervaring.

De metaverse opent nieuwe deuren voor online interacties op een manier die voorheen onmogelijk was en biedt daarmee de gelegenheid voor innovatieve technologieën om deze ervaringen naar een hoger niveau te tillen. Dit zou kunnen betekenen dat alle zintuigen van de gebruiker worden geïntegreerd in de Web 3.0 ervaring, wat nieuwe soorten (gevoelige) gegevens genereert die op allerlei manieren worden verwerkt. De nieuwe onlinewereld belooft gebruikers controle over hun eigen gegevens, maar de groeiende hoeveelheid gevoelige informatie die verwerkt zal worden, leidt onvermijdelijk tot bezorgdheid over privacy.

Om dit onderwerp aan te pakken, is het van belang om te beseffen dat de regels rondom privacy en databescherming oorspronkelijk zijn opgesteld voor het gebruik van fysieke archiefkasten en later pas zijn aangepast voor internetgebruik. Om de web 3.0-omgeving effectief te kunnen reguleren en in te spelen op de nieuwe uitdagingen die deze omgeving met zich meebrengt, moeten we ons bewust zijn van deze veranderingen. Met dit bewust zijn kunnen privacy- en gegevens- beschermende maatregelen worden meegenomen vanaf het begin van het procesontwerp (ook wel bekend als 'privacy by design').

Maar aangezien regelgeving vaak achterloopt op technologische ontwikkelingen, is het belangrijk om te onderzoeken hoe organisaties proactief hun beleid kunnen aanpassen aan de metaverse in de Web 3.0-omgeving. We moeten ervan uitgaan dat dit een levensechte ervaring in de digitale wereld zal zijn. Bovendien zullen er enorme hoeveelheden gegevens continu in omloop zijn. Om de daaruit voortvloeiende uitdagingen aan te gaan is het van essentieel belang eerst de huidige stand van zaken met betrekking tot privacy te evalueren en te bepalen hoe data eigenaarschap in de metaverse het beste kan worden beschermd in de toekomst.

Privacy- en veiligheidsoverwegingen in de metaverse

In de metaverse verbinden mensen zich met hun eigen digitale avatar. Deze avatars kunnen unieke identifiers met gevoelige gegevens bevatten die herleidbaar zijn tot één persoon. Het ligt dan ook voor de hand dat de bestaande privacywetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), van toepassing zal zijn op gegevens in de metaverse. Door het grensoverschrijdende en wereldwijde karakter van de metaverse kan echter niet worden gesteund op slechts één specifieke regelgeving aangezien meerdere privacy- en gegevensbeschermingswetten van toepassing kunnen zijn op dezelfde gegevens en op hetzelfde individu. Vanwege de unieke kenmerken van de metaverse, zullen huidige procedures voor privacybeleid moeten worden herzien. Een voorbeeld kan dit illustreren. Stel dat een persoon in de metaverse interactie heeft met een andere gebruiker door met deze te praten (spraakpatronen) of fysieke bewegingen te maken (via zijn of haar avatar). Deze gegevens kunnen dan worden verzameld en geanalyseerd door derden voor commerciële doeleinden, zoals het aanpassen van reclame of het verbeteren van productontwikkeling op basis van de gedragsgegevens van gebruikers.

Daarnaast worden in de metaverse nieuwe categorieën van zeer gevoelige persoonsgegevens verwerkt, zoals biometrische gegevens (denk aan gezichtsherkenning en hoe je eruitziet) en gegevens over je fysieke bewegingen (zoals eye tracking) en interacties met andere gebruikers (zoals hoe je praat). Dit voorspelt al dat databeveiliging in de metaverse een grote uitdaging kan worden. Met name wanneer persoonsgegevens van de ene naar de andere metaverse worden doorgegeven (interoperabiliteit), of wanneer derden binnen de Web 3.0 omgeving deze informatie voor zakelijke doeleinden mogen gebruiken.

Duidelijk is dat er op dit moment geen specifieke wetgeving bestaat voor dit soort scenario's in de metaverse. Juist daarom kunnen ondernemingen zich nu onderscheiden in de markt door zelf initiatief te nemen om dit soort privacygevoelige onderwerpen in de ontwerpfase te integreren ('privacy by design'). Dit wekt vertrouwen en versterkt hun reputatie bij de gebruikers, zeker als dit gepaard gaat met het bieden van meer eigenaarschap over de gegevens aan hun gebruikers zelf. Organisaties kunnen bijvoorbeeld hun interne privacy beleid herzien en maatregelen treffen om rekening te houden met toekomstige ontwikkelingen als zij van plan zijn metaverse platforms te gebruiken voor hun producten en dienstverlening.

Wat zijn bestaande oplossingen?

Nu we aan de vooravond staan van de implementatie van Web 3.0 en daarmee de metaverse, is het belangrijk om na te gaan hoe bestaande juridische en technische oplossingen kunnen worden aangepast zodat gebruikers eigenaar blijven van hun gegevens. Zo houden ze controle over hun data en beslissen ze wat ermee gebeurt als er interacties plaatsvinden in de metaverse.

Als bij voorbaat blijkt dat gegevens door verschillende bedrijven voor verschillende doeleinden zullen worden gebruikt, zoals interne analyses voor kwaliteitsborging, dan zijn er bestaande oplossingen om zowel bedrijven als het individu te helpen en te beschermen. Ten eerste pseudonimisering, waarmee gebruikers privacy over hun informatie kunnen behouden en waarmee bedrijven hun verwerkingen uit kunnen voeren zonder alle gegevens van de gebruiker te moeten kennen. En ten tweede een decentralized identity die fungeert als een persoonlijke dataset voor eindgebruikers.

Pseudonimisering van data betekent dat persoonlijke gegevens worden vervangen door andere gegevens, zodat deze niet meer direct herleidbaar zijn tot een individu. Dit wordt gedaan om de privacy van mensen te beschermen. Hierbij kan gebruik worden gemaakt van 'placeholders' voor bepaalde waarden die gebruikers in staat stelt om informatie te verifiëren. Zo kan iemand bijvoorbeeld bevestigen dat hij of zij meerderjarig is of een universitair diploma heeft, zonder dat de geboortedatum of naam van de universiteit wordt verstrekt. Dit principe kan niet alleen worden toegepast op simpele use cases zoals deze, maar ook op grotere en complexere datasets met zeer gevoelige informatie zoals neuro-imaging, biometrische informatie en juridische informatie over gebruikers. Dit kan de basis vormen voor op rollen gebaseerde toegangsmodellen tussen verschillende metaverses in de toekomst. Denk bijvoorbeeld aan toegang tot specifieke overheidsmetaverses op basis van paspoort- of identiteitsgegevens.

Pseudonimisering is slechts één essentieel onderdeel van het matchen van de identiteit van een gebruiker binnen een Web 3.0 omgeving: waar zullen deze persoonlijke datasets worden opgeslagen of gearchiveerd? Decentralized identities zijn niet slechts een 'trend'. Het zou de komende jaren zelfs de dominante werkwijze kunnen worden tussen de metaverses.

Decentralized identities als bouwsteen in de metaverse

Het idee van decentralized identities dateert nog uit 1991. In die tijd kwam het internet in een stroomversnelling en waren er al discussies over het gebruik van één enkele identificatiecode om op het web te surfen. Carl Ellison begon in zijn publicatie Establishing Identity without Certification Authority (1996) al over het concept van distributed identities. Daarin analyseerde hij hoe identiteiten werden gecreëerd en stelde hij ideeën voor om de authenticiteit van die identiteiten te behouden zonder de noodzaak van vertrouwde certificaten. Het idee kwam echter pas in de 21e eeuw op gang toen het concept van decentralisatie populairder werd met de komst van blockchain en de opkomst van de cryptomarkten.

Decentralized identities die gepseudonimiseerde persoonsgegevens bevatten, verbeteren de beveiliging van gegevensopslag en voorkomen datalekken of informatieverlies doordat identiteitsinformatie niet in losse databases wordt opgeslagen of wordt bewaard door één enkele vertrouwde uitgever. In plaats daarvan worden gegevens opgeslagen in een zogenaamde 'distributed ledger', beter bekend als 'blockchain'. Deze blockchain is toegankelijk voor zowel de 'uitgever' (issuer) (die ervoor zorgt dat de gegevens correct zijn) en de 'verificateur' (die de authenticiteit van de gegevens checkt). Dit maakt het ook mogelijk om meer dan één uitgever voor dezelfde identiteit te hebben, waardoor de gebruiker identiteitsvalidaties kan verkrijgen van verschillende entiteiten zoals overheden, emailproviders of anderen binnen dezelfde identiteitsset. Dit vermindert ook het aantal interacties tussen elke verificateur en de vele uitgevers die betrokken kunnen zijn bij een identiteitsvalidatie die over verschillende achterliggende databases loopt.

Door identiteiten in de metaverse te beschouwen als autonoom kan niet alleen de omgeving voor gebruikers

veiliger worden gemaakt, maar resulteert het ook in een meer naadloze gebruikerservaring in het metaverse landschap. Bovendien hebben gebruikers meer controle over hun gegevens. Dit omdat de gebruiker zich ervan bewust is dat zijn of haar gegevens niet zullen worden opgeslagen in de databases van andere bedrijven die ook met gebruikers communiceren in dezelfde metaverse.

De metaverse belooft een spannende en grenzeloze digitale toekomst, maar het citaat van Gary Kovacs blijft nog altijd, of zelfs des te meer, relevant. Deze droom kan alleen werkelijkheid worden als we de privacy en gegevensbescherming van gebruikers kunnen waarborgen, zelfs zonder specifiek toepasbare privacywetgeving. Gelukkig zijn er oplossingen binnen handbereik, zoals pseudonimisering en decentralized identities, die ons helpen de gebruikers de controle over hun eigen gegevens te geven en eigenaarschap voorop te stellen. Door deze oplossingen op de juiste manier te implementeren, kunnen organisaties zich onderscheiden op de markt en aantonen dat ze staan voor authenticiteit en privacy.

Over de auteurs:

Alfredo Acuña Salswach

Alfredo combineert zijn technische achtergrond met een doordachte aanpak in zijn werk. Hij is een natuurlijke teamspeler en zijn ervaring op het gebied van Identity and Access Management heeft hem tot referentiepunt gemaakt binnen zijn team. Met een master in Chemische Technologie zijn de complexe en dynamische studievelden van cybersecurity een passie geworden, Web 3.0 en de Metaverse staan in zijn top 3.

Mail: alfredo.acuna-salswach@capgemini.com

LinkedIn: https://www.linkedin.com/in/alfredo-acuna-salswach/

Selma Mujcic

Selma is een ervaren privacyadviseur die haar kennis van innovatieve technologieën combineert met een strategische benadering van privacy en cybersecurity om bedrijven te helpen bij het realiseren van duurzame en veilige groei. Selma's expertise en inzicht maken haar uniek in haar vakgebied en stellen haar in staat om bedrijven te begeleiden in deze voortdurend veranderende digitale wereld.

Mail: selma.mujcic@capgemini.com

LinkedIn: https://www.linkedin.com/in/selmamujcic/

Bronnen:

1. https://www.wired.com/2012/02/ted-mozilla-collusion/

DE WAARDE VAN TESTBEDS BIJ DE OVERGANG NAAR QUANTUM VEILIGE CRYPTOGRAFIE

Hoe kunnen testbeds en innovatieve oplossingen helpen bij het bestrijden van veiligheidsdreigingen en het overwinnen van uitdagingen?

Highlights

- Quantumcomputers bedreigen bestaande encryptiesystemen, waarvoor testbeds en innovatieve oplossingen nodig zijn.
- Post-Quantum Cryptografie (PQC) en Quantum Key Distribution (QKD) worden voorgesteld als reactie op quantumdreiging.
- Overstappen naar quantum-veilige cryptografie is nieuw en vereist voorbereiding en het aanpakken van complexiteit en gebrek aan ervaring.
- Testbeds helpen bij experimenteren met algoritmen en protocollen voor efficiënte implementatie.
- Testbeds helpen bij het verbeteren van het systeemontwerp, de implementatie en vullen ervaringslacunes aan. Ze zijn cruciaal voor succesvolle quantumveilige migratie in OT-omgevingen.

We naderen het tijdperk van quantum computers. Deze computers kunnen problemen oplossen die voor klassieke computers vrijwel onmogelijk zijn. Een onbedoeld gevolg van deze rekenkracht, is dat de veiligheid van onze huidige encryptiesystemen in gevaar komt. Quantum computers kunnen traditionele asymmetrische cryptografische algoritmen breken die wij nu gebruiken om onze gevoelige informatie te beschermen. Huidige cryptografische algoritmen bieden veiligheid op basis van de complexiteit van wiskundige problemen die praktisch onuitvoerbaar zijn voor klassieke computers, zoals het factoriseren van priemfactoren. Volgens berekeningen zou het bijvoorbeeld een standaard computer van nu bijna 300 biljoen jaar kosten om een RSA-2048 bit encryptiesleutel bruteforce te kraken. Maar een quantum computer die groot genoeg is en genoeg capaciteit heeft, zou de factorisering in enkele uren[1] kunnen uitvoeren. Dit vormt een bedreiging voor de veiligheid van onze systemen. Hoe kunnen testbeds en innovatieve oplossingen helpen deze dreiging aan te pakken en de uitdagingen overwinnen?

