TESORION

© 2024, Tesorion Nederland BV



Juni - 2024

Word de baas over je aanvalsoppervlak!

Grip en zicht op alle kwetsbare plekken in je software, hardware, netwerk en fysieke infrastructuur.

Classificatie: publiek

Auteur: **Tesorion Nederland BV**

Auteur: **Tesorion Nederland B.V.**
Titel: Word de baas over je aanvalsoppervlakte
Classificatie: publiek
Datum: Q2 2024
Versie: Versie 1

© 2024, Tesorion Nederland BV
Uitgegeven in eigen beheer
contact@tesorion.com

Vormgeving door: Graphic Lab
Fotografie door: Adobe Firefly (AI)
prompter: Graphic Lab

Alle rechten voorbehouden.
Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand en/of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op enige andere manier zonder

Inhoud

1. Inleiding 6
Groeiend aanvalsoppervlak 6
Kwetsbaar aanvalsoppervlak 6

2. Het aanvalsoppervlak in kaart 8
2.1 Known Knowns 8
2.1.1 Endpoint security is onmisbaar 8
2.1.2 API's blijken kwetsbaar 9
Houd zicht op API's 9
Risico's API onderschat 10
2.1.3 Grip op assets 10

2.2 Known unknowns 10
2.2.1 De risico's die schuilen acher ketenparners 12
Impact op fysiek, technologie en mens 12
Weet met wie je samenwerkt 12
Gebruik NIS2 als referentie 12
2.2.2 Weet wie er toegang heeft tot je IT-landschap 13
Altijd weer dat wachtwoord 13
PAM beperkt aanvalsoppervlak 13
2.2.3 Vulnerability- en patchmanagement 13
Patchen, zo snel mogelijk – indien mogelijk 15
2.2.4 Grip op unmanaged devices 15
Belangrijke maatregelen 15
Voordelen van effectief beheer 15
2.2.5 Denken als een cybercrimineel 15

2.3 Unknown unknowns 16
2.3.1 Open Source Intelligence 16
Schadelijk of onschadelijk? 16
Vind de balans in OSINT 18
2.3.2 Je digitale merk onder vuur 18
Kwetsbaarheden identificeren 18
Monitoring en detectie automatiseren 19

3. Conclusie 21

1. Inleiding

Het digitale aanvalsoppervlak, ook wel bekend als attack surface, heeft zich in het afgelopen decennium razendsnel ontwikkeld. Dit aanvalsoppervlak kun je zien als het geheel van alle mogelijke punten waar een ongeautoriseerde gebruiker (de aanvaller) je systemen kan proberen binnen te dringen of gegevens kan onttrekken.

Met andere woorden, het gaat om alle kwetsbare plekken in je software, hardware, netwerk en fysieke infrastructuur die kunnen worden uitgebuit door cybercriminelen. Het ligt voor de hand technologie als grootste boosdoener aan te wijzen, maar ook de fysieke omgeving en de mens kunnen als aanvalsvector uitgebuit worden. Grofweg kun je dus zeggen dat het aanvalsoppervlak bestaat uit 3 elementen:

- **Technologie**, het patchen van kwetsbaarheden en voorkomen van configuratiefouten.
- **Fysiek**, hoe is de fysieke toegang geregeld? Zijn er poortjes of wordt er met badges gewerkt?
- **De mens**, hier draait het om gedrag en cyberbewustzijn.

Worden elementen als technologie en mens met elkaar gecombineerd, dan hebben we het bijvoorbeeld over phishing.

Kijken we naar de elementen fysiek en mens, dan hebben we het over het meelopen met iemand, zonder je te identificeren.

Kijken we tenslotte naar de combinatie tussen fysiek en technologie, dan hebben we het over het ongeoorloofd toegang forceren tot het (W)LAN.

Groeiend aanvalsoppervlak

Het aanvalsoppervlak van een organisatie bestond nog niet eens zo lang geleden voornamelijk uit de computers van medewerkers en servers binnen het kantoornetwerk. Wellicht met een uitwijkmogelijkheid op een andere locatie. De opkomst van nieuwe technologieën en werkmethoden heeft het aanvalsoppervlak drastisch veranderd. Ontwikkelingen zoals thuiswerken, Bring Your Own Device (BYOD), Internet of Things (IoT), cloudadoptie, ketenintegratie en de populariteit van social media hebben ervoor gezorgd dat het aanvalsoppervlak snel fors is uitgebreid. En dat niet alleen; het verandert ook voortdurend. Je hebt te maken met een dynamisch aanvalsoppervlak. Je werkt samen met nieuwe partners, opent nieuwe handels- of communicatiekanalen en neemt steeds meer flexibel personeel aan.

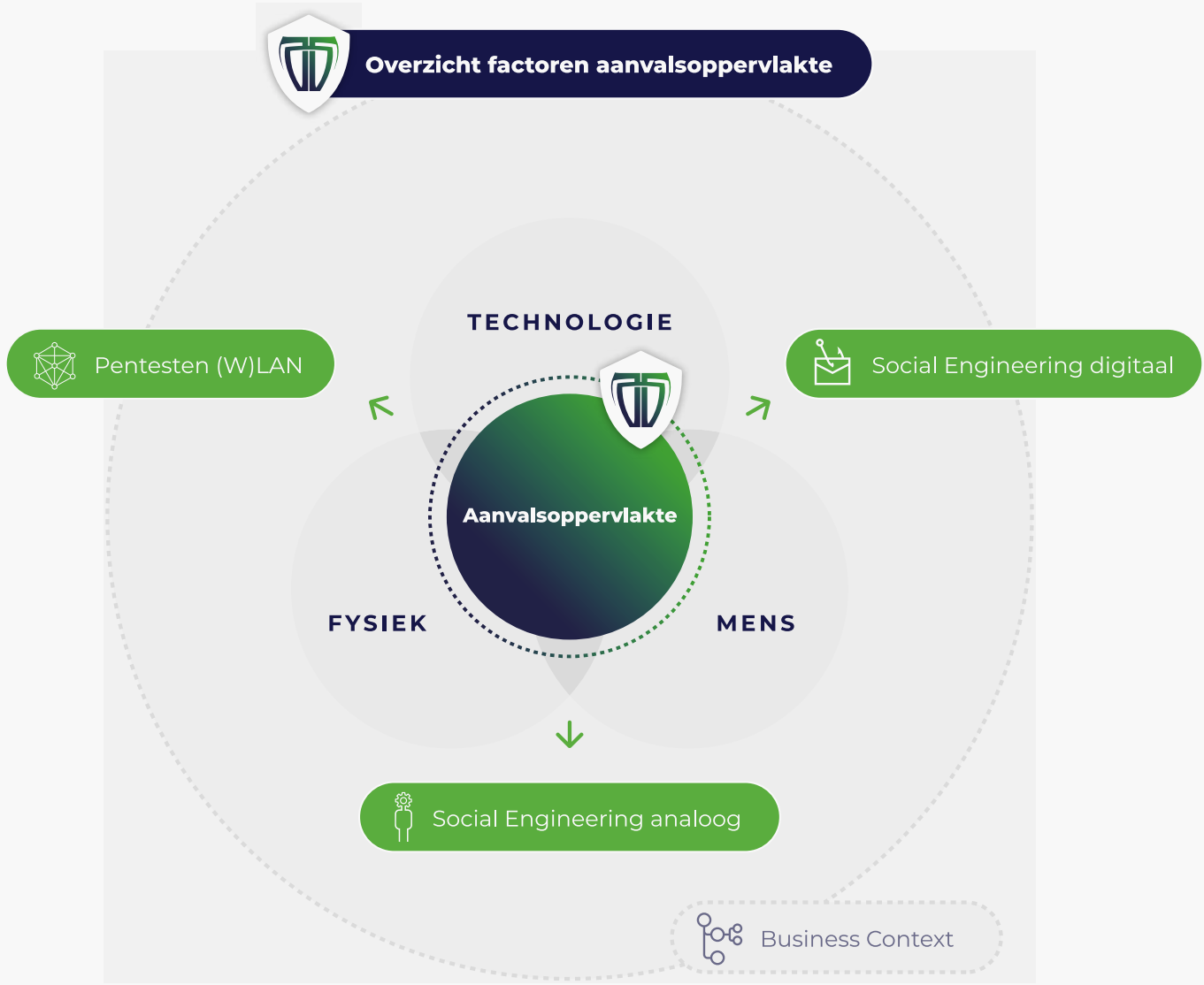
Laten we duidelijk zijn, de ontwikkelingen die ervoor zorgen dat het aanvalsoppervlak groeit, leveren organisaties veel voordelen op. Een aantal voorbeelden:

- Processen kunnen in hoge mate gedigitaliseerd en geautomatiseerd worden.
- Samenwerking met partners in de waardeketen wordt eenvoudiger.
- Medewerkers kunnen waar en wanneer dan ook hun werk doen.
- We verzamelen op steeds meer plekken data die we realtime beschikbaar willen hebben. Denk hierbij aan sensoren in machines of aan het loggen van data over het bezoekgedrag op e-commerce platforms.

