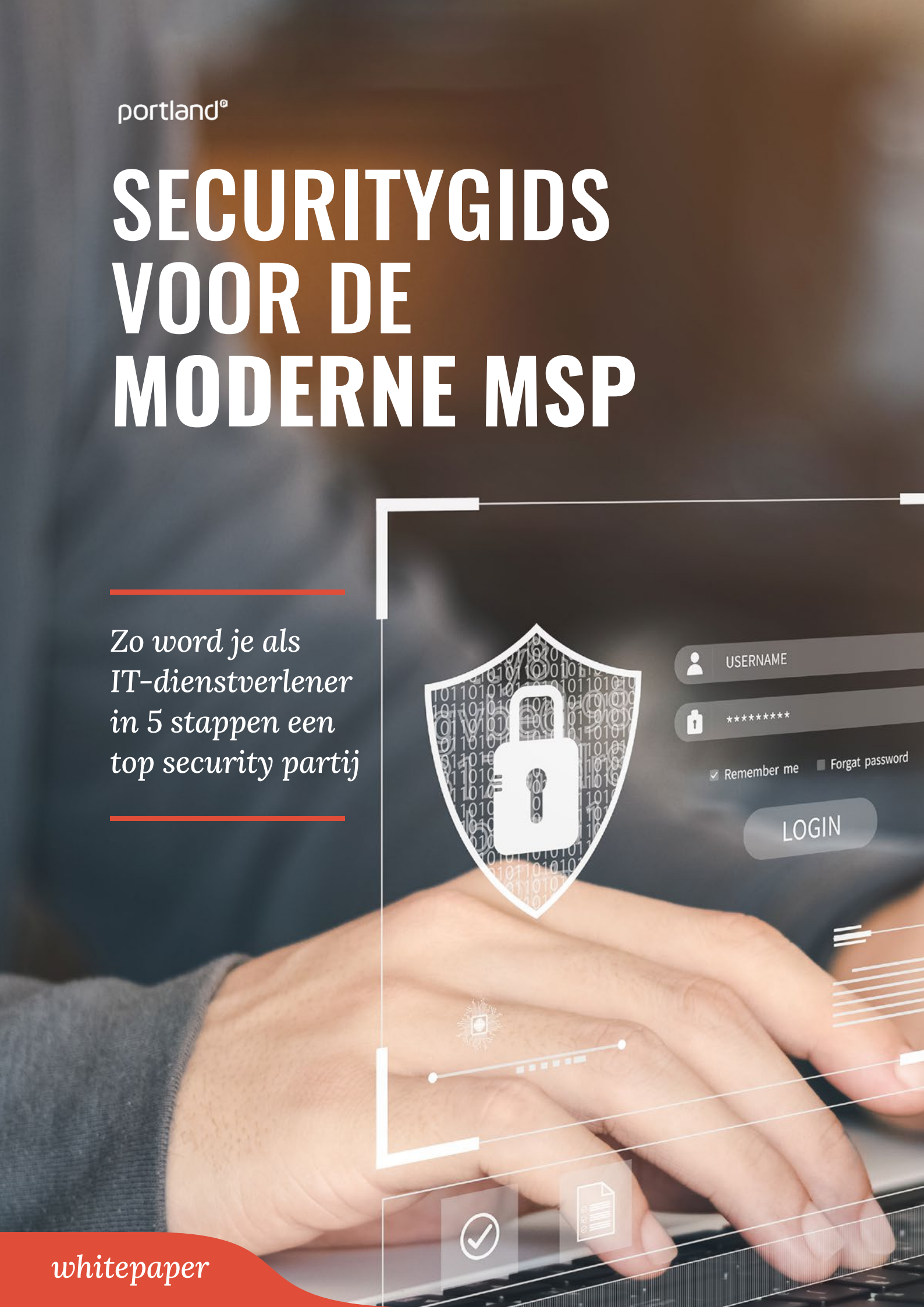
portland

SECURITYGIDS VOOR DE MODERNE MSP

Zo word je als IT-dienstverlener