Twee voorgestelde oplossingen voor deze quantum dreiging zijn:

1. Post-Quantum Cryptografie (PQC). PQC's zijn cryptografische algoritmen die tot het klassieke domein behoren en als veilig worden beschouwd tegen aanvallen van zowel klassieke als quantum computers. Verwacht wordt dat PQC's kunnen samenwerken met bestaande klassieke systemen.
2. Quantum Key Distribution (QKD). QKD is daarentegen gebaseerd op de principes van quantum mechanica en wordt, zodra volwassen, beschouwd als de veiligste encryptiemethode die in het quantum domein werkt.

Gezien de bijkomende hardware-vereisten, het gebrek aan industriële normen en het nog beperkte volwassenheidsniveau van de QKD-technologie, wordt door enkele toonaangevende nationale veiligheidsinstellingen in Frankrijk[2], Duitsland[3], het Verenigd Koninkrijk[4] en de Verenigde Staten[5], PQC aanbevolen als oplossing voor quantum dreiging. Gezien deze aanbevelingen focussen wij ons in de volgende paragrafen op PQC.

Uitdagingen bij de invoering van quantumveilige cryptografie

Om beschermd te blijven tegen bedreigingen van quantum computers moeten alle organisaties hun systemen upgraden, van bestaande quantum kwetsbare cryptografie naar PQC. Het upgradeproces om de huidige cryptografie te vervangen door quantum-veilige cryptografie wordt beschouwd als een enorme, kostbare en complexe opdracht die vele jaren kan duren, afhankelijk van de omvang van een organisatie. Een transitieprogramma met zo'n grote impact en dat bijna elk cruciaal onderdeel van een organisatie raakt, heeft een goede voorbereiding nodig. Een belangrijk onderdeel van de voorbereiding is het verkennen van en experimenteren met nieuwe cryptografie-algoritmen, om te zorgen voor een efficiënte en kosteneffectieve uitvoering van een quantumveilige transitie. Er zijn enkele belangrijke uitdagingen die moeten worden aangepakt voordat de quantumveilige reis kan starten.

1. **Geen drop-in vervanging** PQC-algoritmen verschillen van traditionele versleutelingsalgoritmen. Deze algoritmen zijn gebaseerd op verschillende wiskundige benaderingen die meer rekenkracht vereisen. Ze hebben een verschillende sleutellengte voor openbare en particuliere sleutels, wat leidt tot een nieuw ontwerp van coderingssytemen. Bestaande cryptografie kan niet zomaar worden vervangen door nieuwe quantum veilige cryptografie.
2. **Verscheidene soorten PQC-algoritmen met verschillende eigenschappen**
   Er worden meerdere PQC-algoritmen geselecteerd en gestandaardiseerd. Het is van essentieel belang de juiste combinatie van algoritmen en protocollen te kiezen die het meest geschikt zijn voor specifieke

toepassingen. Deze combinatie moet voldoen aan de bijbehorende beveiligingsvereisten en zorgen voor optimale prestaties.

Het National Institute of Standards and Technology (NIST) van het U.S. Department of Commerce standaardiseert quantumveilige algoritmen voor sleutelcodering en het gebruik van digitale handtekeningen. In elke categorie wordt van het NIST verwacht dat het meerdere algoritmen selecteert en standaardiseert. Dit is een lang selectieproces (geweest) met meerdere rondes. In juli 2022 heeft NIST de selectie aangekondigd van de eerste groep PQC-algoritmen. Deze groep omvat één sleutel-inkapselingsalgoritme; het CRYSTALS-Kyber[6] algoritme voor algemene encryptie en drie algoritmen CRYSTALS-Dilithium[7], FALCON[8] en SPHINCS+[9] voor digitale ondertekening. Daarnaast worden er in ronde vier van het NIST-selectieproces nog vier algoritmen voor sleutelvaststellingsmechanismen geëvalueerd. Verwacht wordt dat deze geselecteerde algoritmen in het jaar 2024 normen zullen worden.

3. **Gebrek aan ervaring en deskundigheid**
   PQC-algoritmen zijn relatief nieuw en zijn nog niet op grote schaal gebruikt in real-world toepassingen. Dit betekent dat er, in tegenstelling tot de traditionele algoritmen, beperkte kennis, ervaring en deskundigheid is in het implementeren en gebruiken van deze algoritmen. Dit gebrek aan ervaring kan het moeilijk maken passende ontwerpbeslissingen te nemen die voldoen aan de beveiligings- en prestatie-eisen voor de algoritmen en toepassingen.
4. **Toegenomen complexiteit door hybride benaderingen**
   Aangezien de PQC-algoritmen nieuw en niet bewezen zijn, maken deskundigen zich zorgen over de duurzaamheid van hun veiligheid[10]. Daarom bevelen deskundigen hybride benaderingen aan (een combinatie van klassieke en PQC-algoritmen). Deze hybride benadering draagt verder bij aan de complexiteit van implementaties van protocollen en applicaties.

Quantum safe testbeds - een mogelijke oplossing

Gezien de beschreven uitdagingen, is het voor elke organisatie noodzakelijk om een goede kennis op te bouwen van de PQC-algoritmen en bijbehorende protocollen plus de resourcevereisten waaronder reken-, geheugen-, en bandbreedtevereisten. Maar er is ook inzicht nodig in algehele impact op de functionaliteit en prestaties van verschillende applicaties voordat de quantumveilige migratieprojecten worden gestart. Zonder dit inzicht kan de migratie op ernstige problemen stuiten, zoals applicaties die geherfactoriseerd moeten worden, suboptimale prestaties, functionele problemen etc. Deze problemen worden aanzienlijk versterkt in het OT-landschap door embedded systems met beperkte middelen en real-time prestatieverwachtingen.

Een mogelijke oplossing voor het gebrek aan inzicht is het evalueren van de PQC-algoritmen en beveiligingsprotocollen in testbeds. Dit zijn speciale omgevingen die zijn ontworpen voor het testen en evalueren van quantumveilige cryptografische algoritmen en protocollen op functionaliteit en prestaties in een specifieke toepassingscontext. De testbeds kunnen bestaan uit alleen software, of een combinatie van software en hardware met de benodigde invoer- en uitvoerinterfaces, evenals andere componenten die nodig zijn om real-life omstandigheden te simuleren voor de evaluatie van quantumveilige cryptografische systemen en toepassingen.

Testbeds stellen onderzoekers in staat te experimenteren met PQC-algoritmen, afzonderlijk of in hybride modus (combinatie van quantumveilige en traditionele algoritmen), voor specifieke gebruikssituaties en toepassingsscenario's in gesimuleerde omgevingen die real-life omstandigheden weergeven. Dit geeft inzicht in sterke en zwakke punten en de geschiktheid van quantumveilige algoritmen en bijbehorende protocollen. Dit is belangrijk omdat sommige combinaties van cryptografie-algoritmen beter geschikt zijn voor bepaalde toepassingen en bijbehorende omgevingen dan andere. De testopstellingen ondersteunen in een laboratoriumomgeving bij het uitvoeren van evaluatie-experimenten voor de functionaliteit, prestatie-eisen en beveiliging van elke applicatie en de bijbehorende systeemscenario's die relevant zijn voor een organisatie.

Hieronder volgen de aanbevolen stappen om evaluaties uit te voeren met quantum testbeds:

- De toepassingen identificeren die bescherming vereisen tegen quantum computers en de toepassingsscenario's bepalen die getest moeten worden.
- De beveiligingseisen vaststellen voor elke toepassing die bescherming biedt tegen klassieke en quantum bedreigingen.
- De details van de resources van bestaande systemen, zoals rekenkracht, geheugen, netwerkbandbreedte etc, vastleggen en analyseren om het testbed te configureren voor geselecteerde toepassingen en bijbehorende use-casescenario's.
- Bepalen en configureren van beperkingen en netwerkvoorwaarden, waaronder latentie, transmissiefouten, omvang van de transmissie-eenheden etc.
- Implementaties van quantumveilige algoritmen (PQC) verzamelen, protocollen evalueren en overbrengen naar het testbed-platform.
- Applicatie POC's implementeren of bestaande applicatiesoftware gebruiken, algoritmen en protocollen, zoals vereist voor applicatiescenario's, configureren.
- Test scenario's voorbereiden om implementaties uit te voeren en te verifiëren, inclusief beoordeling van eventuele beperkingen of restricties door middel van verschillende configuratie-algoritmen en

protocollen die nodig zijn voor de applicaties. Het is beter om bestaande testplannen en testgevallen van applicaties te hergebruiken. Deze evaluatie moet worden uitgevoerd voor zowel quantumveilige algoritmen afzonderlijk, als hun hybride modi.

- De resultaten vastleggen en vergelijken met de prestaties van de bestaande toepassingen. Deze informatie gebruiken om een potentiële roadmap en planningsoefeningen voor te bereiden.

Drie voordelen van het gebruik van testbeds

Hoewel er geen drop-in vervanging bestaat voor de nieuwe post-quantum cryptografie-algoritmen, kunnen testbeds helpen bij een beter systeemontwerp en betere implementaties (software of hardware). Dankzij een beter begrip van de nieuwe algoritmen voor een efficiënte integratie in bestaande systemen. Met behulp van testbeds, zouden we kunnen experimenteren met meerdere post-quantum algoritmen die verschillende beveiligingsniveaus en sleutellengtes hebben, om vervolgens de meest efficiënte configuraties voor een bepaalde toepassing te selecteren. Testbeds verminderen misschien niet direct de complexiteit bij de invoering van hybride benaderingen, maar ze kunnen helpen bij een betere planning en een beter beheer van de migratietrajecten.

Bronnen:

1. https://quantum-journal.org/papers/q-2021-04-15-433/
2. https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/
3. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4#:~:text=QKD%20promises%20theoretical%20security%20based,post-quantum%20cryp-%20tography.
4. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
5. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
6. https://pq-crystals.org/kyber/index.shtml
7. https://pq-crystals.org/dilithium/index.shtml
8. https://falcon-sign.info/
9. https://sphincs.org/
10. https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

Tot slot helpen testbeds, door middel van experimenten, om inzicht te ontwikkelen in beveiligingsniveaus en prestaties van post-quantum algoritmen. Hiermee wordt broodnodige ervaring en deskundigheid opgebouwd.

Gebruik van de testbed inzichten in OT-omgevingen

Voor de migratie van OT-landschappen met IoT en andere embedded systemen kunnen de prestaties en de vereiste resources gebenchmarkd worden met traditionele en post-quantum algoritmen. Op basis van deze benchmarks kunnen we betere beslissingen nemen over het uitvoeren van alleen software-upgrades of hardware-upgrades of het vervangen van hardware met hogere specificaties. Alle quantumveilige migratieactiviteiten zonder een dergelijke benchmarking van de resources in OT-systemen, kunnen leiden tot ernstige problemen zoals verminderde prestaties, verhoogde noodzaak voor refactoring en soms volledig verlies van functionaliteit. Dit leidt vervolgens tot vertragingen, kostenoverschrijdingen en verlies van business.

Conclusie

Organisaties die aan hun reis naar quantumveiligheid beginnen, dienen relevante quantumveilige algoritmen en protocollen die geschikt zijn voor specifieke toepassingsscenario's te evalueren en af te wegen in een gecontroleerde omgeving. Testbeds bieden dé mogelijkheid om zo'n evaluatie uit te voeren in de quantum-veilige migratie. Op basis van de resultaten van de evaluatie kunnen de algoritmen en protocollen met relevante configuraties worden geselecteerd en gedocumenteerd voor real-life implementaties. Dit helpt organisaties om hun quantum-veilige migratiereis met vertrouwen te doorlopen.

Over de auteurs:

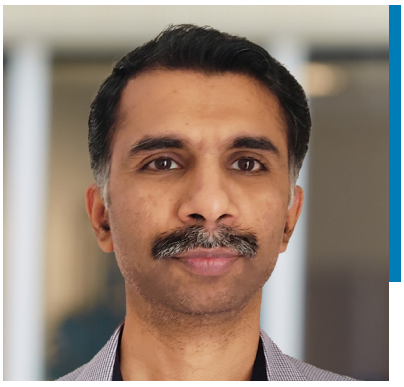
Julian van Velzen

Julian leidt Capgemini's Quantum Lab, een wereldwijd netwerk van experts, partners en faciliteiten voor quantumtechnologie in Sensing, Communication en Computing. Hij onderzoekt en bouwt met klanten aan oplossingen voor complexe zakelijke en maatschappelijke vraagstukken met quantumvoordeel. Julian is een fysicus met een achtergrond in gecondenseerde materie, studeerde aan de Universiteit van Amsterdam en vertegenwoordigt Nederland in het European Quantum Consortium (QuIC). Hij is lid van de CTIO-gemeenschap van Capgemini, het Forbes Technology Council en mede-oprichter van Quantum Gateway Foundation.

Mail: julian.van.velzen@capgemini.com

LinkedIn: https://www.linkedin.com/in/julian-van-velzen/

Gireesh Kumar Neelakantaiah



Gireesh Kumar is verantwoordelijk voor de strategie en marktintroductie van het Quantum Lab en oplossingen voor Quantum Veilige Cryptografie. Hij is een ervaren professional in productmanagement, strategische planning, innovatie van bedrijfs- en commerciële modellene, evenals het beheer van ecosysteempartners en IP-licenties. Daarnaast liggen zijn interesses op het gebied van quantum computing, data science, AI/ML/deep learning, digitale productie, industrial IoT en cloud computing.

Mail: gireeshkumar.n@capgemini.com

LinkedIn: https://www.linkedin.com/in/gireesh-kumar-n-5b5a5b1/

PRIVACY EN ETHIEK IN DE AI-REVOLUTIE: BOUW EEN STERKE ORGANISATIE

Hoe kunnen bedrijven bewust worden van AI-privacy en ethiek?