Kwetsbaar aanvalsoppervlak

Deze ontwikkelingen hebben dus een keerzijde. Zo leidt de uitbreiding van het aanvalsoppervlak tot kwetsbaarheden in de infrastructuur. De uitdagingen op het gebied van security zijn ook complexer geworden. Het overzicht houden over welke assets kwetsbaar zijn, en weten welke maatregelen genomen moeten worden om de organisatie veilig te houden, is nu een continu proces. Bovendien moeten organisaties rekening houden met relevante wet- en regelgeving, en hoe zij aan deze eisen kunnen voldoen.

Dit vereist een andere benadering van cybersecurity. In het verleden waren maatregelen zoals firewalls, antivirussoftware en het regelmatig installeren van patches vaak voldoende. Tegenwoordig, met het uitdijende aanvalsoppervlak, is er een meer omvattende cyberstrategie nodig. Zeker wanneer



je weet dat cybercriminelen geavanceerdere aanvalsmethodes hebben ontwikkeld en blijven ontwikkelen. Deze strategie omvat onder andere uitgebreidere beveiligingstechnologieën, voortdurende monitoring en dynamische responsstrategieën. Ook een SOC (Security Operations Center) speelt hier een belangrijke rol in het veilig houden van een organisatie.

De vraag voor elke organisatie is nu: hoe zorg je ervoor dat je grip krijgt op jouw aanvalsoppervlak? En hoe bepaal je welke maatregelen noodzakelijk zijn om security te waarborgen en te blijven voldoen aan de wettelijke vereisten? En hoe voldoe je daarmee aan wetgeving zoals NIS2, die binnen afzienbare tijd in Nederland als aanpassing van de Wet beveiliging netwerk- en informatiesystemen (Wbni) geïmplementeerd zal worden? Deze vragen zijn essentieel om een effectieve beveiligingsstrategie te ontwikkelen en te onderhouden. Een strategie die meebeweegt met je organisatie en met het ecosysteem waarin je je bevindt.

In deze visiepaper bieden wij antwoorden op deze vragen en handvatten om te zorgen dat jouw organisatie voorbereid is op actuele dreigingen, nu en in de toekomst. Weet hierbij dat aanvallers aan één zwakke plek in het aanvalsoppervlak genoeg hebben om binnen te dringen – terwijl jij als organisatie het gehele oppervlak moet zien te verdedigen. In de wetenschap dat de dynamiek en omvang van het aanvalsoppervlak eerder zullen toenemen dan afnemen, moet je het inzicht vergroten om vervolgens de regie te nemen. Word de baas over je aanvalsoppervlak!

2. Het aanvalsoppervlak in kaart

Kom te weten wat je niet weet én wat je moet doen

In het streven je aanvalsoppervlak in kaart te brengen en de risico's (de kans op een incident vermenigvuldigd met de impact van een incident) te benoemen, moeten we ons realiseren dat er zaken zijn die we weten, maar ook die we niet weten. Donald Rumsfeld, voormalig minister van Defensie in het kabinet van president George W. Bush, formuleerde dit in 2002 treffend. In een militaire context zei hij:

> *"There are **known knowns**; there are things we know we know. We also know there are **known unknowns**; that is to say we know there are some things we do not know. But there are also **unknown unknowns** - the ones we don't know we don't know."*

Deze uitspraak van Rumsfeld is evengoed van toepassing op cybersecurity en het aanvalsoppervlak. Er zijn legio aanvalsvectoren: Van de meest voor de hand liggende tot misschien onverwacht. Van de 'known knowns' tot de 'unknown unknowns'. In deze paper lichten we er een aantal uit.

HET 4E ELEMENT: TIJD

Het is belangrijk je te realiseren dat kennis in de loop van de tijd veroudert. Doe je niets, dan is de kennis die je vandaag hebt over een tijdje minder tot niets meer waard. Het vergt dus een constante inspanning om te zorgen dat 'unknown unknowns' veranderen in 'known unknowns' en uiteindelijk 'known knowns' worden. Kom in actie door steeds meer kennis te verzamelen over je aanvalsoppervlakte. In de volgende hoofdstukken bespreken we daarom een aantal verschillende componenten van het aanvalsoppervlak. Het is namelijk essentieel dat je zorgt dat je bekend wordt met jouw 'unknown unknowns' zodat ze 'known knowns' kunnen worden.

2.1 KNOWN KNOWNS

In cybersecurity zijn 'known knowns' de dreigingen en kwetsbaarheden waarvan we ons bewust zijn en die we begrijpen. Denk hierbij aan bekende kwetsbaarheden in software en hardware waarvoor patches en fixes beschikbaar zijn. Hieronder verstaan we ook gedocumenteerde aanvalsmethoden die vaak voorkomen en waarvoor verdedigingsmechanismen bestaan. Deze categorie dreigingen is voor securityteams doorgaans goed te beheersen. Kom maar op, is het devies. Dat we deze dreigingen door en door kennen, sluit niet uit dat organisaties hierdoor verrast worden. *Begin 2024 werd bekend dat een computersysteem van het ministerie van Defensie slachtoffer was geworden van een cyberaanval.* Aanvallers verschaften zich toegang via een kwetsbaarheid die al in december 2022 door de leverancier bekend was gemaakt. Een patch was dus al lang beschikbaar.

Kijken we naar het groeiende aanvalsoppervlak, dan zijn er verschillende componenten die we kunnen scharen onder de categorie known knowns. We beschrijven hieronder kwetsbaarheden die bekend zouden moeten zijn en waarvan de impact ook duidelijk zou moeten zijn. Helaas is die impact niet altijd voor iedereen vooraf duidelijk, de reden voor deze voorzichtige formulering. Voor ons een extra reden om dit te benadrukken, zodat je de kwetsbaarheden van je eigen aanvalsoppervlak in kaart kunt brengen en kunt mitigeren. In de volgende hoofdstukken beschrijven we een aantal aspecten van het aanvalsoppervlak die we onder de categorie 'known knowns' scharen.

2.1.1 Endpoint security is onmisbaar

De meest voor de hand liggende aanvalsvector is het endpoint. Elke organisatie heeft te maken met endpoints. Een endpoint is in deze context elk apparaat waar de communicatie begint, wordt ontvangen en eindigt. Dat betekent dat een organisatie een enorme hoeveelheid endpoints kan omvatten. Deze hoeven bovendien niet allemaal in beheer te zijn van de organisatie. Deze apparaten kunnen verbonden zijn via:

- Een lokaal intranet
- Cloud-SaaS-platforms
- Het openbare internet

Bron: https://www.independent.co.uk/tv/news/revisiting-donald-rumsfelds-infamous-known-unknowns-quote-b21799715.html
Bron: https://www.security.nl/posting/828347/Militaire+inlichtingendienst+vindt+malware+op+FortiGate-apparaten+Defensie

Misschien gebruik je Single Sign On (SSO) en pas je een Zero Trust Architecture (ZTA) toe. Wellicht verplaats je jouw gegevens binnenkort naar een publieke, on-premise of hybride cloud, waarbij endpoints vanuit meerdere locaties wereldwijd verbinding maken met jouw netwerk. Of misschien heb je dat zelfs al gedaan. Door deze ontwikkeling is een endpoint een gewild startpunt voor een cybercrimimeel. Daarnaast is door het groeiend aantal endpoints ook het aanvalsoppervlak oneindig veel groter geworden. Kortom, de situatie is nu veel complexer dan ongeveer tien jaar geleden, waardoor ook de vereisten waaraan een Endpoint Detection & Response (EDR) -oplossing moet voldoen, veranderen.

Het beheren van grote hoeveelheden apparaten en data is geen eenvoudige taak. Voeg daar afgelegen geografische locaties, verschillende tijdzones en soms zelfs taalbarrières aan toe en je hebt een complexiteit die vraagt om flexibiliteit van leveranciers.

Voor het beheren, reageren op en verzamelen van gegevens van jouw wereldwijde locaties, heb je een oplossing nodig die multi-tenancy en multi-sites ondersteunt. Dit stelt lokale teams in staat om taken van het hoofdbeleid over te nemen en lokaal te beheren waar dat logisch is, zonder de behoeften van anderen in de organisatie in gevaar te brengen.