in 5 stappen een top security partij



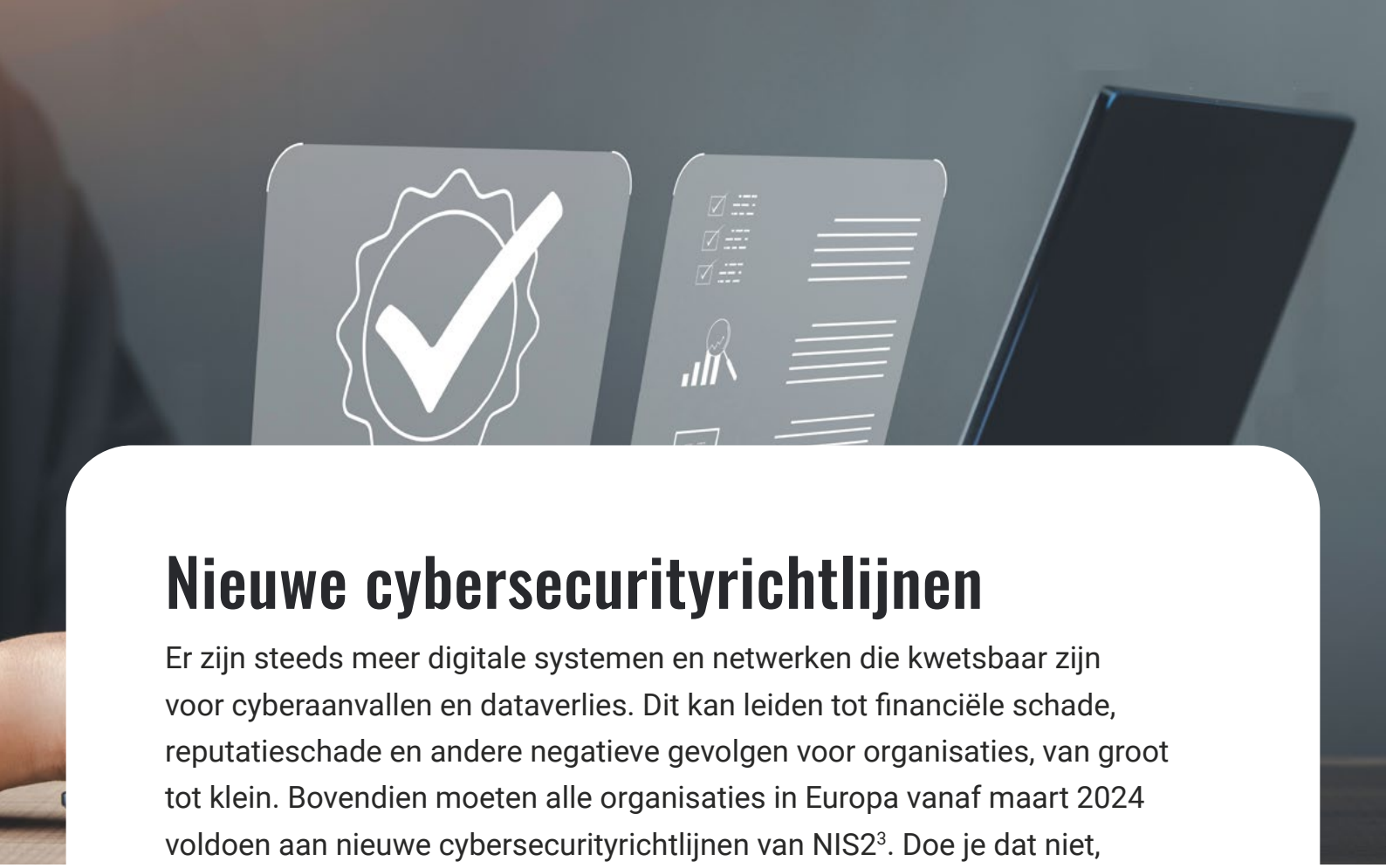
whitepaper

Waarom deze whitepaper?