Highlights

- AI leert van data en vervult taken die menselijke intelligentie vereisen.
- Er bestaat een risico op inbreuk op het auteursrecht wanneer AI auteursrechtelijk beschermd materiaal kopieert dat herkenbaar is in de output.
- Gebruikers en ontwikkelaars van AI kunnen te maken krijgen met verschillende aansprakelijkheden.
- Onethische resultaten kunnen leiden tot wettelijke aansprakelijkheid of negatieve gevolgen voor relaties met klanten of belanghebbenden.
- Bedrijven kunnen zich onderscheiden in de markt door nu stappen te ondernemen.
- De toekomst van privacy in AI voor bedrijven zal worden beïnvloed door nieuwe technologieën zoals The Internet of Things (IoT).

Wat is (generative) AI?

AI staat voor artificiële (of kunstmatige) intelligentie, waarbij computergestuurde machines en apparaten zelfstandig problemen oplossen zonder tussenkomst van een mens. Generative AI is een onderdeel van kunstmatige intelligentie dat machine learning-modellen gebruikt om geheel nieuwe output te creëren op basis van een trainingsset. Met andere woorden, generative AI stelt een algoritme in staat om dingen te creëren zoals een mens zou doen, in tegenstelling tot de standaard analytische aard van AI-systemen.[1]

Het creëren van een AI-systeem omvat verschillende stappen, waaronder het verzamelen van gegevens, het voorbereiden van de gegevens voor gebruik, het trainen van het AI-model en de implementatie hiervan. Over het algemeen gaat AI over het creëren van machines die leren van datasets die aan hen worden aangeboden en taken kunnen uitvoeren die typisch menselijke intelligentie vereisen.

Generative AI wordt tegenwoordig op verschillende manieren gebruikt, waaronder de nu razend populaire chatbots. Een voorbeeld van een chatbot die gebruik maakt van generative AI is ChatGPT van OpenAI. ChatGPT is een chatbot die een groot taalmodel gebruikt om mensachtige antwoorden te genereren op basis van de input van de gebruiker.[2] Bedrijven kunnen ChatGPT gebruiken om klantenservice te automatiseren, virtuele assistenten te creëren en meer.[3] Een ander voorbeeld van generative AI is CarMax Inc, dat een andere versie van de technologie van OpenAI heeft gebruikt om duizenden klantbeoordelingen samen te vatten en klanten te helpen beslissen welke gebruikte auto zij willen kopen.[4] Generative AI kan bijvoorbeeld ook aantekeningen maken tijdens een virtuele vergadering.[5]

Generative AI is dus een handige tool die op veel verschillende manieren door bedrijven ingezet kan worden. Dit gebruik kan echter zowel intern als extern grote risico's voor bedrijven met zich meebrengen. Intern bijvoorbeeld, als werknemers van een bedrijf generative AI-systemen gebruiken voor hun werk en daarbij gevoelige informatie gebruiken. Het bedrijf riskeert zo de controle over deze data te verliezen. Het is namelijk nog onduidelijk hoe generative AI-systemen deze data precies in hun modellen gebruiken. Denk hierbij aan het Samsung lek, waarbij werknemers van Samsung een data lek van bedrijfsgeheimen veroorzaakten door het gebruik van ChatGPT in hun werk.[6] Extern kunnen kwaadwillenden bijvoorbeeld AI gebruiken om schadelijke of misleidende content te creëren die reputatieschade kan opleveren voor het bedrijf. Zo beweerde ChatGPT ten onrechte dat een Australische burgemeester zonder eerder strafblad in de gevangenis zat voor omkoping.[7]

Juridische en ethische overwegingen van generative AI

Het gebruik van AI roept verschillende juridische en ethische overwegingen op. De toepasselijke wetgeving voor AI hangt af van het type, het beoogde gebruik van het AI-systeem en de jurisdictie van de betrokken partijen. De Europese Unie loopt hierin voorop met de AI-Act, die naar verwachting eind 2023 in werking zal treden. Daarnaast zijn er onderling sterk verschillende AI-specifieke regelgevingen en gerelateerde rechtsgebieden, zoals intellectueel eigendom en gegevensbescherming/privacy.

Ten eerste speelt het intellectuele eigendomsrecht een belangrijke rol in AI-ontwikkeling, waarbij verschillende aspecten moeten worden overwogen. Bij het trainen van AI-modellen moeten ontwikkelaars bijvoorbeeld zorgvuldig de vereiste toestemmingen controleren en indien nodig een licentie verkrijgen voor auteursrechtelijk beschermd materiaal, of dit materiaal volledig uitsluiten. Ook bestaat er een risico op inbreuk op het auteursrecht wanneer AI auteursrechtelijk beschermd materiaal kopieert dat herkenbaar is in de output. Bedrijven moeten voorzichtig zijn met het opnemen van open source software (OSS) als onderdeel van hun commerciële softwareproducten, omdat sommige OSS-licenties vereisen dat toestemming nodig is van- of credits worden gegeven aan de oorspronkelijke auteur. Andere OSS-licenties eisen dat alle afgeleide werken ook open source of voor non-profit-gebruik zijn.

Ten tweede is aansprakelijkheid een belangrijk aandachtspunt bij AI. Generative AI kan in sommige gevallen schade toebrengen aan derden, zoals door onnauwkeurige diagnoses in de gezondheidszorg of onjuist beleggingsadvies in de financiële dienstverlening, wat vragen oproept over wie verantwoordelijk is als het misgaat: de makers van de AI of de bedrijven die de output gebruiken. Gebruikers en ontwikkelaars van AI kunnen te maken krijgen met verschillende aansprakelijkheid, waaronder vorderingen wegens

nalatigheid en productaansprakelijkheid. Organisaties die gebruik maken van AI moeten zich bewust zijn van de aansprakelijkheden die kunnen voortvloeien uit de huidige wettelijke kaders en bij het opstellen van hun contractuele regelingen rekening houden met de toewijzing en beperking van deze risico's.

Ten derde is ook dataprivacy een belangrijk aandachtspunt. AI-systemen worden getraind op grote hoeveelheden gegevens die persoonsgegevens kunnen bevatten. Daarom moet zorgvuldig beoordeeld woden of persoonsgegevens worden gebruikt en verwerkt, bijvoorbeeld door werknemers. Het simpelweg laten nakijken op spelfouten van een tekst kan bijvoorbeeld al tot een datalek leiden als hierin klantgegevens worden genoemd.

Tot slot is er nog het vraagstuk van ethiek en discriminatie bij het gebruik van AI. Ethische bezwaren kunnen voortkomen uit vooroordelen in AI-modellen of effecten van AI op gebruikers of de samenleving. Ethische overwegingen kunnen ook ontstaan door gegevens die worden gebruikt of gegenereerd door AI. Onethische resultaten kunnen leiden tot negatieve gevolgen voor klanten en belanghebbenden of wettelijke aansprakelijkheid van het bedrijf. AI kan bestaande vooroordelen en stereotypen in de samenleving weerspiegelen en versterken. Trainingsgegevens kunnen patronen bevatten van systemische discriminatie. Het algoritme zelf kan vooringenomenheid vertonen door afhankelijk te zijn van bepaalde gegevens. Iets voor bedrijven om rekening mee te houden bij hun gebruik van AI.

Hoe waarborg je privacy en ethiek binnen generative AI?

Om privacy en ethiek in AI te waarborgen is het belangrijk dat organisaties hierin stappen nemen:

1. **Kwaliteitscontrole:** Controleer de output om er zeker van te zijn dat de gegevens niet bevooroordeeld zijn en of deze relevant, nauwkeurig en betrouwbaar zijn. Experts in hun vakgebied kunnen sneller beoordelen of de output juist en relevant is. Sommige modellen kunnen namelijk erg overtuigende output genereren die niet inhoudelijk juist blijkt te zijn. Standaardprocedures kunnen worden ingericht om om iedere output op juistheid te checken.
2. **Contractuele controle:** Bespreek van tevoren met klanten of er gegevens zijn die niet gedeeld mogen worden. Ook niet binnen goedgekeurde AI-modellen. Het is namelijk vaak onzeker hoe AI-modellen precies de ingevoerde informatie gebruiken, zelfs als de privacyverklaring van het AI-model aangeeft dat gegevens verwijderd zullen worden.
3. **Aanpassen privacybeleid:** Duidelijk is dat het gebruik van generative AI aan privacy gerelateerde risico's met zich mee kan brengen. Om deze te mitigeren kan een aanpassing in het privacybeleid een oplossing bieden. Een voorbeeld is een kennisgeving aan klanten over welke soorten AI worden gebruikt, voor welke doeleinden, hoe eventuele toestemming van de klant wordt gevraagd en of zij opt-in of opt-out opties hebben voor het gebruik van AI.
4. **Verantwoording en toezicht:** Zorg voor verantwoording en toezicht door het aanwijzen van verantwoordelijke personen of teams die belast zijn met het beheer van AI-systemen en de bescherming van privacy en ethiek. Zorg ervoor dat er duidelijke lijnen van verantwoordelijkheid en aansprakelijkheid zijn.

Als voorbeeld kan hierbij gekeken worden naar Microsoft dat al een reeks initiatieven heeft genomen om privacy en ethiek binnen AI te bevorderen. Hiervoor hebben zij het AI and Ethics in Engineering and Research (AETHER) Committee opgericht, dat toezicht houdt op de ethische praktijken van AI binnen het bedrijf. Daarnaast heeft het ook de Microsoft AI-principes geïntroduceerd, waarin de nadruk wordt gelegd op eerlijkheid, transparantie, privacy en verantwoording bij het ontwikkelen en implementeren van AI-technologieën.

Het AETHER-comité fungeert als adviserend orgaan voor de senior board en het "office of Responsible AI". Het formuleert aanbevelingen op het gebied van beleid, processen en best practices. Het comité heeft zes werkgroepen die zich richten op het ontwikkelen van specifieke richtlijnen op basis van hun expertise.

OpenAI, het bedrijf achter ChatGPT, heeft zich toegelegd op het waarborgen van ethische en verantwoorde AI. Het heeft hiervoor richtlijnen opgesteld om het gebruik van AI in overeenstemming te brengen met huidige normen en heeft maatregelen genomen om mogelijke misbruiken te voorkomen. Hiervoor beperkt OpenAI bijvoorbeeld de gegevensopslag tot 30 dagen, werkt ze aan anonimiseren van verzamelde gebruikersgegevens en zorgt ze ervoor de verzamelde gegevens niet te gebruiken voor doeleinden die de privacy van gebruikers kunnen schenden.

Deze organisaties zijn zich bewust van ethische en privacygevoelige aspecten van AI en komen tot een verhoogde privacy in hun AI-systemen door rekening te houden met enkele basis stappen [8].

De toekomst van privacy in AI voor bedrijven zal waarschijnlijk verder worden beïnvloed door nieuwe ontwikkelingen zoals het Internet of Things (IoT), virtuele assistenten en autonome voertuigen. Deze ontwikkelingen hebben het potentieel om de manier waarop we met technologie en elkaar omgaan te transformeren. Ze brengen echter ook

extra uitdagingen op het gebied van privacy met zich mee. Het Internet of Things verwijst bijvoorbeeld naar het netwerk van verbonden apparaten, zoals slimme kantoren en draagbare apparaten, die gegevens kunnen verzamelen en delen. IoT-apparaten verzamelen vaak grote hoeveelheden gegevens, zoals onze locatie, gewoonten en voorkeuren. Deze gegevens kunnen worden gebruikt om gedetailleerde profielen van individuen te maken, wat zelfs kan leiden tot vormen van profilering en geautomatiseerde besluitvorming. Generative AI is dus nog maar het begin.

Generative AI kan ongetwijfeld een gamechanger zijn op het gebied van productiviteit en effectiviteit voor veel bedrijven. Echter brengt het, zoals in dit artikel besproken, ook verschillende vormen van mogelijke privacy-schendingen en ethische bezwaren met zich mee. Deze zullen alleen maar groter worden met de introductie van AI in combinatie met nieuwe technologieën zoals IoT. Organisaties die nu al inspelen op privacy en ethiek met bovengenoemde suggesties binnen hun AI-gerelateerde bedrijfsvoering, onderscheiden zich hiermee positief op de markt. Zij zijn de concurrentie een stap voor en bieden hun gebruikers meer vertrouwen.

Over de auteurs:

Jorrit Tromp

Jorrit is een privacy consultant met een solide juridische achtergrond. Hij heeft een passie voor privacy en gelooft sterk in het belang van het beschermen van persoonlijke gegevens in het digitale tijdperk. Hij zet zijn analytische vaardigheden graag in om mee te denken over complexe privacyvraagstukken.

Mail: jorrit.tromp@capgemini.com

LinkedIn: https://www.linkedin.com/in/jorrit-tromp-402627aa/

Selma Mujcic

Selma is een ervaren privacyadviseur die haar kennis van innovatieve technologieën combineert met een strategische benadering van privacy en cybersecurity om bedrijven te helpen bij het realiseren van duurzame en veilige groei. Selma's expertise en inzicht maken haar uniek in haar vakgebied en stellen haar in staat om bedrijven te begeleiden in deze voortdurend veranderende digitale wereld.