Bij een omvangrijke organisatie met meerdere locaties en sub-netwerken is een effectieve oplossing noodzakelijk om het netwerk in kaart te brengen. Dit kan worden gedaan door fingerprinting van apparaten. Dit is een techniek die wordt gebruikt om individuele apparaten binnen een netwerk te identificeren en te profileren op basis van unieke kenmerken. Deze kenmerken kunnen hardware- en software-attributen omvatten, zoals MAC- en IP-adres, besturingssysteem en geïnstalleerde software. Zo kun je niet alleen bepalen wat verbonden is, maar ook wat onbeveiligd is.

Met deze kennis heb je een beveiligingsoplossing nodig die het zware werk kan doen, zoals het inzetten van agents om gaten in de dekking te dichten of bijvoorbeeld een NDR-oplossing om inzicht te krijgen in de datastromen tussen de verschillende assets. Securityteams hebben het vaak te druk en hebben slimme automatisering nodig om hun werk effectiever te doen en het aanvalsoppervlak van de organisatie te beheersen, of liever nog, te verkleinen. Mocht dit voor een securityteam te veel worden, dan is een andere optie om gebruik te maken van een extern SOC.

2.1.2 API's blijken kwetsbaar

Een tweede, wellicht minder voor de hand liggende aanvalsvector, zijn API's. Met de opkomst van webapplicaties is de rol van application programming interfaces (API's) belangrijker geworden. De API is de schakel tussen de front- en de backoffice en tussen applicaties onderling. Het zorgt ervoor dat medewerkers efficiënt kunnen werken en dat transacties met klanten online soepel verlopen. Met de toename van het aantal applicaties is ook het aantal API's fors toegenomen. *Grofweg tachtig procent van het webverkeer is API-gerelateerd, en daarmee is direct duidelijk wat de impact is op het digitale aanvalsoppervlak.* Doorgaans zitten in de API securitywaarborgen ingebakken. Zo wordt de gebruiker van de API gecheckt: wie ben jij (authenticatie) en wat mag jij (autorisatie)? De praktijk leert echter dat API's kwetsbaar zijn en dat cyberaanvallers deze achilleshiel in het aanvalsoppervlak weten te benutten.

Houd zicht op API's

API's zijn echter onmisbaar en dus is het noodzakelijk de security te versterken. Dit begint met het detecteren van kwetsbaarheden. Een veelvoorkomende fout bij API's betreft de BOLA (Broken Object Level Authorization). Bij deze beveiligingskwetsbaarheid voert een applicatie onvoldoende autorisatiecontroles uit voor toegang tot specifieke objecten. Hierdoor kan een gebruiker toegang krijgen tot gegevens of functionaliteiten die voor anderen bedoeld zijn. BOLA-fouten ontstaan wanneer de applicatie niet controleert of een gebruiker bevoegd is om toegang te krijgen tot een specifiek object. Wellicht is dit het gevolg van de snelle toename van het aantal webapplicaties en API's in een organisatie. Feit is dat veel organisaties überhaupt niet goed weten hoeveel API's zij hebben en het ontbreekt daarbij vaak ook nog eens aan de juiste en volledige documentatie. Dit maakt het lastig de API's te beheren. Bovendien bestaat het risico dat er een lek ontstaat, bijvoorbeeld wanneer er wijzigingen plaatsvinden in de programmatuur.

Bron: https://apicontext.com/why-apis-are-eating-the-world-wide-web/

Bij zo'n driekwart van de cyberaanvallen die via een webapplicatie verlopen, ligt het probleem bij de API. Werk aan je API's, zou je zeggen, dan wordt je aanvalsoppervlak een stuk steviger. Om API's veiliger te maken, is het in de eerste plaats van belang dat je ze in kaart brengt:

- Hoeveel API's heb je nu eigenlijk?
- Wat is het kenmerk van de API's, qua omvang en bereik? Zitten er bijvoorbeeld al bestaande kwetsbaarheden in?
- Wat voor soort vragen stuur je richting de API? Welke klanten hebben of krijgen toegang en welke applicatie wil je ermee ontsluiten?

Risico's API onderschat
Heb je een beeld van je API- landschap, dan kun je vervolgens de baseline in kaart brengen. Als je bepaald gedrag en bepaald verkeer hebt, weet je wat de afwijkingen zijn en kun je handelend optreden. Zou bouw je aan een stevige posture van je API. Werk tegelijkertijd aan een Swagger, een open-source framework dat wordt gebruikt voor het ontwerpen, bouwen en documenteren van webservices. Het maakt deel uit van de OpenAPI Initiative, die de OpenAPI Specification (OAS) beheert. In termen van security, biedt Swagger verschillende voordelen:

- Duidelijke documentatie, die je ook kunt delen met ketenpartners
- Beveiligingsdefinities voor authenticatie en autorisatie
- Consistente implementatie
- Geautomatiseerd testen
- Snellere detectie van kwetsbaarheden

De risico's rond API's worden onderschat. Je denkt achter een firewall veilig te zijn, maar een aanvaller kan ook al binnen zijn en vervolgens zijn weg zoeken naar meer waardevolle informatie. Daar komt bij: een firewall controleert de autorisatie niet. Misbruik van privileges ligt dan ook altijd op de loer. Maak dus werk van je API-beheer.

2.1.3 GRIP OP ASSETS

Wanneer je het aanvalsoppervlak van een organisatie in kaart brengt, blijkt al snel dat het om een enorme hoeveelheid assets gaat. Dit betekent dat er prioriteiten gesteld moeten worden op basis van een inschatting van alle mogelijke risico's voor hun omgeving en hoe deze risico's kritieke bedrijfsapplicaties en -processen kunnen beïnvloeden.

De huidige fragmentatie van IT-beheer, DevOps en beveiligingstools maakt het moeilijk om alle activa in het bedrijf te zien en de onderlinge relaties te begrijpen. De telemetrie van endpoints en cloud-omgevingen is een essentieel onderdeel om in te schatten hoe het aanvalsoppervlak eruitziet. Om deze inzichten te benutten, moet al deze informatie worden gecorreleerd met data die over het algemeen wordt verzameld in allerlei verschillende tools in de bedrijfsomgeving. Op deze manier kunnen teams een veel beter begrip krijgen van zowel de context als de cyberbeveiligingsrelatie tussen alle gerelateerde activa in de organisatie.

Het is één ding om te ontdekken dat een endpoint een kritieke misconfiguratie heeft. Het is een heel ander verhaal wanneer je ontdekt dat dit endpoint zich op een productienetwerk bevindt, met toegang tot een zeer gevoelige dataset. En dat het een cruciaal onderdeel is ter ondersteuning van een belangrijke bedrijfstoepassing.

2.2 KNOWN UNKNOWNS

Naast de eerder besproken 'known knowns' kennen we ook 'known unknowns'. Bekende onbekende informatie (dingen waarvan we weten dat we ze niet weten) kunnen we zien als potentiële kwetsbaarheden in systemen die bekend zijn maar waarvan de impact of het exacte exploitatiemechanisme onbekend is. Denk hierbij aan zero day kwetsbaarheden; als securityteam weet je dat ze bestaan of zullen komen, maar je weet niet waar ze zich bevinden? en er is nog geen patch voor. Daarnaast ontwikkelen de technieken van cyberaanvallers zich razendsnel, onder andere met behulp van AI. Met AI worden social engineering en phishing-aanvallen steeds geavanceerder, iets waar veel organisaties zich nog niet bewust van zijn.

In tegenstelling tot de 'known knowns', moeten CISO's en securityteams toch wel eens wakker liggen van de 'known unknowns'. Het moet aan je knagen dat je weet dat er kwetsbaarheden in je aanvalsoppervlak zitten, maar dat je hier geen (voldoende) inzicht in hebt. Waar hebben we het dan specifiek over? Wat dacht je van je aanvoerketen? In dit hoofdstuk gaan we een aantal van deze 'known unknowns' behandelen, te beginnen met de supply chain.