Als Managed Service Provider help je organisaties aan toekomstbestendige IT-oplossingen én creëer je terugkerende inkomsten voor je eigen organisatie. Daarbij is cybersecurity belangrijker dan ooit. Het aantal cyberincidenten is de afgelopen jaren enorm gegroeid en deze trend zal zich de komende jaren zeker voortzetten.

Security Delta (HSD) is hét nationale veiligheidscluster waarbinnen zo'n 275 bedrijven, overheidsorganisaties en kennisinstellingen samenwerken om het verschil te maken in de veiligheid van onze digitaliserende samenleving. In hun jaarplan 2023[1] geven zij aan dat in 2023 de cyberweerbaarheid van het mkb één van hun prioriteiten is. Dat geeft al aan dat cyberdreigingen niet alleen een probleem zijn voor de grote corporates, maar bij bedrijven van alle groottes en in alle sectoren. Sterker nog, kleine en middelgrote bedrijven zijn vaak een gemakkelijker doelwit voor hackers vanwege hun gebrek aan middelen en beveiligingsexpertise. Volgens de Cost of Cybercrime Study van Accenture[2] is 43 procent van de cyberaanvallen gericht op kleinere bedrijven, maar is slechts 14 procent in staat zichzelf te verdedigen. Werk aan de winkel dus voor MSP's.

1 https://securitydelta.nl/media/com_hsd/report/555/document/Jaarplan-HSD-2023.pdf
2 https://www.accenture.com/us-en/insights/cyber-security-index



Nieuwe cybersecurityrichtlijnen

Er zijn steeds meer digitale systemen en netwerken die kwetsbaar zijn voor cyberaanvallen en dataverlies. Dit kan leiden tot financiële schade, reputatieschade en andere negatieve gevolgen voor organisaties, van groot tot klein. Bovendien moeten alle organisaties in Europa vanaf maart 2024 voldoen aan nieuwe cybersecurityrichtlijnen van NIS2[3]. Doe je dat niet, riskeer je een fikse boete. Die kan oplopen tot maar liefst tien miljoen euro of twee procent van de jaarlijkse omzet, de helft van de boete die de Autoriteit Persoonsgegevens op kan leggen voor het overtreden van de AVG.

> *Losse securityoplossingen vormen de zwakste schakel.*

3 https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf

NIST heilige graal voor MSP's vanaf 15 medewerkers

Het beveiligen van bedrijfsdata heeft de komende jaren dus de hoogste prioriteit. Losse securityoplossingen vormen de zwakste schakel, zo valt onder andere te lezen in Techzine[4]. Om data-inbraken te voorkomen, moeten bedrijven veel meer gebruik gaan maken van geïntegreerde securityplatforms in de cloud. Wil je dat succesvol doen, is het aan te raden de best practices, regels en richtlijnen te gebruiken van het Cybersecurity Framework (CSF), uitgegeven door het National Institute of Standards and Technology (NIST). Dit framework is de heilige graal van de informatiebeveiligingsraamwerken. Het helpt je als MSP de cyberbeveiligingrisico's van je klanten optimaal te beheersen. Zo optimaliseer je de beveiliging van hun digitale systemen en netwerken. CSF is gebaseerd op vijf pijlers die je helpen een holistisch en succesvol cyberbeveiligingsplan op te stellen: identificeren, beschermen, detecteren, reageren en herstellen. Elke pijler is ingedeeld in categorieën en subcategorieën.

Het initiële CSF, gelanceerd in 2014, bracht een lang en ingewikkeld implementatieproces met zich mee dat voor de meeste mkb-organisaties niet haalbaar was. Inmiddels is het framework geüpdatet. CSF 2.0 is eenvoudiger en flexibeler, zodat het ook voor kleinere organisaties toepasbaar is. CSF 2.0 legt ook veel nadruk op incidentrespons en de acties die nodig zijn om te reageren op en te herstellen van een datalek of ander beveiligingsincident.