Mail: selma.mujcic@capgemini.com

LinkedIn: https://www.linkedin.com/in/selmamujcic/

Bronnen:

1. https://targettrend.com/nl/generative-ai/
2. https://www.entrepreneur.com/science-technology/how-chatgpt-and-generative-ai-can-transform-your-business/445066
3. https://www.entrepreneur.com/science-technology/how-chatgpt-and-generative-ai-can-transform-your-business/445066
4. https://nl.marketscreener.com/beursnieuws/laatste/Wat-is-Generative-AI-de-technologie-achter-OpenAI-s-ChatGPT--43272490/
5. https://nl.marketscreener.com/beursnieuws/laatste/Wat-is-Generative-AI-de-technologie-achter-OpenAI-s-ChatGPT--43272490
6. Samsung ChatGPT leak: Samsung workers accidentally leak trade secrets to the AI chatbot | Mashable
7. ChatGPT: Mayor starts legal bid over false bribery claim - BBC News
8. https://help.openai.com/en/articles/7730893-data-controls-faq

03

Trends in Cybersecurity 2023

DETECTEREN EN REAGEREN

VERSTERK JE OT-BEVEILIGING: ONTDEK DE KRACHT VAN DE CLOUD EN EEN DREIGINGSANALYSE OP MAAT

Hoe kunnen organisaties hun OT-installaties beschermen tegen de cyberdreigingen van vandaag en morgen?

Operational Technology-systemen (OT) zijn een geliefd doelwit voor cyberterroristen. Dat blijkt wel uit recente aanvallen op OT overal in de wereld[1]. Het bewijst het cruciale belang van goede beveiliging voor OT-omgevingen en voor de controle van fysieke systemen en processen. OT-omgevingen zijn gebaseerd op specifieke architecturen en protocollen, en hebben in vergelijking met traditionele IT-omgevingen hele specifieke beveiligingseisen. Helaas vergeet men OT-omgevingen vaak als het om beveiliging gaat, of die beveiliging voldoet niet. Vandaar dus dat cybercriminelen er graag en vaak hun pijlen op richten.

De implementatie van een OT SOC (Operational Technology Security Operations Center), in combinatie met een SIEM-oplossing in de cloud (Security Information en Event Management) kan de beveiliging van OT een flinke boost kunnen geven. Dankzij continue monitoring, dreigingsanalyse en robuuste incident response capabilities levert een dergelijke aanpak een vitale bijdrage aan de beveiliging van OT-omgevingen tegen cyberdreigingen. Dit artikel biedt een verkenning van de mogelijkheden en een aantal strategieën om de beveiliging van OT te versterken.

Synergie tussen mens, proces en technologie

Voor sommige sectoren zijn OT-systemen cruciaal. Gezien het belang van die sectoren – neem energie – is robuuste cyber-beveiliging essentieel. Een OT SOC kan die robuustheid leveren, dankzij de volgende kerncomponenten:

- **Mensen:** Multi-skilled domein-experts en engineers in Supervisory Control and Data Acquisition (SCADA) en Distributed Control Systems (DCS), automatisering en procescontrole;
- **Technologie:** Workflows, dreigingsdetectie, log data-collectie, asset visibility;
- **Proces:** Consensus gebaseerd op overeenstemming in en tussen teams, volledig getest, aanpasbaar en altijd in ontwikkeling.

Het OT SOC beschermt niveau 0, 1, 2 en 3 van de systeemarchitectuur; deze niveaus zijn gedefinieerd in het referentiemodel van Purdue en het contextuele IEC-62443-model voor industriële systeemarchitecturen.

De kerncomponent technologie omvat technologieën zoals EDR CMDB, firewall management, ticketing, vulnerability management, SIEM en OT monitoring. SIEM speelt een cruciale rol in de correlatie van logs afkomstig van alle technische controlepunten binnen de OT-installatie.

Highlights

- Een gedegen aanpak van digitale veiligheid voor Operational Technology (OT)-systemen begint met de implementatie van een OT SOC (Security Operations Centre).
- Ten opzichte van traditionele on-premise-beveiliging heeft cloud-gebaseerde SIEM (Security Information and Event Management) grote voordelen; denk aan grotere schaalbaarheid, beschikbaarheid, kosteneffectiviteit, flexibiliteit en betere beveiliging.
- De outsourcing van het OT SOC naar een MSSP (Managed Security Service Provider) verlicht de druk op de organisatie. Deze hoeft immers niet te investeren in de vorming en het management van een team en het beheer van een security-infrastructuur.
- Maatwerk-dreigingsanalyse draagt bij aan de effectiviteit van het OT SOC: accurate detectie en reactie, grotere zichtbaarheid, snellere reactietijden en beter risk management.
- De combinatie van cloud-gebaseerde SIEM-oplossingen en dreigingsanalyse op maat resulteert in een meer volledige en effectieve benadering.

Cloud-gebaseerde SIEM-oplossingen zoals Microsoft Sentinel, Splunk en QRadar bieden voordelen als het gaat om schaalbaarheid, kosteneffectiviteit en beveiligings-features. Dreigingsanalyse biedt maatwerk-oplossingen voor dreigingsdetectie en –mitigatie.

Verbeterde OT-beveiliging dankzij SOC: verschillende benaderingen

Het SOC kan op verschillende manieren worden ingezet:

- Integratie van OT-capaciteiten in het IT SOC;
- Toepassing van een dedicated OT SOC;
- Outsourcing van OT SOC naar MSSP;
- Hybride benadering van het bovenstaande.

Cyber-dreigingen komen steeds vaker voor – en ze zijn steeds geraffineerder. Organisaties staan daarom onder continue druk om hun OT-systemen beter te beveiligen. Aanvallers met gespecialiseerde kennis zijn in staat om kwetsbaarheden uit te buiten en de operatie te verstoren, met financiële schade en gevaren voor de publieke veiligheid tot gevolg. In OT-systemen staat bovendien waardevolle data en waardevol intellectueel eigendom opgeslagen. Dat maakt ze vatbaar voor diefstal of bedrijfsspionage. In antwoord op deze dreiging zijn gespecialiseerde OT SOC's ontwikkeld. Daarmee kunnen bedreigingen worden opgespoord en wordt een effectieve reactie mogelijk op digitale bedreigingen als aanvallen met ransomware, aanvallen op de supply chain, aanvallen door insiders en fysieke sabotage van OT-systemen.

De in het OT SOC gebruikte tools zijn afkomstig uit de IT, maar aangepast aan de specifieke bedreigingen van de

OT-sector en de specifieke eisen en communicatieprotocollen van OT. De aanpassingen behelzen onder meer het volgende:

- Analyse en interpretatie van industrie-specifieke protocollen;
- Toepassing van OT-jargon en -afkortingen;
- Grote diversiteit in endpoints, variërend van Windows tot Linux, van PLCs tot proprietary operating systems en firmware;
- Gevolgen van technologie: het uitvoeren van een tool in een OT-omgeving;
- Aanpassingen aan OT- en sectorspecifiek dreigings-'landschap'.

Stel je voor dat je een security manager bent voor een oliemaatschappij die haar productie op verschillende locaties wil uitbreiden. Om overal de cybersecurity te borgen en een hoog beveiligingsniveau te garanderen met 24/7 monitoring van bedreigingen, zou je normaal gesproken op elke locatie een OT SOC moeten bouwen. Dat is kostbaar en tijdrovend. Door toepassing van een cloud-gebaseerde SIEM-oplossing in het OT SOC is additionele hardware niet nodig. Zo'n SIEM-oplossing biedt bovendien toegang op afstand, is kosteneffectief, flexibel en veilig. Het is de ideale keuze voor organisaties die willen uitbreiden en tegelijkertijd digitale dreigingen buiten de deur willen houden.

De voordelen van de cloud-gebaseerde SIEM-oplossing

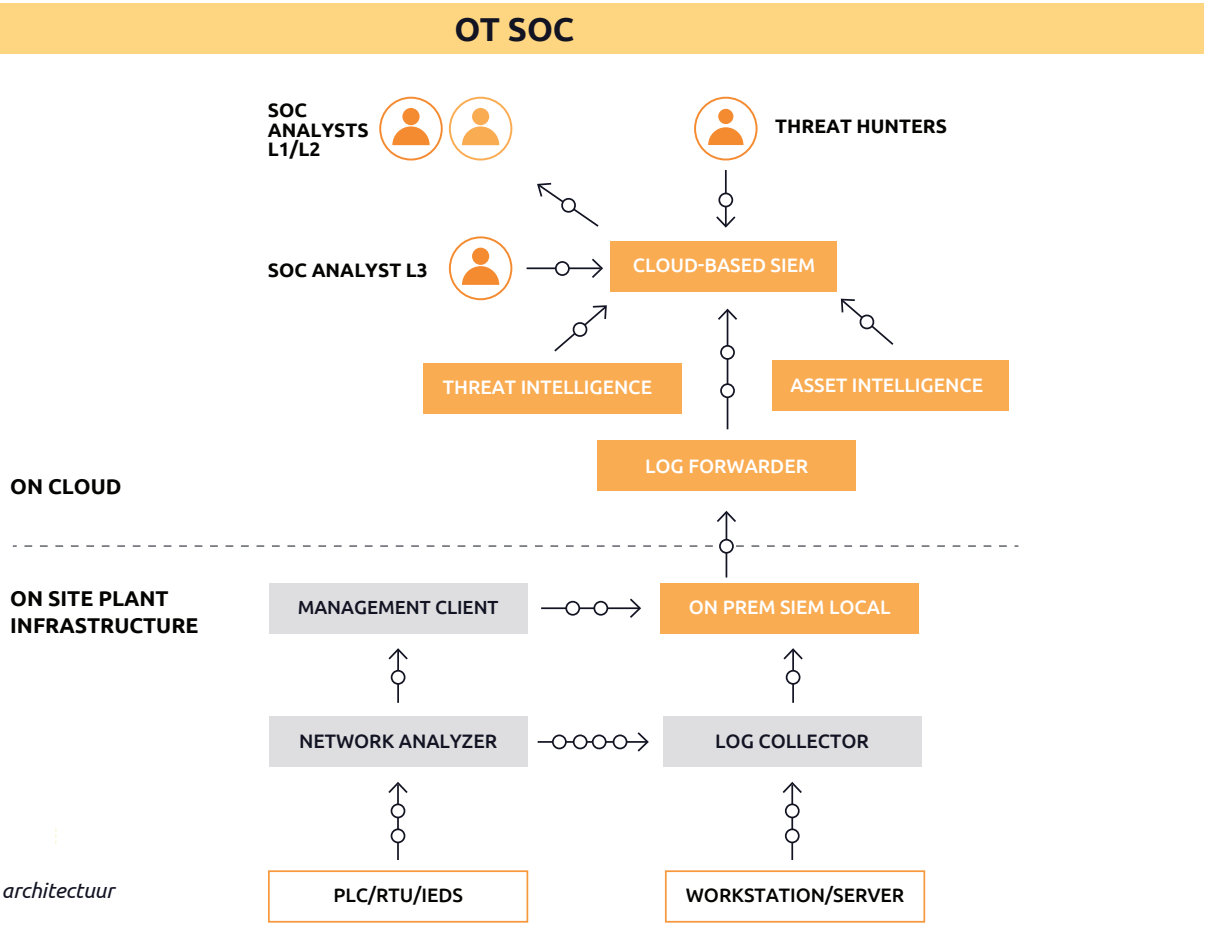
Cloud-gebaseerde SIEM biedt voor OT SOC's de volgende voordelen:

- **Schaalbaarheid:** Eenvoudig op- en afschalen in het geval van veranderde eisen, zonder dat extra hardware of infrastructuur nodig is.
- **Beschikbaarheid:** Is overal beschikbaar en benaderbaar. Daardoor kunnen security-teams overal ter wereld met elkaar, met andere teams en met andere stakeholders samenwerken.
- **Kosteneffectiviteit:** Biedt kostenvoordelen in vergelijking met on-premise-oplossingen; er is immers geen hardware, onderhoud of upgradecyclus nodig. Daardoor komen middelen vrij voor andere belangrijke investeringen in cybersecurity.
- **Flexibiliteit:** Biedt grotere flexibiliteit als het gaat om de in te zetten tools en opties. Organisaties kunnen zo de oplossing samenstellen die het beste invulling geeft aan hun specifieke behoeften en eisen.
- **Betere beveiliging:** Biedt verbeterde beveiligingsmogelijkheden, inclusief robuust authenticatie- en toegangsbeheer, encryptie en continue monitoring.
- **Integratie:** Biedt grotere integratiemogelijkheden met on-premise oplossingen voor monitoring zoals Nozomi, Dragos en Tenable. Daardoor daalt de overhead voor on-site monitoring op applicatieniveau.

Om een on-premise SIEM in de lucht te houden moet de organisatie een team van beveiligingsprofessionals inhuren en managen. Dat kan tijdrovend en duur zijn. Door een cloud-gebaseerde SIEM te outsourcen naar een MSSP, krijg je de beschikking over een dedicated team van beveiligingsexperts. Dit team beheert en onderhoudt de infrastructuur. De organisatie hoeft haar cybersecurity niet in eigen huis te beheren. Dat scheelt tijd, middelen en aandacht.

Cloud-aanbieders werken volgens certificerings- en compliance-standaarden. Daardoor wordt het makkelijker om te voldoen aan regelgeving. Cloud-data wordt bovendien opgeslagen in een specifieke geografische regio; dat kan helpen bij het voldoen aan plaatselijke regelgeving omtrent privacy. Door data op te slaan op verschillende locaties binnen dezelfde regio kun je bovendien de weerbaarheid verbeteren en het risico beperken op downtime of verlies van data.