Bron: https://www.akamai.com/lp/soti/lurking-in-the-shadows



AI Generated with Adobe Firefly.
Prompt: “A photo of a highly complex and constructed small digital bug entering a modern network”

2.2.1 DE RISICO'S DIE SCHUILEN ACHTER KETENPARTNERS

We hebben al vastgesteld dat de bedrijfsvoering van organisaties steeds meer en verder wordt gedigitaliseerd en geautomatiseerd. Gebaseerd op data optimaliseren organisaties hun processen en werken zij efficiënter samen met andere organisaties in de keten. Bestellingen gaan via een portal, productieprocessen worden geautomatiseerd bijgestuurd en declaraties worden automatisch ingediend bij de verzekeraar. Al deze digitale stromen zorgen ervoor dat heel veel verschillende organisaties met elkaar verbonden zijn. Cybercriminelen zullen op zoek gaan naar de zwakste partner in deze keten en via deze organisatie proberen andere organisaties te raken. Dit raakt dus ook jouw aanvalsoppervlak en de impact is groot op het gebied van fysiek, technologie en mens.

Impact op fysiek, technologie en mens

Dit soort supply chain attacks vindt steeds meer plaats. *Uit het Verizon Data Breach Investigation Report 2024 wordt duidelijk dat vijftien procent van de data breaches te maken had met ketenpartners, ook wel third parties genoemd.* Dit is een stijging van 68 procent ten opzichte van het voorgaande jaar. Dit komt vooral door het gebruik van zero-day exploits voor ransomware- en afpersingsaanvallen. *Je herinnert je vast nog het lek bij een onderzoeksbureau dat werkte voor organisaties als NS, VodafoneZiggo en CZ*. Bij een softwareleverancier van dat bureau wisten cyberaanvallers binnen te dringen waardoor klantgegevens buit gemaakt konden worden. *Of de meer recente incidenten bij Ticketmaster en AddComm. Een ander fameus voorbeeld is van Target Corporation, alweer ruim tien jaar geleden.* Target, na Walmart de tweede department store keten in de VS, werkte samen met een partij die de temperatuur van de koel- en vriesapparatuur beheerde. Dit beheer gebeurde via internet en dit is exact hoe hackers binnenkwamen en uiteindelijk diep in de systemen wisten door te dringen. Tientallen miljoenen klantgegevens werden toen buitgemaakt.

Weet met wie je samenwerkt

Wat gaat er dan mis in die toeleveringsketen of met je samenwerkingspartners? In de eerste plaats valt het op dat lang niet iedere organisatie strak heeft geregeld met wie zij samenwerkt. Laat staan dat zij weten in hoeverre ketenpartners hun security op orde hebben. Er zijn interacties en transacties met verschillende partijen en er zijn steeds verschillende afspraken over het delen van informatie en de wijze waarop dit gebeurt. Als gevolg hiervan, maar ook door technologische ontwikkelingen, ontstaat er een steeds complexere infrastructuur. Je ziet hybride- en multi-cloudomgevingen met verschillende serviceproviders – lokale maar ook hyperscalers als Azure, AWS en Chinese partijen. Het gaat om veel wisselende gebruikers die zich met verschillende devices op het netwerk melden – allen vanaf verspreide locaties. Voor een cyberaanvaller is er op deze manier altijd wel een zwakke plek te vinden.

Gebruik NIS2 als referentie

Een belangrijke oplossingsrichting is het opstellen van beleid met duidelijke regels en grenzen. Je kunt NIS2 gebruiken om dit beleid op te stellen; de uitgangspunten van NIS2 kun je vertalen naar beleid, wat je je ketenpartners kunt voorhouden. Zorg hierbij dat securitymaatregelen binnen de keten bespreekbaar zijn. Ga niet je eigen eisen opleggen, maar spreek een resultaat af. Door dit in beleid te gieten, voorkom je dat het in kaart brengen en monitoren van ketenpartners een eenmalige actie wordt. Dit beleid moet ook gedragen worden in de organisatie. Een manier om dit te bereiken, is om deze activiteiten zoveel mogelijk toe te passen in bestaande processen. Hierbij is het van belang om de hele levenscyclus van een derde partij mee te nemen. Cybersecurity moet je al meenemen bij de selectie en aanschaf van een product of dienst in bijvoorbeeld aanbestedingsprocedures. Net zoals je op financieel vlak een due diligence onderzoek uitvoert als je gaat samenwerken (bij bijvoorbeeld een fusie of overname), zou het niet gek zijn als je dit ook doet voor de security-omgeving.

Verder is het belangrijk om ervoor te zorgen dat je medewerkers regelmatig getraind worden op het herkennen van phishingmails en bekend zijn met voice-phishing. Help je medewerkers door een cultuur te creëren waar medewerkers zich veilig voelen om phishing te melden, ook als ze al op de link geklikt hebben. Zorg ervoor dat wanneer er twijfel is over de legitimiteit van een verzoek, het verzoek via een ander kanaal of via een collega wordt geverifieerd op echtheid.

Tot slot bestaat er ook nog de mogelijkheid dat de cybercrimineel fysiek probeert binnen te komen bij jouw organisatie. Weet wie je leveranciers zijn, controleer of de persoon ook daadwerkelijk is wie hij/zij zegt te zijn en laat gasten niet zonder begeleiding door het pand lopen. Eenvoudig gezegd: zorg dat je niet voor verrassingen komt te staan.

Bron: https://www.verizon.com/business/resources/reports/dbir/
Bron: https://nos.nl/artikel/2469354-datalek-treft-ook-vodafoneziggo-gegevens-700-000-klanten-op-straat
Bron: https://www.addcomm.nl/addcomm-geraakt-door-ransomware-update-27-mei-2024/

2.2.2 WEET WIE ER TOEGANG HEEFT TOT JE IT-LANDSCHAP

Mens, technologie en fysiek

De focus van deze paper ligt op het verkleinen van je aanvalsoppervlak. In dit kader is het goed om stil te staan bij Privilege Access Management (PAM). Deze beveiligingsaanpak is een set technologieën die is ontworpen om de toegang tot cruciale systemen, applicaties en gegevens te controleren en te beschermen door de toegang van geavanceerde accounts te beheren. Dit zijn gebruikersaccounts met uitgebreide rechten, waardoor ze in staat zijn systemen, netwerken en applicaties te beheren. Én wat ervoor zorgt dat ze een zeer aantrekkelijk doelwit voor aanvallers zijn. Overigens, nu gaat het vooral om toegang tot systemen, maar het kan ook gaan om toegang tot fysieke omgevingen. Zo heeft een medewerker die actief is op productielijn A niets te zoeken bij lijn B. Bij dit voorbeeld raken we dus opnieuw alle elementen van de attack surface: fysiek, technologie en mens.

Altijd weer dat wachtwoord

In het kader van het beheren van toegangsrechten van deze bevoorrechte accounts kan er veel fout gaan. Een veelvoorkomende fout is het niet vaak genoeg wijzigen van wachtwoorden. Gestolen of gelekte credentials kunnen zo langdurig worden gebruikt door aanvallers. Verder zien we vaak dat voormalige medewerkers of gebruikers die een andere rol hebben gekregen nog altijd dezelfde rechten hebben. Ex-medewerkers kunnen hier misbruik van maken; een datalek ligt op de loer. Dit is ook het geval wanneer medewerkers meer rechten krijgen dan nodig is voor hun functie. Daarnaast zien we dat deze super accounts niet goed worden gemonitord. Activiteiten worden onvoldoende gelogd terwijl je dit eigenlijk goed in de gaten wil blijven houden, ook in het kader van auditing voor wet- en regelgeving. Als er 'onregelmatigheden' optreden, dan wil je kunnen zien we er verantwoordelijk voor is en hoe deze misstap tot stand is gekomen. Ten slotte zien we nog vaak dat deze geprivilegieerde accounts niet zijn voorzien van multifactorauthenticatie.

PAM beperkt aanvalsoppervlak

De oplossing voor het beperken van het aanvalsoppervlak door het toegangsbeheer – fysiek en digitaal – strak te controleren, begint ook nu met inzicht. Zeker als het gaat om bevoorrechte accounts. Weet je als organisatie welke accounts 'superrechten' behelzen en weet je welke gebruikers hier aanspraak op kunnen maken? Kijk nog eens goed naar de rollen en functies in je organisatie en hou dit aan tegen de huidige toegekende rechten. Bepaal vervolgens de voorwaarden voor dit toegangsbeheer, zoals:

- Waar mogen gebruikers toegang krijgen? Bijvoorbeeld niet via een publieke Wifi of alleen binnen een kantooromgeving. Of: alleen in productiehal 1.
- Wanneer krijgen gebruikers toegang? Bijvoorbeeld van 9:00 tot 17:00 uur of in verschillende tijdzones?
- Wat mogen de bevoorrechte gebruikers doen? Ook voor hen zijn er beperkingen.