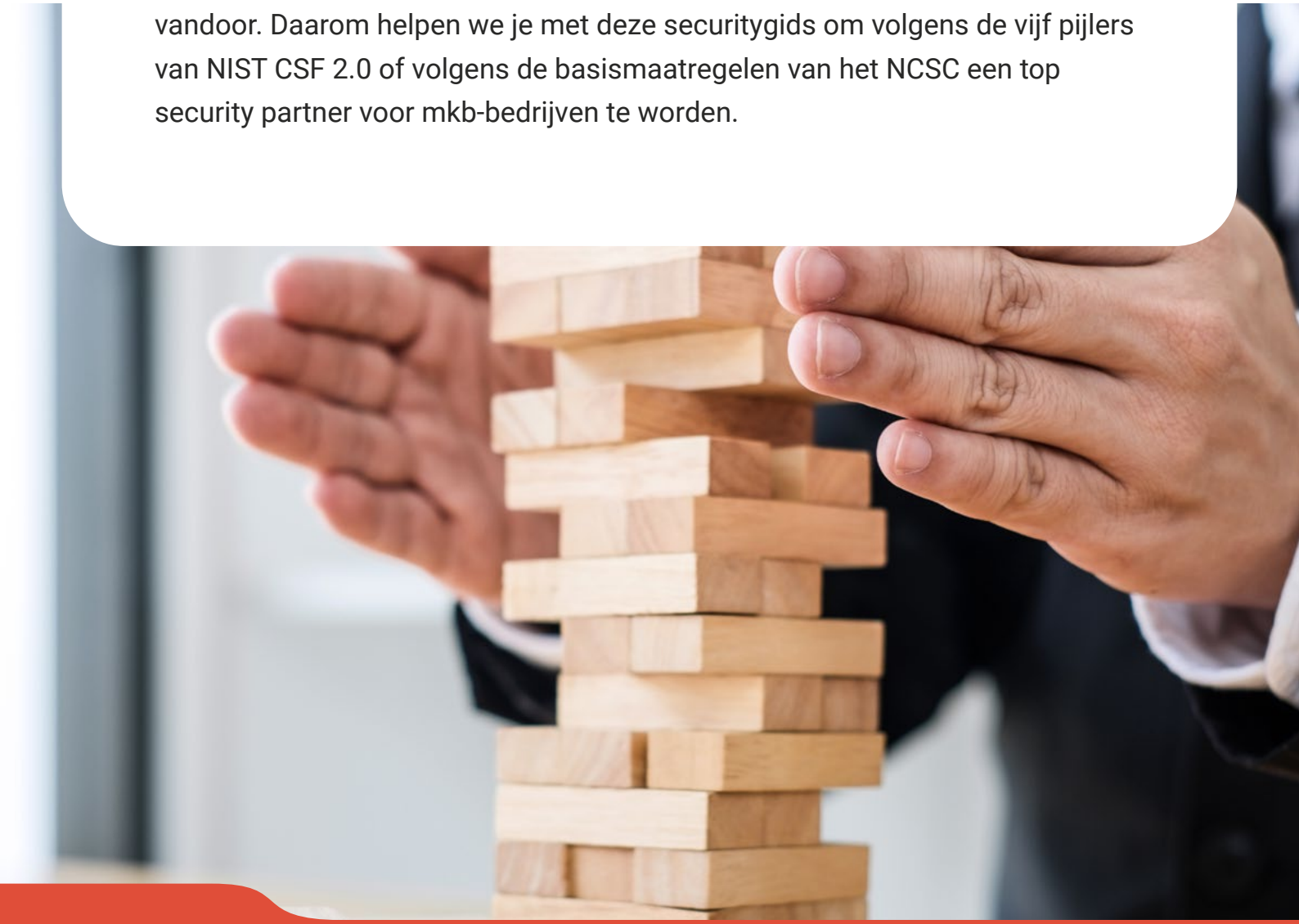
4 https://www.techzine.nl/experts/security/513675/security-voorspellingen-2023-uw-data-zijn-het-belangrijkste-doelwit/

Basismaatregelen van NCSC voor MSP's tot 15 medewerkers

Ook al is het CSF 2.0 makkelijker en flexibeler, we weten uit ervaring dat het voor veel kleinere organisaties alsnog onhaalbaar is om zich te certificeren voor NIST of ISO 27001. Gelukkig zijn er meerdere wegen die naar Rome leiden en dat weet ook de overheid. Met de basismaatregelen van het Nederlands Cyber Security Centrum, zoals besproken op pagina 19 en 20, kom je al een heel eind.