Op macroniveau ziet het SOC, hier met Microsoft Sentinel, eruit zoals weergegeven in figuur één. MSSP's kunnen Microsoft Sentinel vanaf elke locatie benaderen, terwijl de data zelf opgeslagen blijft op een en dezelfde geografische locatie.



Figuur 1: OT SOC architectuur

Hoe dreigingsanalyse op maat binnen cloud-gebaseerde OT SIEM kan resulteren in maximale operationele efficiëntie

De toevoeging van dreigingsanalyse op maat aan cloud-gebaseerde OT SIEM kan zorgen voor grotere operationele efficiëntie. Dreigingsanalyse op maat is aangepast aan het unieke dreigingslandschap van de organisatie en biedt verschillende voordelen. De analyse is afkomstig van experts die de activiteit van vijanden observeren binnen specifieke sectoren of geografische regio's. De dreigingsanalyse kan informatie bevatten over de tactieken, technieken en procedures (TTP's) van de aanvallers; bijvoorbeeld het type phishing-email dat ze gebruiken, het lokaas dat ze inzetten om ontvangers te verleiden op een link te klikken of een attachment te downloaden, of de malware die ze gebruiken om de computer van het slachtoffer te infecteren. Met deze informatie kunnen beveiligingsteams proactief op dergelijke bedreigingen monitoren, deze detecteren en gepaste actie ondernemen om de aanval te voorkomen of mitigeren.

Laten we nog een aantal andere voordelen van OT SOC nader bekijken:

- Ten eerste kan het OT SOC worden aangepast aan specifieke OT-omgevingen, met hun eigen, unieke bedreigingen en kwetsbaarheden. Daardoor wordt meer gerichte, effectievere detectie van bedreigingen mogelijk en groeien de mogelijkheden om effectief te kunnen reageren.
- Ten tweede kun je, door OT-assets maximaal te integreren in SIEM, de 'monitorbaarheid' van de OT-omgeving vergroten. Dat stelt beveiligingsteams in staat om potentiële bedreigingen en kwetsbaarheden sneller en makkelijker te identificeren.
- Ten derde biedt het OT SOC real-time alerts en automatische maatregelen, gebaseerd op aanpasbare regels en beleid. Dat stelt beveiligingsteams in staat sneller te reageren op potentiële bedreigingen.
- Ten slotte: dreigingsanalyse op maat draagt bij aan een breder inzicht in het risicoprofiel van de organisatie. Daardoor kunnen beveiligingsteams middelen prioriteren en beheersmaatregelen implementeren die passen bij de unieke behoeften en uitdagingen van de organisatie.

Dankzij de voordelen van OT SOC, cloud-gebaseerde SIEM en dreigingsanalyse op maat kunnen organisaties hun OT-omgeving beter beschermen tegen potentiële dreigingen en kwetsbaarheden. Een fabriek kan bijvoorbeeld dreigingsanalyse op maat gebruiken om het machinepark te monitoren op potentiële aanvallen, en snel reageren op gedetecteerde dreigingen om zo uitval van de productie te voorkomen.

De voordelen van een SIEM in de cloud en van dreigingsanalyse op maat zijn nauwelijks te overschatten. Cloud-gebaseerde OT SIEM-oplossingen bieden grotere schaalbaarheid, beschikbaarheid, kosteneffectiviteit, flexibiliteit en uitgebreide beveiligingsmogelijkheden. Een dreigingsanalyse op maat helpt bij de verfijning van dreigingsdetectie en de implementatie van effectieve beheersmaatregelen die zijn ontworpen voor de unieke uitdagingen van OT-omgevingen.

Door OT SOC en cloud gebaseerde SIEM te combineren kunnen organisaties hun kritische infrastructuur en assets beter verdedigen tegen de dreigingen van vandaag en morgen, en zijn ze beter in staat om hun cybersecurity-risico's te beheren. Organisaties die prioriteit geven aan de toepassing van cloud-gebaseerde SIEM-oplossingen en dreigingsanalyse op maat kunnen een robuuster veiligheidsprofiel opbouwen, dat ze in staat stelt om de groeiende cybersecurity-uitdagingen het hoofd te bieden.

Het loont de moeite om onderzoek te doen naar verschillende cloud-gebaseerde OT SIEM-oplossingen en naar aanbieders van dreigingsanalyse op maat die zijn gespecialiseerd in beveiliging van industriële controlesystemen. Ze kunnen een grote rol spelen in de effectieve beveiliging van de kritische infrastructuur van je organisatie.

Over de auteur:

Sourabh Suman

Sourabh, Managing Consultant bij Capgemini, ondersteunt klanten in Olie & Gas, Energie en Manufacturing voor robuuste veiligheid. Hij is gespecialiseerd in implementatie van beveiligingsstandaarden (62443, NIST) en ontwerp van beveiligingsarchitectuur. Sourabh is een gecertificeerde GICSP-expert en auteur van "Unblocking Your Potential in ICS Cybersecurity". Hij traint ook via Udemy in ICS Cybersecurity. Met expertise en ervaring helpt hij organisaties veiligheidsrisico's te traceren en te verminderen, voor bescherming tegen cyberdreigingen.

Mail: sourabh.suman@capgemini.com

LinkedIn: https://www.linkedin.com/in/sourabhsuman0/

Bron: https://www.techtarget.com/searchsecurity/news/252504484/Gartner-Weaponized-operational-tech-poses-grave-danger

PROBEREN TE RENNEN, TERWIJL JE NOG NIET KUNT LOPEN: DE RELATIE TUSSEN THREAT HUNTING EN CYBERSECURITY MATURITY

Hoe helpt threat hunting bij het weren van geavanceerde bedreigingen?

Highlights

- Threat hunting draait om een gerichte, iteratieve benadering waarin je je inzicht in je netwerk inzet om je verdediging ervan op een proactieve manier vorm te geven – en threat actors in een vroeg stadium te betrappen.
- De volwassenheid van je organisatie en je bereidheid te investeren in de basale maatregelen hebben directe invloed op de effectiviteit van je threat hunting-programma.
- Ben je een aantrekkelijk doelwit, of een target of opportunity? Het antwoord op die vraag biedt richting in de vormgeving van je eigen beveiligingsstrategie en biedt inzicht in de investering die daarvoor nodig is.
- De hierarchy of needs van Matt Swann is een uitstekende visualisatie die je helpt te begrijpen waarom de bouwstenen van cyberbeveiliging van elkaar afhankelijk zijn.
- Threat hunting is in elk stadium van de cybersecurity-reis een waardevolle investering, maar de effectiviteit ervan groeit naarmate de volwassenheid toeneemt.

'Dat betekent wat anders dan je denkt!' Het is een zinnetje dat experts op het gebied van cyberveiligheid regelmatig in de mond nemen. En dat is een beetje onze eigen schuld. In de nooit aflatende strijd die de verdedigers voeren tegen kwaadwillenden, worden continu nieuwe methodes en technologieën ontwikkeld. Daar bedenken we dan allerlei spannende namen voor. Die namen bereiken vervolgens het grote publiek – en die hangen er vervolgens een spannende betekenis aan die niet strookt met de werkelijkheid. Threat hunting is zo'n term. In dit artikel willen we de verwarring die ook over dit begrip bestaat wegnemen; wat is het, hoe past het in je cyberveiligheids-profiel en – het belangrijkste – hoe helpt het je organisatie om geavanceerde bedreigingen buiten de deur te houden?

Wat is threat hunting?

Het SANS-whitepaper The (Who, What, Where, When, Why and How of Effective Threat Hunting) geschreven door Robert M. Lee[1] geeft de beste definitie: threat hunting is "een gerichte, iteratieve benadering om kwaadwillenden die zich ophouden binnen het eigen netwerk te zoeken, identificeren en doorgronden."

Threat hunting gaat niet over de identificatie, prioritering en aanpak van dreigingsmeldingen in je beveiligingssysteem, of de toepassing van informatie over Indicators of Compromise (ioc; indicatoren van kwaadwillende activiteiten) in je endpoint response and detection-platform. Wat het dan wel is: een proactief, gericht onderzoek op basis van hypotheses, met als doel kwaadwillenden een halt toe te roepen nog voordat ze hun aanval kunnen inzetten. Met 'aanval' bedoelen we zaken als datadiefstal, ransomware of andere overtredingen die je Data Privacy Officers een slechte dag bezorgen.

De definitie van SANS vestigt de aandacht op twee elementen die van belang zijn voor succesvolle threat hunting: het doorgronden van jezelf en van de vijand. Om de organisatie die je verdedigt te kunnen doorgronden, moet je eerst je eigen infrastructuur begrijpen en je eigen zichtbaarheid daarin. Om je vijand te kunnen doorgronden, moet je diens capaciteiten, intenties en mogelijkheden om je met succes aan te vallen doorgronden, waarbij je de laatste inschatting maakt op basis van informatie over de cyberdreigingen waaraan je organisatie mogelijk kan worden blootgesteld. De threat hunter voert op basis van deze elementen een proactief onderzoek uit, ondersteund door de juiste technologie, om het brandgevaar te identificeren voordat de brand uitbreekt en het vermogen van je organisatie om zaken te doen in de as wordt gelegd. De threat hunter maalt niet om standaard-malware of een beetje crypto currency mining; we maken ons meer druk om Advanced Persistent Threats (APT) en georganiseerde cybercrime-bendes; het soort vijanden dat er steeds weer in slaagt om je geautomatiseerde security te omzeilen.

Het is ontegenzeggelijk de droom – de bad actor tot staan brengen en eindelijk tastbaar bewijs leveren dat je verzoek voor een groter budget voor cyberbeveiliging terecht was. Maar is je organisatie volwassen genoeg om threat hunting te implementeren? De Threat Hunting Survey 2022 van SANS[2] legt de vinger op de gevoelige plek: vaak ontbreekt het aan personeel met de juiste skills, budget, technologie of processen om threat hunting goed te kunnen organiseren. Ook zijn vaak niet de benodigde inlichtingen over dreigingen voorhanden, en ziet het management threat hunting niet als prioriteit. De survey is al met al de moeite van het lezen waard – het is een verhelderend verhaal over de uitdagingen en successen waarmee organisaties te maken krijgen bij de implementatie van een programma voor threat hunting. Daarmee zegt de survey iets over de manier waarop organisaties kijken naar cyberbeveiliging, en de relatieve beveiliging van organisaties: zijn ze bereid om te investeren in mensen en technologie die dit zeer specialistische werk moeten uitvoeren? Is er commitment voor de meest basale maatregelen en bouwstenen, zoals een visie, strategie, governance, budget, inventarisatie van je assets en wellicht een functionerend SOC? Het is goed je daarvan te vergewissen, voordat je je threat hunters op pad stuurt met

niet meer dan het equivalent van een scherpe stok en een rol duct tape als instrumenten. Threat hunting kan in elk stadium van volwassenheid zinvol zijn, maar de impact ervan neemt flink toe als je hebt geïnvesteerd in de basics die ik net noemde en als je vervolgens verder blijft bouwen aan de robuustheid van je cyberbeveiliging. Hoe minder tijd je threat hunting team bezig is met compenseren voor zaken die niet voorhanden zijn, of verdwaald raakt in onduidelijke processen en communicatielijnen, hoe beter het is. De tijd die ze besparen kunnen ze immers gebruiken om daadwerkelijk boeven te vangen.

Threat hunting en de volwassenheidskwestie

Bij dit soort overwegingen is enige nuance natuurlijk op zijn plaats. Threat hunting is in geen enkel opzicht een triviale investering. De potentiële kosten van een ernstig incident kunnen de kosten overstijgen die zijn gemoeid met de beveiliging van je organisatie, maar dan nog moet je er wel voor zorgen dat de investeringen die je doet in proportie blijven met de potentiële schade die een aanval jouw specifieke organisatie kan berokkenen. Of het voor jouw organisatie urgent is om een threat hunting-programma uit te rollen, hangt ervan af of je een aantrekkelijk doelwit vormt. Daar zou je dus eerst eens het gesprek over aan moeten gaan.

Of je een aantrekkelijk doelwit bent, hangt dan weer af van de intenties van de cyber-bedreiger. Wat zou die bedreiger beschouwen als je kroonjuwelen? En wat zou hij willen met die kroonjuwelen: stelen, ontregelen, beschadigen? Laat ik een voorbeeld geven: organisaties die gelieerd zijn aan overheden of kritieke infrastructuren, of organisaties die zich specialiseren in heel specifieke (medische) technologie of manufacturing kunnen heel wel een doelwit vormen voor natiestaten die uit zijn op algehele ontwrichting. Zo'n vijand investeert tijd, moeite en middelen om rond jouw organisatie een aanvalscampagne op te tuigen, waarin al je kwetsbaarheden worden uitgebuit – of dat nou je leveranciers zijn, of de slordige omgang met wachtwoordbeveiliging van je medewerkers, of een slecht gepatched systeem. Tegen de dreiging van APT's zoals deze moet je een volwassen, goed georganiseerde en proactieve cyberbeveiliging in stelling brengen. Met alle toeters en bellen die beschikbaar zijn – inclusief een robuust Cyber Threat Intelligence-systeem (CTI). Alleen zo kun je dergelijke aanvallen wellicht weerstaan. Als je geen primair doelwit vormt, maar eerder een target of opportunity, dan ben je kwetsbaar voor aanvallen die niet per se specifiek zijn ontworpen om jouw kwetsbaarheden te benutten; bij dergelijke aanvallen vorm je één van vele doelwitten in een campagne die tot doel heeft zoveel mogelijk organisaties te treffen die een vergelijkbare kwetsbaarheid delen. Dit klinkt misschien minder verontrustend dan het eerste scenario, maar of dat ook zo is hangt ook hier af van de aanwezigheid van een goed functionerend CTI-programma. Dat laatste is de vraag, want gezien de in theorie minder grote dreiging is de investering die je daarvoor moet maken ook moeilijker te verantwoorden. In alle gevallen is een goede 'hygiëne' als het gaat om cyberbeveiliging cruciaal – maar ook dat hangt natuurlijk af van de volwassenheid van je organisatie. En in welke categorie je ook thuishoort, de impact van een incident is altijd groot.