Het is raadzaam een PAM-oplossing te implementeren die een groot aantal beheertaken automatiseert. Daarbij moet je denken aan de volgende functionaliteiten:

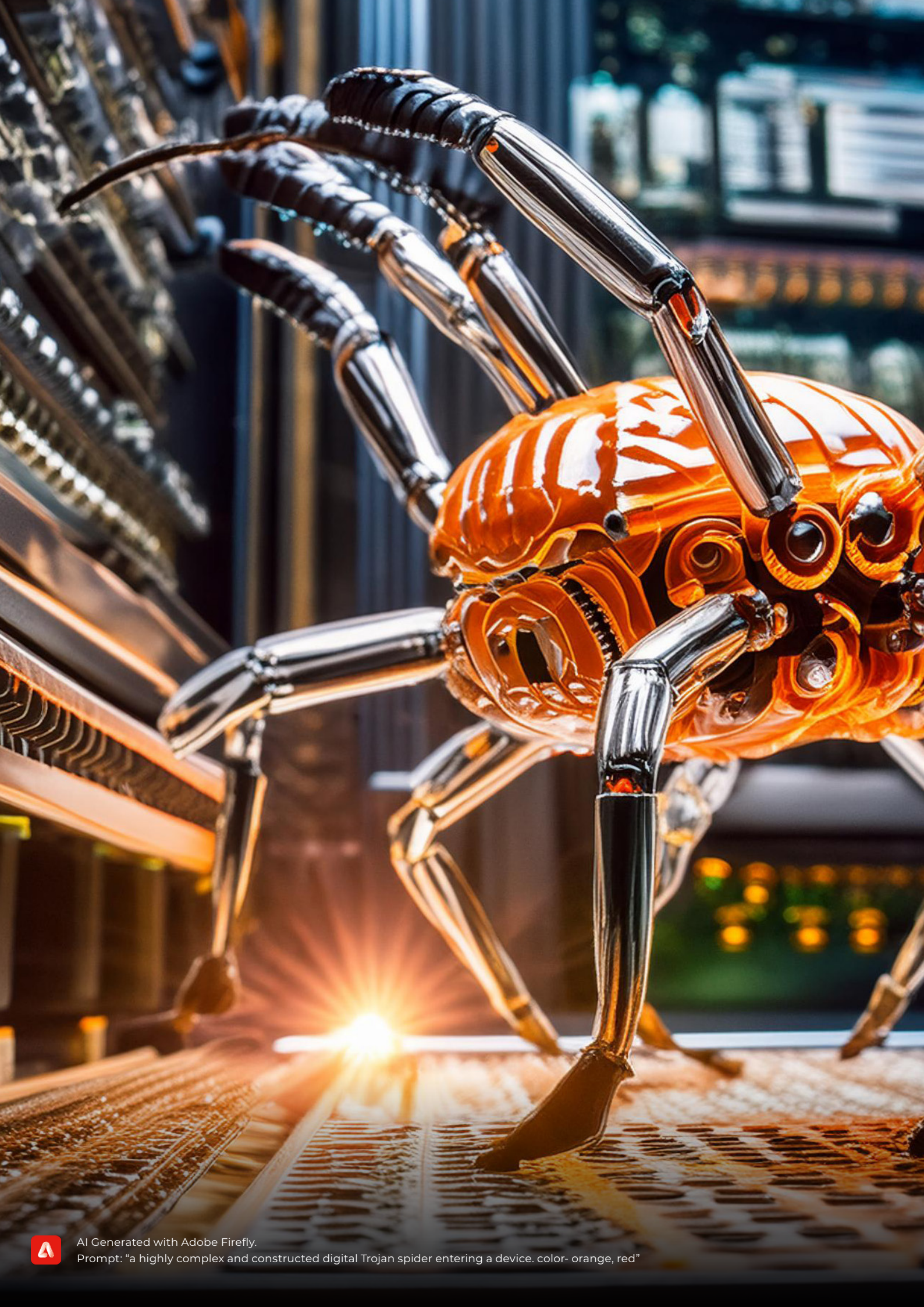
- Automatische wachtwoordrotatie: PAM-oplossingen beheren en roteren wachtwoorden van geprivilegieerde accounts regelmatig om het risico op misbruik te minimaliseren.
- Realtime bewaking van activiteiten uitgevoerd door geprivilegieerde accounts om verdachte activiteiten te detecteren. Dit is ook van belang in het kader van NIS2.
- Implementeren van het least privilege-principe, waarbij gebruikers alleen toegang krijgen tot de resources die zij nodig hebben voor hun werk.
- Uitgebreid inzicht in het gebruik en beheer van geprivilegieerde accounts.

Kortom, een PAM-oplossing zorgt ervoor dat het aanvalsoppervlak niet groter is dan strikt noodzakelijk.

2.2.3 VULNERABILITY- EN PATCHMANAGEMENT

Een aantal mogelijke oplossingen om het aanvalsoppervlakte van een organisatie te verkleinen hebben we inmiddels besproken. Vulnerability- en patchmanagement mag in dit rijtje niet ontbreken. Wanneer we kijken naar het aanvalsoppervlakte van een organisatie dan zien we dat niet gepatchte kwetsbaarheden en misconfiguraties nog steeds een belangrijke manier is om bij een organisatie binnen te komen. *Verizon Data Breach Investigation Report 2024 spreekt zelfs over een stijging van 180 procent waar het de uitbuiting van kwetsbaarheden betreft.*

Bron: https://www.nbcnews.com/technology/massive-target-credit-card-breach-new-step-security-war-hackers-2D11778083
Bron: https://www.verizon.com/business/resources/reports/dbir/



AI Generated with Adobe Firefly.
Prompt: “a highly complex and constructed digital Trojan spider entering a device. color- orange, red”

Patchen, zo snel mogelijk – indien mogelijk
Met een toenemend aantal systemen binnen een organisatie, die vaak een verbinding hebben met het internet, is het bijna ondoenlijk om zicht te houden op alle systemen, applicaties en versies. Er is slimme tooling voor nodig om voor alle assets versiebeheer uit te voeren en te controleren of de configuraties geen ongewenste risico's introduceren. Een ander probleem is dat niet elk systeem te patchen is. Soms zijn er specifieke machines in gebruik waarvan de economische levensduur nog niet bereikt is, maar waarvan de fabrikant of leverancier niet meer in staat is om noodzakelijke updates te leveren. Het principe direct patchen gaat niet in alle situaties op, productielijnen kunnen niet per direct stilgelegd. Vaak is het credo, zo snel mogelijk, indien mogelijk.

In dit geval wil je om het aanvalsoppervlakte te verkleinen frequent inzicht in welke systemen er in gebruik zijn, of deze op de laatste softwareversies draaien en of ze wellicht configuratiefouten bevatten. Daar waar systemen kwetsbaar zijn maar niet gepatcht kunnen worden, wil je in de periferie afdoende maatregelen treffen om het risico op een incident zo veel mogelijk te mitigeren.

2.2.4 GRIP OP UNMANAGED DEVICES

Naast alle apparaten die je als organisatie in beheer hebt, komt het ook voor dat er onbeheerde apparaten toegang krijgen tot het netwerk. Denk aan een laptop van een servicemonteur of de mobiele telefoon van een bezoeker. Onbeheerde apparaten vormen een aanzienlijk risico voor het aanvalsoppervlak van een organisatie. Deze apparaten, die vaak niet zijn opgenomen in het reguliere beheer- en beveiligingsbeleid, kunnen ongemerkt toegangspunten voor cyberaanvallen worden. Het is dan ook essentieel om proactief het aanvalsoppervlak te minimaliseren om de digitale assets van je organisatie te beschermen. Deze uitdaging neemt verder toe door de toename van cloudservices en mobiel computergebruik.

Belangrijke maatregelen:
- **Identificatie**: Met geavanceerde tooling kun je onbeheerde apparaten automatisch identificeren.
- **Beheer**: Zodra geïdentificeerd, moeten deze apparaten worden beheerd om het risico dat ze vormen te verminderen.

Voordelen van effectief beheer:
- **Risicoreductie**: Vectra AI stelt dat organisaties het risico op een cyberaanval met wel 80% kunnen verlagen door gebruik te maken van slimme detectietechnieken als NDR. Op het moment dat preventieve maatregelen niet succesvol zijn kan NDR helpen risico's te mitigeren.
- **Overzicht**: Het is cruciaal dat organisaties een duidelijk overzicht hebben van alle apparaten die verbinding maken met hun netwerken.
- **Beveiligingsmaatregelen**: Implementeren van passende beveiligingsmaatregelen om deze potentiële zwakke punten aan te pakken.