Aan de slag met je cybersecurity stack

Als MSP is 2023 hét jaar waarin je hoe dan ook aan de slag moet met je cybersecurity stack. Doe je het niet, dan gaat een ander er met jouw klanten vandoor. Daarom helpen we je met deze securitygids om volgens de vijf pijlers van NIST CSF 2.0 of volgens de basismaatregelen van het NCSC een top security partner voor mkb-bedrijven te worden.



1. IDENTIFICEREN

In het kort

De pijler ‘Identify’ bevat best practices, regels en richtlijnen betreft het identificeren van systemen, data en andere waardevolle assets die beschermd moeten worden omdat ze van belang zijn voor de organisatie om haar doelstellingen te halen. Hoe ziet de bedrijfsomgeving eruit en welke bedrijfsprocessen zijn kritisch? Waar zitten potentiële risico’s?

Asset management

Het is belangrijk dat een organisatie een nauwkeurige inventaris opstelt en kan beheren van alle data, applicaties, apparaten en andere (geautomatiseerde) systemen die de organisatie in staat stellen om haar doelstellingen te bereiken. Hoewel asset management ook gaat over mensen en de processen binnen een organisatie, moet de focus uiteraard liggen op technologieën die kunnen worden bedreigd van buitenaf. Pas als je een organisatie hebt geholpen dit goed in beeld te brengen, kun je effectief een robuust cyberbeveiligingsprogramma implementeren.

Bedrijfsomgeving

Breng de missie, doelstellingen en activiteiten van de organisatie in beeld en prioriteer ze. Leg ook vast wat de plek van een organisatie is binnen de leverancierskеten en branche. Op basis daarvan kunnen cyberbeveiligingsrollen, verantwoordelijkheden en risicobeheerbeslissingen worden vastgesteld.

Governance

Maak een inventarisatie van het beleid, de rollen en verantwoordelijkheden binnen de organisatie en de wettelijke risico-, milieu- en operationele eisen en procedures waaraan de organisatie moet voldoen.

Risicobeoordeling

Identificeer potentiële beveiligingsrisico's en leg die risicobeoordeling vast in een eenvoudig te begrijpen rapport. In dit rapport moeten de volgende zaken zijn opgenomen:

- ✔ Wat een organisatie doet aan het cyberbewustzijn van medewerkers.
- ✔ Hoe bedreigingen intern worden gedocumenteerd en aangepakt.
- ✔ Hoe de organisatie IT-middelen beoordeelt op kwetsbaarheden.
- ✔ Welke plannen en processen een organisatie heeft voor het aanpakken van cyberincidenten, inclusief een beoordeling of deze processen ook daadwerkelijk worden gehanteerd als een incident zich voordoet.

Op basis van de informatie in dit rapport, kun je bruikbare aanbevelingen doen om de beveiliging verder te versterken. Door dit zo concreet mogelijk te maken, maak je de dreiging van cyberaanvallen reëler en versterk je het bewustzijn van het management van de organisatie. Een grondige risicobeoordeling omvat netwerkkwetsbaarheden, problemen met gegevensnaleving, maar ook interne dreigingen. Deze risicobeoordeling vormt ook een mooi startpunt voor een gesprek over de naleving van belangrijke beveiligings- en privacyregelgevingen, zoals de AVG en de NIS 2-richtlijn[5] die vanaf maart 2024 van kracht is.

Op basis van deze risicobeoordeling kun je een organisatie helpen een risicobeheerstrategie op te stellen die operationele risicobeslissingen ondersteunt.