Cyberbeveiliging en de Hierarchy of Needs

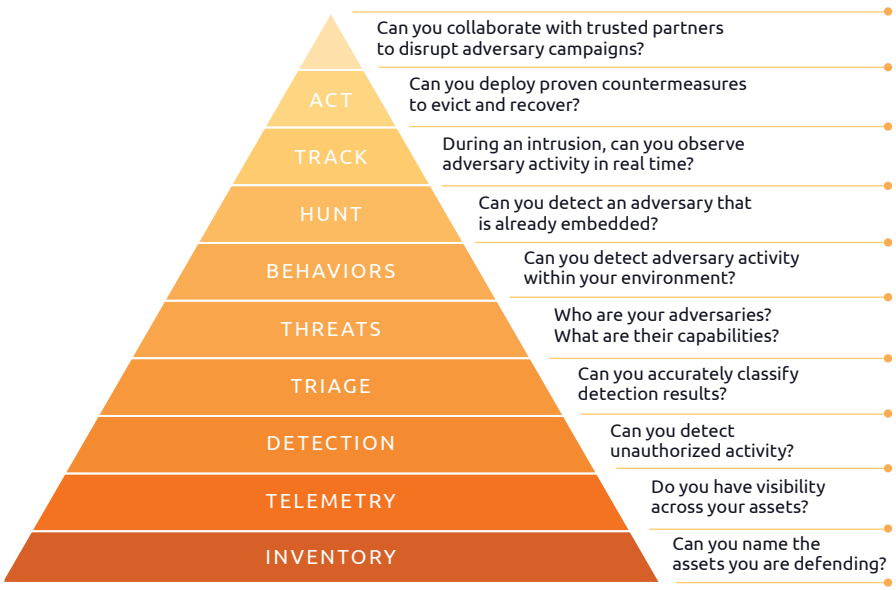
In het kader van 'ken de vijand en ken uzelf' staan we nu stil bij de volgende overweging: een realistisch beeld van de fundamentele bouwblokken voor cyberbeveiliging die op dit moment al aanwezig zijn in de organisatie. Matt Swann bedacht een heel bruikbare visualisering van de hiërarchie die bepaalt of een organisatie in staat is om haar assets te verdedigen (figuur 1).

Van onderaf bekeken vormt elke bouwsteen een voorwaarde voor de beantwoording van de vraag erboven. Zoals je ziet staat 'Hunt' pas vrij hoog in de piramide genoemd. Dat is ook logisch; het wordt een stuk lastiger om de 'jacht' naar behoren uit te voeren als je niet je niet in staat bent in staat bent een netwerktopologie te onderscheiden of een inventaris te maken van alle bestaande software binnen het landschap. Op dezelfde manier heb je telemetrie en databronnen nodig, wil je de jacht überhaupt kunnen starten.

Voor elk van deze bouwstenen bestaat een spectrum. Aan de ene kant van dat spectrum staat bijvoorbeeld een Endpoint Detection & Response (EDR)-platform dat al je systemen bestrijkt. Dat zorgt absoluut voor uitstekende dekking en vormt een waardevolle databron voor threat hunting. Aan de andere kant van het spectrum staan basale bronnen zoals netwerkdata, logging en het vermogen om endpoint-data te bevragen met een op maat geschreven set PowerShell-scripts; ook dat is al genoeg om een basale behoefte in te vullen.

Maar zoals zo vaak met modellen die zaken simpel voorstellen: de werkelijkheid is een stuk gecompliceerder. Wat threat hunting vooral zo interessant maakt, zelfs als het wordt toegepast in minder volwassen omgevingen, is het vermogen om de meest kritieke kwetsbaarheden (en daarmee de meest waarschijnlijke aanvalsroutes) als eerste te vinden. Een voorname bijvangst (en uiteindelijk vaak een van de grootste voordelen) van threat hunting is dat je er foutieve configuraties, hygiëne-problemen en blinde vlekken mee blootlegt; er is geen betere manier om je een beeld te verschaffen van de huidige situatie dan eens goed onder de motorkap van je IT-omgeving te kijken. Dit beeld kan dan weer dienen als input voor een realistische roadmap voor cyberveiligheid, die effectief gebruikmaakt van wat je al hebt en kritieke lacunes blootlegt die je als eerste moet aanpakken. Vooropgesteld uiteraard dat het management in staat en bereid is om te luisteren naar slecht nieuws.

Tot slot is er nog een interessante – maar misschien minder voor de hand liggende – maatstaf voor het vermogen van je organisatie om de voordelen van threat hunting te benutten: de visie van de organisatie op de toepassing van CTI. De oplettende lezer zal inmiddels hebben begrepen dat de effectiviteit van threat hunting direct



Figuur 1: Piramide van Matt Swann

verband houdt met (het niveau van) de toepassing van CTI in de organisatie. We moeten immers ergens beginnen. Een sterke CTI, inclusief begrip van organisatie-inzicht over potentiële tegenstanders en hun tactieken (TTP), biedt een realistisch vertrekpunt voor analisten. Door analyse en inzicht in het threat landscape van je organisatie, zijn threat hunters in staat om als eerste de indicatoren voor aanvallen aan te pakken die een grote impact hebben en die veel schade kunnen berokkenen. Hoeveel waarde jouw organisatie hecht aan een CTI, en in hoeverre het CTI is toegerust op haar taak, geeft een indicatie van de mate van begrip die bestaat over hoe holistische cyberverdedigings-maatregelen eruit horen te zien. Je zou kunnen beweren dat het omgekeerde ook waar is; in een organisatie met een volwassen threat hunting-programma is CTI als het goed is een kernproces (zoals ook de SANS 2022 Threat Hunting Survey al impliceerde) – en dat wijst dan weer op een hoge mate aan volwassenheid overall. Volwassenheid ligt niet alleen besloten in de processen, tooling en capabilities van een organisatie, maar ook in de buy-in en de bereidheid van het management team als het gaat om de herkenning en bestrijding van dreigingen. Een organisatie die de voordelen onderkent van een proactieve benadering zal eerder geneigd zijn om threat hunting en CTI op een geïntegreerde manier toe te passen en ze niet te zien als losstaande dingen die ook nog ergens op het afvinklijstje staan.

Waar staan we nu?

Concluderend: threat hunting is een proactieve manier om complexe, ingebedde dreigingen in een zo vroeg mogelijk stadium te vinden. Threat hunting kan een zeer waardevolle toevoeging zijn, ook als je organisatie nog maar beperkt volwassen is als het gaat om cyberbe-veiliging. Toch is er een directe correlatie tussen de effectiviteit van je threat hunting team en de aanwezigheid van een effectief beeld van je eigen positie in het dreigingslandschap, of je een eerlijke inschatting kunt maken over je eigen interne sterke punten en kwetsbaarheden, of en in hoeverre beslissers bereid zijn om de noodzaak van robuuste cyberbeveiliging te onderkennen – en of de wil bestaat om in al deze factoren te investeren. Uiteindelijk is het slechts een kwestie van tijd totdat je zult worden geconfronteerd met een inbreuk in je netwerk. Aan jou de keuze of je daarop een proactief of een reactief antwoord hebt. Hoe het ook zij: happy hunting!

Over de auteur:

Saskia Kuschke

Saskia Kuschke is een ervaren, GIAC gecertificeerde, Digital Forensics and Incident Response Investigator, en was Managing Consultant in het ATHIR (Advanced Threat Hunting & Incident Response) team ten tijde van het schrijven van dit artikel.

LinkedIn: https://www.linkedin.com/in/saskia-kuschke-9b3a22b3

Bronnen:

1. https://www.sans.org/white-papers/who-what-where-when-why-how-effective-threat-hunting/.
2. https://www.sans.org/white-papers/sans-2022-threat-hunting-survey/.
3. https://github.com/swannman/ircapabilities/.

04

Trends in Cybersecurity 2023

TECHNOLOGIEGERICHTE VEILIGHEIDSASPECTEN

SAP-BEVEILIGING: EEN ALLESOMVATTENDE BLUEPRINT VOOR OPTIMALE BESCHERMING

Hoe ontwerp je een blueprint voor de beveiliging van de SAP-applicatielaag?

Highlights

- De meeste cyberaanvallen vinden tegenwoordig plaats binnen de applicatie zelf. We moeten de beveiliging van de applicatie laag dus serieus nemen en niet alleen kijken naar de buitenste lagen.
- Het niet doorvoeren van belangrijke security patches vormt een groot risico.
- Ga je de core verstevigen? Begin dan met het laag hangende fruit. Daarmee kom je al een heel eind.
- Integreer SAP in bestaande SIEM-tools en maak gebruik van SAP-standaardtools zoals de SAP ASE en de SAP Solution Manager.
- Het beheren van je securitystrategie is een continu proces in verband met snel veranderende dreigingen, nieuwe wet- en regelgeving en maatregelen.

In het snel veranderende dreigings-landschap is meer nodig dan alleen verdediging van de buitenste laag van je SAP-systeem. Cyberaanvallen zijn steeds geraffineerder en gerichter. Organisaties moeten daarom een gelaagde benadering kiezen als het gaat om de security van SAP. Firewalls en inbraakdetectiesystemen blijven belangrijk, maar zulke systemen alleen zijn niet genoeg om je te verdedigen tegen de meer geavanceerde, hardnekkige bedreigingen waaraan SAP kan worden blootgesteld.

In dit artikel bekijken we de best practices en frameworks die je kunt inzetten om tot een blueprint voor SAP-security te komen. Zo'n blueprint biedt een solide basis om veranderingen in de organisatie te ondersteunen en helpt je het risico te elimineren op verlies van marktaandeel of reputatieschade. Deze SAP security-blueprint bestrijkt het volledige SAP-landschap, of het nu gaat om on-premise, een oplossing in de cloud of een hybride vorm. Als je een combinatie van landschappen hebt, zul je verschillende frameworks en benaderingen moeten combineren; alleen dan kun je er zeker van zijn dat je niks mist. Zo houd je kritieke componenten onder controle en beperk je het risico op problemen.

Beveiliging van applicaties in SAP

SAP-systemen zijn voor veel organisaties van levensbelang. Dat maakt ze tot een geliefd doel voor cyberterroristen. Om de organisatie goed te beschermen tegen zulke aanvallen is een allesomvattende benadering nodig van applicatiebeveiliging in SAP. Laten we daar eens wat langer bij stilstaan.

In SAP-systemen staan enorme hoeveelheden gevoelige data opgeslagen; denk bijvoorbeeld aan financiële informatie of klantgegevens. Inbreuk op deze data kan serieuze gevolgen hebben, zoals financiële schade, reputatieschade en juridische issues. Cyberaanvallen zijn steeds geraffineerder en aanvallers gebruiken allerlei technieken om toegang te krijgen tot SAP-systemen. Ze proberen kwetsbaarheden uit te buiten en zetten daarbij zaken in zoals social engineering en phishing. Het is van het grootste belang om een robuuste SAP-applicatiebeveiligingsstrategie te hebben. Alleen dan kan de organisatie dergelijke aanvallen weerstaan.

SAP-applicatiebeveiliging verwijst naar de maatregelen die worden genomen om de vertrouwelijkheid, integriteit en beschikbaarheid van SAP-systemen en data te bewaken. We hebben het dan bijvoorbeeld over toegangscontrole, monitoring van activiteit van gebruikers, bescherming tegen externe dreigingen en compliance met regelgeving. Beveiliging is cruciaal, om gevoelige businessgegevens te beschermen, niet-geautoriseerde toegang te voorkomen en ongewenste modificatie of vernietiging van data in SAP-systemen tegen te gaan. Het is een goed idee om als eerste de SAP security baseline te reviewen en te implementeren. De baseline is een set van beveiligingsconfiguraties en best practices die door SAP zelf worden aangeraden. De baseline bestrijkt verschillende gebieden, zoals authenticatie, autorisatie, encryptie, logging en monitoring. Implementatie van de SAP security baseline helpt bij de veilige configuratie van het SAP-systeem. Bovendien kun je zo borgen dat je systeem is ingericht op basis van best practices.

Door de SAP security baseline te implementeren, beperk je het risico op data-inbreuk of andere beveiligingsincidenten. Het is echter wel van belang dat je onthoudt dat

de baseline pas het begin is. Om het SAP-systeem echt te beveiligen, moet je verder gaan dan de baseline alleen. Er zijn additionele beveiligingscontroles voor nodig, gebaseerd op erkende frameworks zoals ISO27001, ISO27002 en zoals ISO207017, die specifiek zijn gericht op de cloud. Er zijn verschillende manieren om ISO-controles te integreren in SAP.

Door voor elke ISO-controle de corresponderende SAP-controle te identificeren, kun je vaststellen of alle controles een plek hebben in het SAP-systeem.