Een oplossing als Tesorion Immunity identificeert apparaten die toegang tot het netwerk willen. Vervolgens vindt er toegangscontrole plaats: welke apparaten hebben er toegang hebben tot het netwerk. De volgende stap is geautomatiseerde detectie en isolatie. Zo ontstaat er een krachtige combinatie. Kortom, jij bepaalt wie er toegang krijgt tot het netwerk en wat acceptabel gedrag is, waardoor je het aanvalsoppervlak effectief kunt beheersen.

2.2.5 DENKEN ALS EEN CYBERCRIMINEEL

In de voorgaande hoofdstukken ging het met name om technische oplossingen om grip op het aanvalsoppervlakte te krijgen en bij voorkeur te verkleinen. Red Teaming is hier een goede aanvulling op. Red Teaming is het gecontroleerd binnendringen in een organisatie met behulp van digitale, fysieke en sociale methoden om toegang te krijgen tot de belangrijkste assets. Het doel is om de cybersecuritymaatregelen van een organisatie grondig te testen, inclusief:

- Technische testen, zoals vulnerability- en penetratietesten
- Detectie en response, zoals controleren of alerts werken en processen goed zijn ingericht en gevolgd
- Social engineering, zoals testen van menselijke naïviteit respons op incidenten
- Simuleren van aanvallen zoals een Advanced Persistent Threat (APT)
- Gebruik van technieken, tactieken en procedures (TTP) zoals een cyberaanvaller
- Identificeren van kwetsbaarheden die succesvol kunnen worden benut

Social engineering is een aanvalstechniek waarbij de menselijke factor wordt uitgebuit om toegang te krijgen tot systemen, netwerken of data. Met een groter aanvalsoppervlak door meer medewerkers, apparaten en diensten, nemen de potentiële zwakke punten toe. Het is daarom cruciaal om medewerkers bewust te maken van phishing- en vhishing-pogingen om het aanvalsoppervlak te verkleinen.

Uiteindelijk werkt een Red Team toe naar een rapport met bevindingen en aanbevelingen, dat beschrijft hoe systemen zijn binnengedrongen, welke cybersecuritymaatregelen zijn omzeild en welke gegevens zijn bemachtigd. Dit rapport bevat ook:

- Alle ontdekte hiaten, inclusief verholpen en openstaande
- Maatwerk aanbevelingen voor de organisatie.

Red Teaming is vooral effectief voor organisaties met een volwassen beveiligingsprogramma, die regelmatig penetratietests uitvoeren en over het algemeen positieve resultaten hebben. Het helpt om resterende hiaten aan het licht te brengen, zelfs als technische controles zwak zijn of er geen detectie- en responsemaatregelen zijn. Kortom, Red Teaming biedt een diepgaande test van de beveiliging door middel van gecontroleerde digitale inbraken en het helpt organisaties de weerbaarheid van hun aanvalsoppervlak te versterken.

2.3 UNKNOWN UNKNOWNS

De laatste categorie die we behandelen zijn de ‘unknown unknowns’. Omgaan met het onbekende is iets wat ondernemers eigen is, zou je zeggen. Nieuwe, onverwachte en soms ook disruptieve ontwikkelingen komen zo nu en dan op je pad. In het kader van security moet je dan denken aan compleet nieuwe aanvalsmethoden die aanvallers ontwikkeld hebben. Of je krijgt te maken met onvoorziene beveiligingsproblemen bij een ketenpartner, die ontstaan door de complexiteit van deze ketens. Verschillende clouds werken met elkaar samen en on premise applicaties draaien naast webapplicaties.

Waar het vooral bij deze totaal onbekende securitydreigingen om gaat, is in de eerste plaats erkennen dat deze er zijn en dat je ernaar moet handelen. In de tweede plaats dien je een omgeving te creëren die je in staat stelt snel in actie te komen. Flexibel, agile, in staat om te handelen. Erken en herken direct de risico’s, neem mitigerende maatregelen en vooral: kom in actie.

Om je hierbij op weg te helpen, beschrijven we hieronder een aantal belangrijke unknown unknowns, waar iedere organisatie mee te maken heeft. Ook die van jou.

2.3.1 OPEN SOURCE INTELLIGENCE

Een sluimerend gevaar binnen je aanvalsoppervlak is dat er op diverse online plekken informatie over je organisatie beschikbaar is, zonder dat jij daar weet van hebt. OSINT, wat staat voor ‘Open Source Intelligence’ is niet alleen kennisnemen van allerlei losse brokjes informatie, maar deze combineren en aanwenden om zo tot kennis te komen. Dergelijke bronnen zouden sociale media, websites, openbare registers en andere gegevens kunnen zijn. Denk ook aan academische bronnen, zoals scripties en onderzoek van universiteiten. OSINT kan voor verschillende doeleinden worden gebruikt, zoals:

- Het schatten van beveiligingsrisico’s.
- Het spotten van potentiële dreigingen.
- Of het vergaren van bewijsgegevens voor forensisch onderzoek.

Dit alles zonder hacken of inbreken in gesloten systemen. Het is dan ook een waardevolle aanpak binnen cybersecurity. Je krijgt inzicht in de vraag hoe de informatie van je organisatie beschikbaar is en mogelijk door cybercriminelen kan worden misbruikt. En reken maar dat openbare bronnen gebruikt worden voor het verzamelen van intelligence over jouw organisatie.

Schadelijk of onschadelijk?
Openbare bronnen beschouwen we op het eerste gezicht als onschuldig en onschadelijk. Het wordt al een stuk minder onschuldig wanneer je je bedenkt dat wanneer iemand alle openbare bronnen van een bedrijf langere tijd monitort, diegene iets kan zeggen over de ontwikkeling van dat bedrijf. Groeit de onderneming, heeft het aandelen uitgegeven, zijn er investeerders aan boord gekomen, heeft het een bekende CEO aangesteld of gaat het juist bergafwaarts met een onderneming? Allemaal interessante informatie in een historische context op basis waarvan aanvallers een mogelijk doelwit kunnen selecteren.

Andere openbare bronnen worden vervolgens gebruikt om een manier te vinden om in te breken op systemen. Laten we er aan aantal opsommen:



AI Generated with Adobe Firefly.
Prompt: “a unknown hologram with a person looking at it. the hologram facing towards from the camera”

- Je kunt veel informatie halen uit DNS domeinnamen, gepubliceerde certificaten en IP-adressen. Zo is het mogelijk te achterhalen welk e-mailsysteem een organisatie gebruikt en welke firewalls er worden ingezet.

- Vervolgens kun je in vacatureteksten terugvinden wat voor type netwerkbeheerder er gevraagd wordt en welke certificeringen deze moet hebben. Dit geeft een uitstekend beeld van de complete netwerkconfiguratie.

- Ten slotte zien we een referentie op de website van een architectenbureau waarin de renovatie van een nieuw kantoorgebouw wordt gepresenteerd. Op de foto's zijn duidelijk de namen van de vergaderzalen te zien; namen die zeer waarschijnlijk ook gebruikt worden in de office en agenda applicaties van het bedrijf. En mocht een fysieke inbraak noodzakelijk zijn, dan weet je meteen de indeling van het kantoor.

Als je al deze broodkruimels bij elkaar veegt, dan kun je een belangrijk deel van het aanvalsoppervlak reconstrueren. Je weet al heel veel over de fysieke en technologische inrichting van een organisatie. Dit is exact wat cyberaanvallers doen. Eventueel aangevuld met gestolen credentials zodat ook de factor mens aangevallen kan worden. Zie hier het recept voor de aanleiding van een succesvolle cyberaanval.