- De SAP security baseline en Secure Operations Map (SOM) vormen samen een bruikbare leidraad voor de vormgeving van een blueprint voor de beveiliging van het SAP-systeem. Check de verschillende lagen die worden genoemd in de security baseline van SAP en de SOM en maak op basis daarvan een checklist voor de applicatielaag, de database, het OS, de interface (netwerk), de governance, enzovoort.
- Gebruik de bestaande ISO-controles en vertaal ze in controles die van toepassing zijn op het SAP-landschap.
- Doe dit voor zowel on premise SAP-oplossingen als voor cloudapplicaties als Ariba en SAC. Er moet in elk geval een robuust autorisatieconcept aanwezig zijn en je moet ook invulling geven aan monitoring van de audit logs (ook, indien van toepassing, in verband met SIEM).
- We kunnen verschillende SAP-tools toepassen: Security Recommendation Tool voor ontbrekende SAP Security Notes, EWA (Early Watch Alerts) om de SAP-kernelversie en database te monitoren en te controleren op ontbrekende beveiligingsconfiguraties, Solution Manager om inzicht te krijgen in landschap en monitoring en SAP Read Access Logging om gevoelige informatie te monitoren.

Verstevig de core: 'laaghangend fruit', dat weinig inspanning en/of ingewikkelde tools vergt.

Ben je weleens op uitdagingen gestuit bij het verhelpen van complexe SAP-beveiligingsissues? Vind je het beter om je eerst te richten op deze issues, of is het verstandig om eerst de issues aan te pakken die snel te verhelpen zijn?

SAP-security is een cruciaal component van de security posture - het veiligheidsprofiel - van elke organisatie. Het SAP-systeem is een complex platform met vele facetten en dat componenten omvat met allerlei onderlinge afhankelijkheden. Zo'n systeem beveiligen vergt daarom ook een aanpak met verschillende facetten. Het is echter altijd een goed idee om de core te verstevigen en het laaghangende fruit te plukken.

De core verstevigen wil zeggen dat je fundamentele beveiligingsfouten in het systeem identificeert en aanpakt. Het gaat dan om zaken als beveiliging van de database, hardening van het Operating System, en borging van goede controle van netwerktoegang. Dit lijken misschien voor de hand liggende maatregelen, maar ze vormen een essentiële basis voor andere, meer geavanceerde beveiligingsmaatregelen.

Het laaghangende fruit verwijst naar makkelijk te verhelpen kwetsbaarheden die een grote impact hebben op de algehele beveiliging. Deze kwetsbaarheden kunnen zaken omvatten als default-SAP-accounts en zwakke wachtwoorden, patches die niet zijn doorgevoerd en parameters die met de installatie zijn gezet, maar nooit meer zijn herzien. Door eerst deze kwetsbaarheden aan te pakken kunnen organisaties flinke stappen zetten in de versteviging van hun algehele beveiliging, zonder dat daar heel veel tijd of middelen mee zijn gemoeid.

- Maak gebruik van standaard SAP-tools als RSUSR003 en SUIM om het system snel te scannen op default SAP-accounts en gebruikers met hoge autorisatieniveaus (zoals SAP_ALL-profielen) en/of kritische transacties zoals SE16.
- De integratie van SAP SIEM kan in beeld komen; dat is onderdeel van cyberverdediging en cyber-dreigingsdetectie. Onderzoek de mogelijkheden om SAP-systemen te integreren met de bestaande SIEM-tool.
- De System Monitoring-applicatie binnen SAP Solution Manager biedt een overzicht van de huidige status van technische systemen, waaronder gerelateerde instances, databases en hosts.

Gebruik tools van vertrouwde partners voor assessments en scans.

Zou automatisering van waarde kunnen zijn voor het beveiligingsbeheer van je SAP-systeem?

In dat geval zou je eens kunnen kijken naar de in de markt beschikbare beheertools. Gelukkig zijn er tegenwoordig verschillende dienstverleners die in SAP-beveiliging zijn gespecialiseerd en die tools bieden waarmee het beheer van SAP-beveiliging een stuk eenvoudiger wordt.

Zo zijn er bijvoorbeeld tools en technologieën die potentiële kwetsbaarheden identificeren en de overall robuustheid van de beveiliging van je SAP-systeem kunnen inschatten. Met deze tools kun je een maatwerk-strategie ontwikkelen voor de bescherming van je waardevolle data tegen cyberdreigingen. Door technologisch geavanceerde tools voor Vulnerability Assessment en Management Activities in SAP toe te passen, kun je op een holistische manier, en op basis van inzicht in de laatste trends, de kwetsbaarheden in je systeem blootleggen. Sommige tools bieden real time monitoring en alerts, om snel verdachte activiteiten te kunnen vaststellen en maatregelen te treffen om de risico's te mitigeren.

De benadering voor de creatie van een blueprint voor SAP-beveiliging kun je ook toepassen bij de vergelijking van

verschillende tools voor SAP security management. Geeft de tool van jouw voorkeur invulling aan alle componenten van de SAP security baseline? En aan alle ISO-controles? Is de tool compatible met je bestaande SIEM-oplossing? En past de tool binnen je IT-strategie? Sommige tools zijn alleen in cloud-vorm beschikbaar; andere bestaan in versies voor zowel on-premise als cloud.

Concluderend: de beveiliging van je SAP-systeem moet je aanvliegen vanuit een blueprint, een beveiligingsplan dat alle aspecten van het systeem omvat. Zorg ervoor dat je die blueprint regelmatig tegen het licht houdt! Door het plan regelmatig te reviewen en te updaten, zorg je ervoor dat je organisatie beschermd is en blijft tegen de dreigingen van vandaag en morgen.

Over de auteurs:

Ali Cifci

Ali Cifci is een SAP Basis & Security consultant met meer dan 15 jaar ervaring. Hij heeft gewerkt aan verschillende SAP-migraties en -implementaties. Vanuit inzicht in regelgeving over data- en privacybescherming, analyseert hij SAP-systemen en adviseert hij organisaties over de potentiële risico's en de maatregelen om die risico's te beheersen.

Mail: ali.cifci@capgemini.com

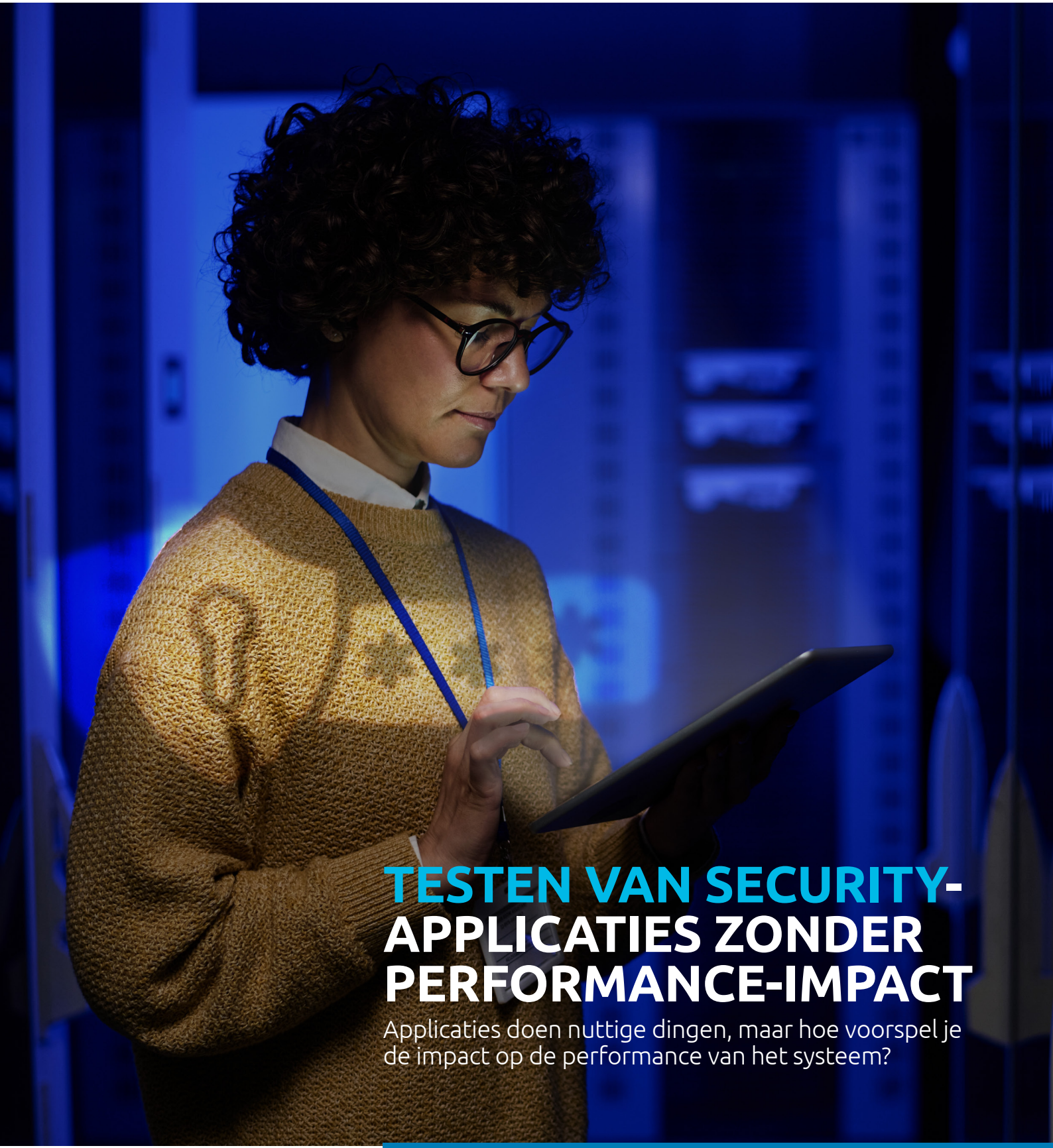
LinkedIn: https://www.linkedin.com/in/cifci/

Ankit Arya

Ankit is een SAP Security and GRC consultant, met 10 jaar ervaring en verschillende rollen. Zijn specialisaties zijn Audit, Risk en Compliance Management. Ankit ontwerpt en implementeert end-to-end, business-georiënteerde beveiligingsmodellen voor SAP ERP-producten. Uiteraard altijd compliant met alle audit-vereisten.

Mail: ankit.arya@capgemini.com

LinkedIn: https://www.linkedin.com/in/ankitarya1103/



TESTEN VAN SECURITY-APPLICATIES ZONDER PERFORMANCE-IMPACT

Applicaties doen nuttige dingen, maar hoe voorspel je de impact op de performance van het systeem?

Highlights

- Performance testing moet worden overwogen voordat een product gekozen wordt.
- Systeem impact omvat naast CPU, RAM en Storage ook configuratie.
- Alle scenario's testen is onrealistisch, system testing biedt hier mogelijkheden.
- Er zijn strategieën op Performance Optimization of Resource Utilization.
- Niet elke applicatie gaat elke test doorstaan.

De beveiligingsoplossingen liggen voor het oprapen. Deze oplossingen brengen ook nog eens vele voordelen met zich mee. Helaas komen voordelen niet gratis, er is altijd een prijs, en deze prijs is niet alleen in euro's uit te drukken.

Wanneer we overwegen om een applicatie wel of niet te installeren wordt er vaak nagedacht over functionaliteit en financiële kosten. Belangrijke overwegingen, maar vaak onvolledig. De introductie van een nieuwe applicatie heeft immers ook gevolgen op het werking van de computersysteem als geheel.

Dit is extra waar wanneer het over beveiligingssoftware gaat. Neem als voorbeeld de virusscanner die, wanneer nodig, de hoofdprocessor (ook wel CPU) gebruikt om het systeem te scannen. Met als gevolg dat er geen CPU-kracht meer over is om de e-mail van de gebruiker te laden.

We zoeken dus naar een balans tussen de veiligheid en de bruikbaarheid van het systeem.

Drie systeemeigenschappen die je moet overwegen

Wanneer we spreken over een bruikbaar systeem, proberen we drie primaire systeemeigenschappen in harmonie te houden. De eerdergenoemde CPU, het geheugen (ook wel RAM) en de opslagruimte (ook wel Disk Space). Deze eigenschappen kunnen we samenvatten in de categorie 'system resources'.

Er bestaat echter een vierde eigenschap die vaak pas overwogen wordt als er problemen zijn, configuratie. Wanneer diverse applicaties dezelfde system resources aanspreken, kan ook interactie ontstaan tussen de handelingen van applicaties. Denk bijvoorbeeld aan een applicatie die gebruik maakt van de logging van het systeem zelf. Applicatie A wil mogelijk een ander log level dan applicatie B.

Effectief of efficiënt omgaan met systemresources

Ervaren systeembeheerders zullen vragen stellen over piekbelasting van de applicatie. Dit is het punt waar het lastig begint te worden. Een applicatie is niet altijd dezelfde handelingen aan het verrichten of dezelfde system resources aan het gebruiken. De virusscanner die niets te doen heeft, gebruikt minder resources dan de virusscanner die actief virussen aan het opruimen is.

De twee meest gehanteerde strategieën hierin zijn; Peak Performance Optimization (PPO), en Peak Resource Utilization (PRU). Bij PPO is het streven om een zo effectief mogelijk draaiend systeem te realiseren. Hierbij willen we dat applicaties altijd in staat zijn hun primaire taak uit te voeren met minimale resource problemen. Maar bij PRU streven we naar een zo efficiënt mogelijk draaiend systeem. Waarbij we een zo hoog mogelijk gebruik willen van onze system resources bij het uitvoeren van de primaire taak.