Vind de balans in OSINT
Het is haast niet te doen om alle informatie die je publiekelijk deelt tegen het licht te houden. Je wil toch ook laten zien wat je doet en commerciële ondernemingen moeten zichzelf ook op de kaart zetten. Waar het om draait, is dat je je als organisatie bewust bent van het feit dat dit soort informatie gebruikt kan worden. En dat het aanvalsoppervlak dus groter en kwetsbaarder wordt met OSINT. Vervolgens kun je beleid maken om de grootste risico's te mitigeren. Zet dus geen foto's online die iets zeggen over de inrichting van je bedrijf, weet welke data niet geschikt zijn voor een vacaturetekst en neem maatregelen om domeinnaamregistraties zo veel mogelijk af te schermen. In al deze afwegingen is het belangrijk om de balans te vinden tussen wat nodig is om het security-level hoog te houden en wat nodig is om de situatie werkbaar te houden voor de organisatie. Tegelijkertijd kun je zelf OSINT gebruiken om je digitale weerbaarheid te versterken. Want diezelfde broodkruimels die cybercriminelen op kunnen pikken met behulp van openbare bronnen, wil je zelf ook in beeld hebben. Sterker nog: als organisatie wil je niet alleen de broodkruimels, maar de hele boterham zien. Wanneer je de informatie over deze assets opvoert in een monitoringsdienst als Intelligence Driven Protection (IDP) kun je vaststellen of er ergens op het web broodkruimels gedeeld worden, achterblijven, lekken of gestolen zijn. IDP maakt gebruikt van een zeer groot aantal openbare bronnen. Op een geautomatiseerde wijze wordt de hoeveelheid beschikbare data behapbaar gemaakt en voorzien van een risico-indicator. Je hoopt een aanvalspatroon te kunnen waarnemen om in een vroeg stadium een mogelijke aanval te kunnen verstoren. Dus, staat je organisatie in de verkeerde belangstelling of gaat er iets rond over jouw organisatie op hackersfora? Dan kun je tools inzetten om deze te detecteren en tijdig in actie te komen. Denk aan het proactief opnieuw instellen van wachtwoorden of het informeren van ketenpartners. Deze tools detecteren ook pogingen om domeinnamen na te bootsen, zodat je in actie kunt komen om je digitale identiteit te beschermen.

2.3.2 JE DIGITALE MERK ONDER VUUR

Digitale aanwezigheid is oneindig
Je digitale aanwezigheid is haast oneindig en dit zorgt ervoor dat je aanvalsoppervlak net zo groot is. Het lijkt bijna onmogelijk om je merk en andere digitale assets over de hele wereld te monitoren en misbruik tegen te gaan. De gevolgen zijn merkbaar. Er zijn veel voorbeelden van merkinbreuken door cybercriminelen. Phishing-sites zijn daar een bekend voorbeeld van. Dit zijn nepwebsites die zich bijvoorbeeld voordoen als pagina's van bekende merken. Ze zijn bijna niet van de echte te onderscheiden en worden ingezet om persoonlijke gegevens te stelen. Ook zijn er 'domain name lookalikes', zoals amazom.com of goggle.com.

Cybercriminelen registreren domeinnamen die sterk lijken op die van legitieme bedrijven. Consumenten denken dat ze met het echte bedrijf te maken hebben, plaatsen bestellingen en raken hun geld kwijt. Of de lookalikes worden ingezet voor het uitvoeren van phishingcampagnes. Voor organisaties is het dan ook een uitdaging om 24/7 wereldwijd het internet te monitoren op nepsites. Hoe ga je deze sites detecteren en offline te halen? We bieden je een aantal handvatten in de volgende hoofdstukken.

Kwetsbaarheden identificeren
De schade kan enorm zijn, zeker wanneer de reputatie van het merk onder vuur komt te liggen, zoals recent bij bunq. De schuldigen zijn natuurlijk de cy-

bercriminelen maar de consumenten die slachtoffer worden komen toch bij jou als merk verhaal halen. De aandacht lijkt meer uit te gaan naar het voorkomen van e-mailphishing en ransomware, maar merkfraude, phishing-sites en typosquatting (misbruik maken van typfouten die gebruikers vaak maken bij het invoeren van een webadres in hun browser) kunnen net zo destructief zijn. Wellicht is het naïviteit of is het een kwestie van 'niet weten waar je moet beginnen'. Feit is dat je dit kwetsbare element in je aanvalsoppervlak moet identificeren en verhelpen.

Monitoring en detectie automatiseren
De oplossing ligt in de eerste plaats bij het in kaart brengen van je belangrijkste digitale assets. Dit is al direct een lange lijst, met naast je servers, PC's en smartphones onder andere:

- Domeinnamen
- IP-adressen
- Merknamen, logo's en handelsmerken
- Projectnamen
- Namen van CEO's, andere executives of oprichters/eigenaren
- E-maildomeinen

Handmatige controles van deze assets zijn ondoenlijk, daarom zijn AI en machine learning – in combinatie met cyberbeveiligingsexpertise – nodig om monitoring en detectie te automatiseren. Hierdoor kun je snel valse websites, social media-accounts en mobiele apps die zich voordoen als jouw merk ontdekken. Deze technologieën passen detectieparameters voortdurend aan op basis van veranderende dreigingen. Daarnaast gaat het ook gewoon om praktische maatregelen: registreer alle domeinnamen die ook maar een beetje lijken op die van jezelf. Ook als je dit fonetisch naast elkaar legt. Mailservers kun je zo inrichten dat vervalste accounts geblokkeerd worden. En de monitoringomgeving kan zo geconfigureerd worden dat ontdekte nepsites direct worden aangemeld bij een provider die vervolgens snel in actie kan komen om de site uit de lucht te halen. Hoe eerder, hoe beter, uiteraard. Ten slotte is het goed om de link te leggen met OSINT. Vaak is via het darkweb of langs andere kanalen duidelijk dat er een aanval op een bepaald merk op komst is. Daar kun je je dan tijdig tegen verweren.

INTELLIGENCE DRIVEN PROTECTION IN DE PRAKTIJK

Situatieschets 1: vertrouwelijke info
Vertrouwelijke orders, voorzien van alle tekenbevoegde persoonlijke gegevens inclusief handtekening, werden aangetroffen op het darkweb. Nader onderzoek leerde dat deze data afkomstig was van een 4th party "breach". Dit wil zeggen dat deze order door onze klant naar zijn leverancier (3th party) was gestuurd. Deze heeft de order doorgestuurd naar een toeleverancier. Deze leverancier van de leverancier (een 4th party in het buitenland) was slachtoffer van een ransomware-aanval waarbij oa. de gegevens van onze klant waren gelekt. De 4th party had naar eigen zeggen de juiste officiële stappen doorlopen nav de ransomware en zijn "breach" maar die informatie is nooit bij de 3th party, de leverancier van onze klant gekomen.

Wat had er kunnen gebeuren?
Je kan je voorstellen dat een geval van fraude/afpersing/oplichting met de persoonlijke gegevens van de tekenbevoegde inclusief handtekening een reële optie is.

Elke ogenschijnlijk echte order die geplaatst zou worden door de cybercriminelen namens onze klant, zou geaccepteerd kunnen worden omdat de gelijkenis met die eerdere orders praktisch 1-op-1 zou zijn geweest. Dit zou kunnen leiden tot betalingsverplichtingen aan de kant van onze klant, uren aan onderzoek en mogelijke reputatieschade in de leverancierskeketen.

Situatieschets 2: typosquatting bedrijfsdomein
Omdat IDP monitort op typosquatting zien we in een vroeg stadium een mogelijk aanval. Wat voor soort aanval is niet altijd gelijk duidelijk voor ons, maar veelal betreft het phishing. In dit geval zagen we een typosquatted domein. Deze kreeg van onze analisten een hoge risicoscore ivm de gelijkenis. Extra waakzaamheid was geboden nadat we zagen dat de ge-typosquatted domeinnaam ook MX-records kreeg . Daardoor wordt het mogelijk om een phishing mail te sturen. Deze oplichting ging zo ver dat er zelfs criminelen uit China overkwamen om de oplichting verder kracht bij te zetten.

In dit geval is gekozen voor het uitvoeren van een aanvullende "technische sweep" van de kantooromgeving . Hierbij werd gecontroleerd of er geen ongewenste apparatuur is achtergelaten. Daarnaast is er een OSINT onderzoek uitgevoerd naar de criminelen uit China en een onderzoek door een particulier rechercherbureau. Tot slot is er een uitgebreide netwerkscan van het bedrijfsnetwerk uitgevoerd.

Bron: https://nos.nl/artikel/2521727-phishing-aanvallers-opvallend-succesvol-bij-bunq-veiligheid-geen-thema

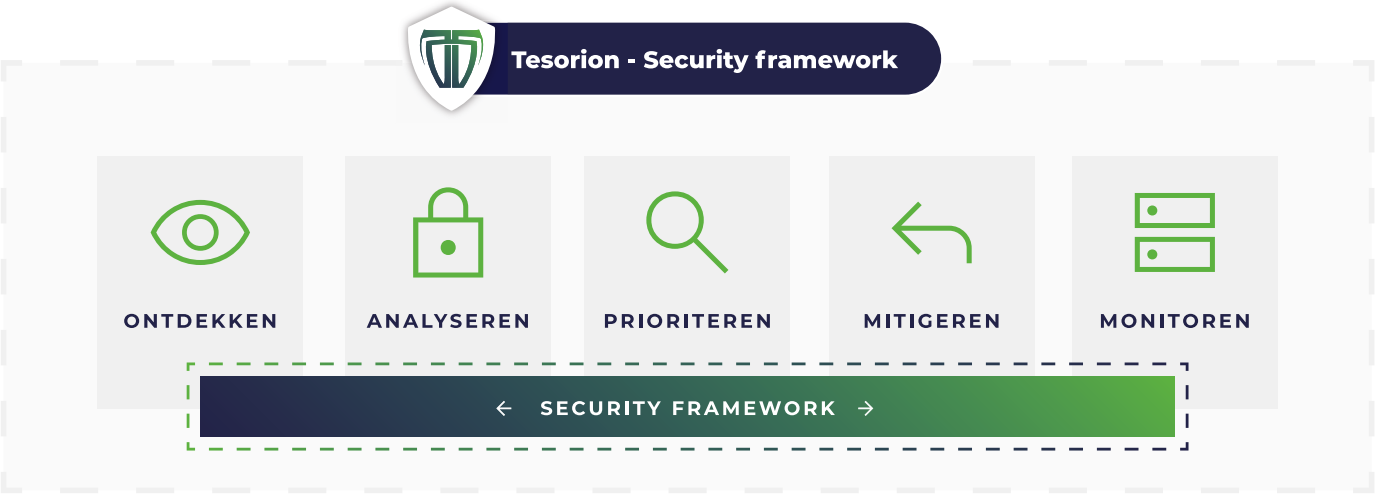


AI Generated with Adobe Firefly.
Prompt: “A person in a futuristic library about the unknown shown as a hologram.”

3. Conclusie

Iedereen heeft zijn organisatie de laatste tien jaar ontzettend zien veranderen. De digitale transformatie is bij veel organisaties in volle gang of nadert voltooiing. We werken flexibel, op verschillende locaties en op verschillende tijden met devices die we zelf prefereren. En om succesvol te zijn, maak je als organisatie deel uit van een dynamisch ecosysteem met uiteenlopende en wisselende partners. Dit vraagt ontzettend veel van de technologische infrastructuur die door de nieuwe manier van werken nieuwe kwetsbaarheden vertoont. Dit gebeurt in een tijd waarin cyberaanvallers hun methoden alleen nog maar verder verfijnen en doeltreffend maken. Zij hebben het niet alleen op de technologie gemunt; de fysieke omgeving en de mens zijn even kwetsbaar. We moeten hoe dan ook vaststellen dat het aanvalsoppervlak verder uitdijt: cyberaanvallers hebben een grotere attack surface tot hun beschikking om binnen te dringen en cyberaanvallen los te laten. Dat we dit beseffen is stap één in het realiseren van een adequate digitale afweer.

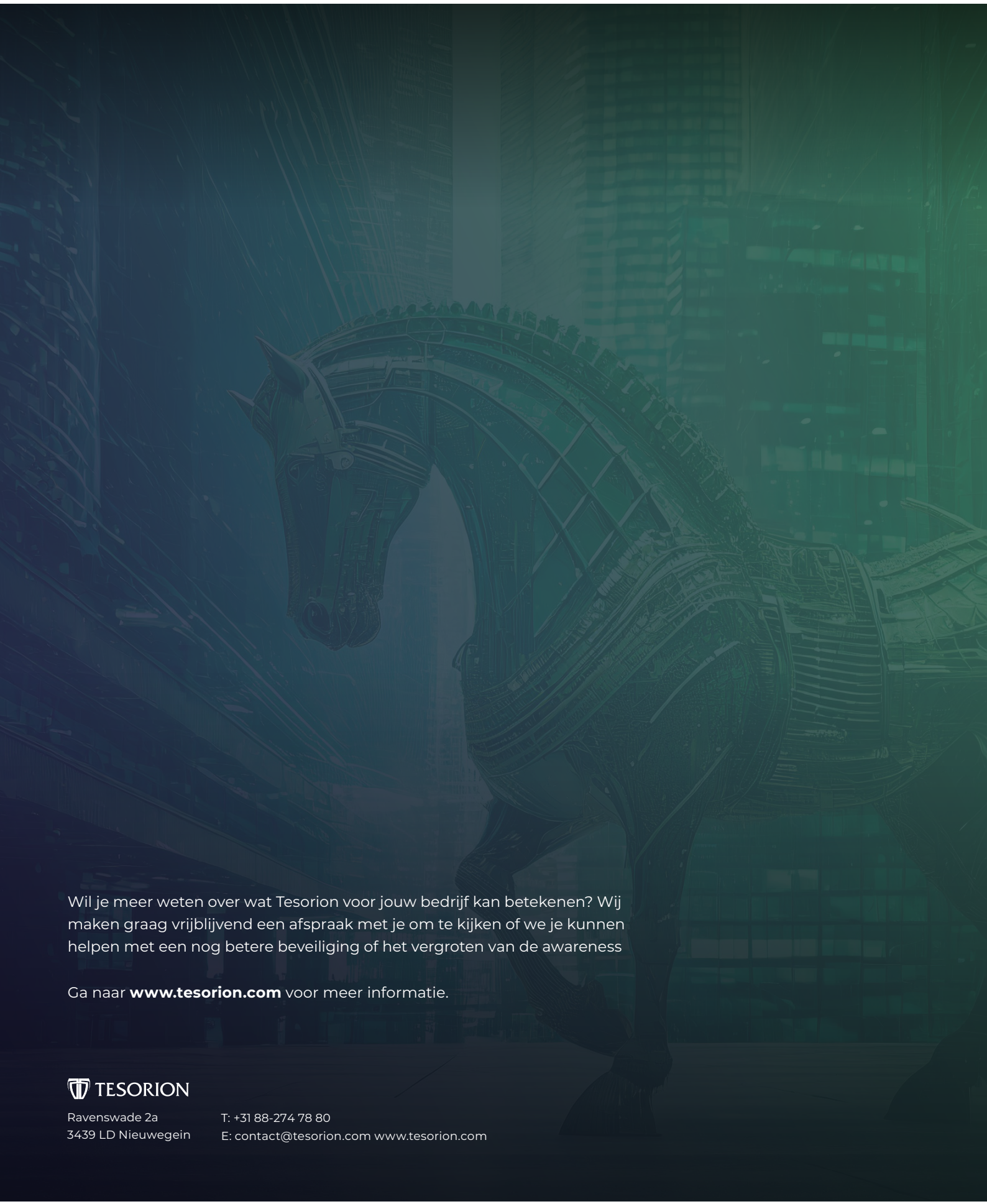
Stap twee is het identificeren van zwakke plekken in het aanvalsoppervlak. In deze paper hebben we een reeks aspecten van het aanvalsoppervlak benoemd, die versterkt moeten en kunnen worden. Veel hangt samen met het in kaart brengen van je eigen aanvalsoppervlak, iets wat je continu moet blijven doen. Het aanvalsoppervlak is immers geen statisch geheel. En omdat het heel lastig blijkt om alle cyberaanvallen, foute configuraties en inbreuken op je online identiteit tegen te houden, ligt de nadruk op monitoring en **detectie**. Hierbij word je geholpen door oplossingen die een aanval kunnen voorzien (**predict**) en vervolgens ook kunnen voorkomen (**prevent**). Om vervolgens direct in actie te komen om schade te voorkomen (**response**).



Tegelijkertijd hebben we in deze paper handreikingen gedaan om onbekende dreigingen meer bekend te maken. Het grootste risico zit ‘m in de unknown unknowns, die het aanvalsoppervlak kwetsbaar maken. Je tast volledig in het duister, maar met de inzichten uit deze paper kun je deze onbekendheden steeds verder ontmaskeren. Gebruik intelligente security-tools en platformen zodat je in ieder geval steeds meer inzichtelijk krijgt van wat je (nog) niet weet.

Tesorion weet ook dat dit handreikingen zijn die niet allemaal tegelijk geïmplementeerd kunnen worden. We laten je graag zien hoe je stapsgewijs je aanvalsoppervlak in kaart brengt en de juiste maatregelen neemt om cyberrisico’s tot een minimum te beperken.

© Tesorion 2024



Wil je meer weten over wat Tesorion voor jouw bedrijf kan betekenen? Wij maken graag vrijblijvend een afspraak met je om te kijken of we je kunnen helpen met een nog betere beveiliging of het vergroten van de awareness

Ga naar **www.tesorion.com** voor meer informatie.

TESORION

Ravenswade 2a
3439 LD Nieuwegein

T: +31 88-274 78 80
E: contact@tesorion.com www.tesorion.com