Uiteraard zijn hier veel nuances in te vinden, maar beide strategieën hebben aan de grondslag dezelfde vraag "Hoeveel resources gebruikt die applicatie?"

Natuurlijk kunnen we bij een PPO-strategie zeggen dat we gewoon meer system resources toevoegen, maar een goede onderbouwing hiervoor is belangrijk. Anders investeert men geld in de oplossing, zonder de zekerheid dat het probleem wordt opgelost.

Zeven verschillende tests om impact te voorspellen

Meten is weten, maar meten is lastig. We hebben drie systeem resources die zullen fluctueren tijdens het gebruik van de applicatie. Daarnaast worden deze beïnvloed door de configuratieverschillen op het systeem. Dat zijn behoorlijk wat variabelen die invloed op elkaar hebben.

In plaats van elk mogelijk scenario proberen te meten en in een tabelletje te zetten, gebruiken wij zogenoemde 'system testing' methodieken. Bij system testing wordt het systeem als geheel getest, in tegenstelling to unit testing waarbij losse componenten van een system getest worden.

De ontwikkelaar van de applicatie heeft waarschijnlijk al tests uitgevoerd op generieke scenario's. Maar dit betekent niet dat de applicatie op elk systeem dezelfde resultaten zal hebben, aangezien configuratieverschillen een aanzienlijke impact kunnen hebben.

Tabel 1 geeft een overzicht wat je van de ontwikkelaar mag verwachten en welke tests je zelf zou moeten overwegen.

Een goede test heeft scherp gedefinieerde acceptatiecriteria

Het bepalen of de resultaten van een test goed of slecht zijn moet gedaan worden met scherp gedefinieerde acceptatiecriteria. Criteria die voorafgaande aan de test worden vastgelegd in lijn met de gekozen strategie voor PPO of PRU.

Acceptatiecriteria worden vaak gedocumenteerd als "what to test", het test scenario, in combinatie met "expected results", de verwachte uitkomst van de test. Hierbij is het van belang zo precies mogelijk te zijn in het beschrijven wat de verwachtingen zijn. Wanneer we deze zaken hebben gedefinieerd kunnen we nadenken over welke test data we nodig hebben om dit te meten.

Omdat dit wel erg abstract begint te worden gebruiken we in tabel 2 een voorbeeld van 'Performance Testing'. Hierbij kijken we weer naar de virusscanner. Specifiek bij het uitvoeren van een virusscan op een laptop.

Nu is al snel duidelijk wat de vervolg stappen zijn. We pakken een laptop om te testen, installeren de applicatie en kijken naar de resultaten. Tot slot vullen we de testresultaten en beoordeling in, zie als voorbeeld tabel 3.

SOFTWARE TEST TYPE	OMSCHRIJVING	DOOR ONTWIKKELAAR	TER OVERWEGING
Functionality Testing	Ter bevestiging dat de functionaliteit van de applicatie naar behoren werkt		
Recoverability Testing	Ter bevestiging dat de applicatie om kan gaan met foutieve input zonder te breken		
Interoperability Testing	Ter bevestiging dat de applicatie met andere applicaties samen kan functioneren		
Performance Testing	Ter bevestiging dat de applicatie binnen bepaalde scenario's binnen de bandbreedte van de system resources blijft		
Regression Testing	Ter bevestiging dat de applicatie met alle bijbehorende sub-systemen naar behoren functioneert		
Usability Testing	Ter bevestiging dat gebruikers en/of systemen correct gebruik kunnen maken van de applicatie		
Migration Testing	Ter bevestiging dat de applicatie verhuist kan worden naar een nieuw systeem of infrastructuur zonder problemen		

Tabel 1: Wie test wat?

Test Case ID	Test Naam	What to Test	Expected Results	Test Data	Actual Results	Pass/ Fail
001	CPU gebruik tijdens virus scan	De totale CPU Consumptie van de virusscanner tijdens het verrichten van een virusscan op een laptop	20% CPU Consumptie door de virusscanner	CPU Consumptie van alle processen op de laptop		

Tabel 2: Voorbeeld van 'Performance Testing'

Test Case ID	Test Naam	What to Test	Expected Results	Test Data	Actual Results	Pass/Fail
001	CPU gebruik tijdens virus scan	De totale CPU consumptie van de virusscanner tijdens het verrichten van een virusscan op een laptop	20% CPU consumptie door de virusscanner	CPU consumptie van alle processen op de laptop	15% CPU consumptie door de virusscanner	Pass, 15% is lager dan de verwachte 20%

Tabel 3: Testresultaten en beoordeling

De beste acceptatiecriteria zijn de meest realistische

We kunnen natuurlijk duizend test cases opstellen in een poging alles af te vangen, maar in de praktijk zien we dat er een handje vol test cases zijn die altijd relevant zijn. Test cases die gericht zijn op de eerdergenoemde primaire systeemeigenschappen.

- Hebben we genoeg CPU?
- Hebben we genoeg RAM?
- Hebben we genoeg Disk pace?

Nu zijn ontwikkelaars ook niet gek en menig commercieel product zal deze informatie al beschikbaar hebben. Wanneer zij het hebben over "minimum system requirements" bevat dit gemiddelde system resource consumptie, mogelijk hebben ze ook nog een "recommended system requirements" die meer rekening houden met piekbelastingen. Je hoeft dan alleen nog rekening te houden met hoe jouw situatie afwijkt van de norm. Denk hierbij aan applicaties en systemen die je zelf heeft ontwikkeld en niet publiekelijk beschikbaar zijn.

Tot slot moet je nog rekening houden met configuraties. Ook hier zal de ontwikkelaar vaak specificaties aanleveren op basis van de test resultaten. De meest voorkomende configuratie eisen zijn met betrekking tot virusscanners en firewalls rond de applicatie.

Soms is het antwoord gewoon nee

We zien vaak dat testen pas ter sprake komt nadat er een product gekozen is. Het is ook onrealistisch om een volledige test te vragen van alle mogelijke producten. Het is zeker mogelijk om vooraf succes te bepalen. Hierbij kun je denken aan het vooraf vaststellen van de verwachtingen voor usability- en interoperabiliteitstests. Daarnaast kan zelfs een eenvoudige smoke test in een testomgeving van grote waarde zijn.

Aan het einde van de dag ontkom je er ook niet aan; soms werkt een applicatie gewoon niet binnen de bestaande omgeving. Dan moet je ook 'nee' durven zeggen en op zoek gaan naar een ander product. Maar als we dat doen, laten we dan wel voor een bijpassend test plan kiezen.

Over de auteurs:

Sebastiaan de Vries

Sebastiaan de Vries is een ervaren Security expert die naast zijn technische kennis ook op de hoogte is van de laatse compliance standaarden. Hij houdt zich bezig met het helpen van klanten door security te veranderen van een noodzaak naar een voordeel.

Mail: sebastiaan.de.vries@capgemini.com

LinkedIn: https://www.linkedin.com/in/gsdevries/

Dennis van de Water

Dennis is een veelzijdige Cybersecurity Consultant bij Capgemini. Hij heeft uitgebreide ervaring met het opzetten en ontwerpen van cybersecurity-oplossingen, advies geven op het gebied van EDR-tooling cybercrisismanagement, en cybercrisis-simulaties.

Mail: dennis.vande.water@capgemini.com

LinkedIn: https://www.linkedin.com/in/dennis-van-de-water/

Jeroen van Hulst

Jeroen is een zeer technische cybersecurity specialist die IT en strategie combineert. Met zijn achtergrond in zowel IT als OT R&D heeft hij een breed scala aan projecten beheerd, van het ontwikkelen van oplossingen voor kwetsbaarheidsbeheer voor overheidsorganisaties tot het opzetten van een bedrijfscloudomgeving voor het leveren van beveiligingsdiensten aan meerdere klanten over de hele wereld.

Mail: jeroen.van.hulst@capgemini.com

LinkedIn: https://www.linkedin.com/in/jeroen-van-hulst-aa863b97/

Laura Adelaar

Laura is een cybersecurity consultant met een affiniteit voor beveiligingsopties met AI. Met een achtergrond in Communicatie en kennis van datacenters brengt Laura een diverse visie.

Mail: laura.adelaar@capgemini.com

LinkedIn: https://nl.linkedin.com/in/laura-adelaar-38728758/

Publicaties

Naast het Trends in Cybersecurity rapport publiceren we ook andere rapporten, studies en whitepapers die mogelijk relevant voor je kunnen zijn. Hieronder vind je een beknopt overzicht. Het volledige overzicht is te vinden op *http://www.capgemini.nl*.

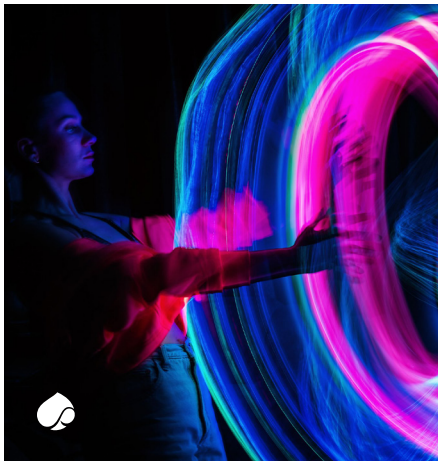
Trends in Cybersecurity 2022 – Secure an accelerated digital transformation

Cybersecurity is een vereiste binnen ieder bedrijf, biedt een veilige basis voor transformatie en ondersteunt alle werkzaamheden. Hoe zorg je voor overzicht en controle over jouw cyber risk programma? Hoe snel kun je terug naar je dagelijkse werkzaamheden wanneer cybercriminaliteit jouw organisatie raakt? En heeft jouw organisatie een schaalbare aanpak als het gaat om IT-beveiliging?

Waarom we het over Zero Trust moeten hebben

Zero trust is here to stay. Zero trust-concepten beginnen zelfs een plek te krijgen in nieuwe regelgeving. Het is dus duidelijk veel meer dan een modegril.

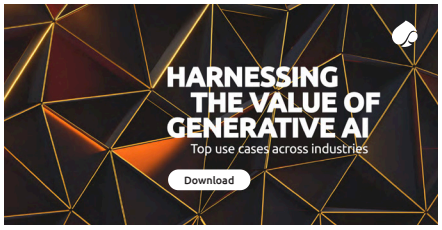
De naam 'zero trust security' zegt het precies: als het gaat om cybersecurity kun je niets of niemand vertrouwen. Elke gebruiker wordt gewantrouwd, totdat het tegendeel is bewezen. Dat klinkt niet zo vriendelijk, maar deze benadering zorgt er juist voor dat mensen veilig kunnen blijven (samen) werken, waar of wanneer ze dat ook willen. Door zero trust te adopteren, verleggen organisaties hun primaire focus naar de beveiliging van informatie op alle platforms. Daarom is het tijd om het over zero trust te hebben, hoog tijd.



Transformation Essentials

Digitale transformatie is essentieel voor een bedrijf om te blijven bestaan en zich te onderscheiden van de concurrentie. Maar hoe doe je dat? Welke ‘Transformation Essentials’ zijn voorwaarden voor succes?

Laat je inspireren door te lezen, luisteren en kijken naar praktijkvoorbeelden van organisaties in transitie op het gebied van technologie, bedrijfscultuur en processen. Elk met hun eigen uitdagingen, in hun eigen tempo, maar wel met hetzelfde doel: grip op morgen.



Generatieve AI in organisaties

70% van de leidinggevenden denkt dat generatieve AI meer reikwijdte geeft aan de kenniswerkers in hun bedrijf. Bijna alle bestuurders (96%) erkennen dat generatieve AI een belangrijk onderwerp voor hun organisatie is. Dit blijkt uit het nieuwste rapport van het Capgemini Research Institute, ‘Harnessing the value of generative AI: Top use cases across industries’ waarin de transformatieve kracht van generatieve AI voor innovatie binnen ondernemingen wordt onderzocht.

Colofon:

Dit rapport is in samenwerking opgesteld met bijdragen van Bart van Riel, Martijn Gardenier, Natasja Pieterman, Anton Enkelaar, Marieke van de Putte, Hans Marcus, Serge Dujardin, Folkert Visser, Werner Branje, Mohit Sikka, Giselle van Wissen, Storm Poot en Thomas de Klerk.

Advies, ontwerp en productie werden verzorgd door Johanna Achterberg en Arindam Dey van het Marketing & Communicatie team Capgemini Nederland B.V.

Over Capgemini

Capgemini is een wereldwijde, maatschappelijk verantwoorde en multiculturele marktleider met 360,000 mensen in bijna 50 landen. Als strategisch partner ondersteunt Capgemini organisaties bij hun transformatie door gebruik te maken van de kracht van technologie. Hierbij laat de Group zich leiden door zijn bestaansreden: menselijke energie vrijmaken door middel van technologie voor een inclusieve en duurzame toekomst. Met meer dan 50 jaar ervaring en expertise in uiteenlopende sectoren, vertrouwen klanten de aanpak van hun zakelijke behoeften toe aan Capgemini: van strategie en ontwerp tot operationeel beheer. Dit gebeurt door gebruik te maken van innovaties in cloud, data, kunstmatige intelligentie, connectiviteit, software, digital engineering en platforms. De Group behaalde in 2022 een omzet van € 22 miljard.

GET THE FUTURE YOU WANT | www.capgemini.nl

Capgemini Nederland B.V.
Postbus 2575 - 3500 GN Utrecht
Tel. + 31 30 203 05 00
www.capgemini.nl

2D-008.23