5 https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/en/pdf

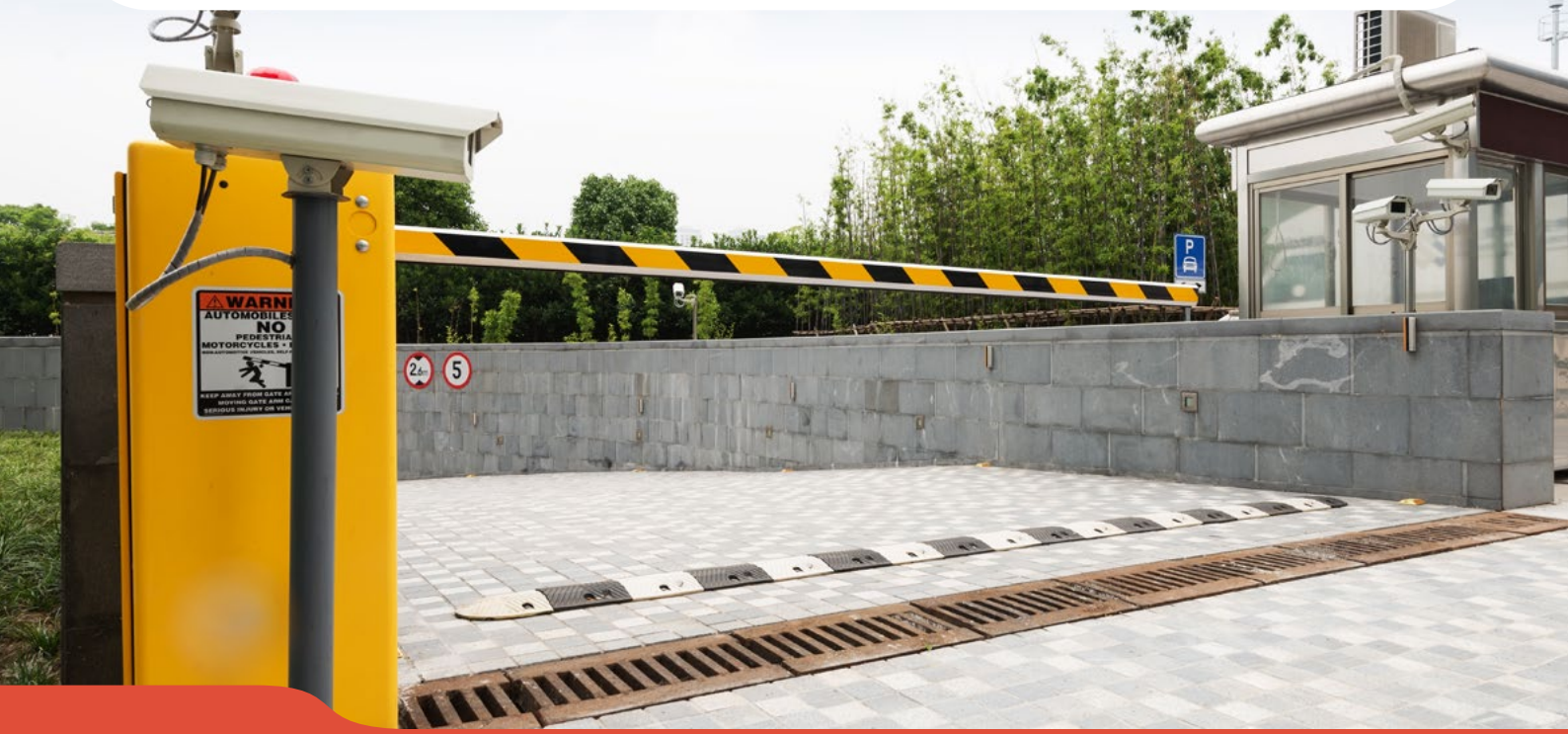
2. BESCHERMEN

In het kort

De pijler ‘Protect’ gaat over het implementeren van de juiste beveiligingsmaatregelen om de geïdentificeerde systemen, data en andere waardevolle assets daadwerkelijk te beschermen.

Toegangscontrole

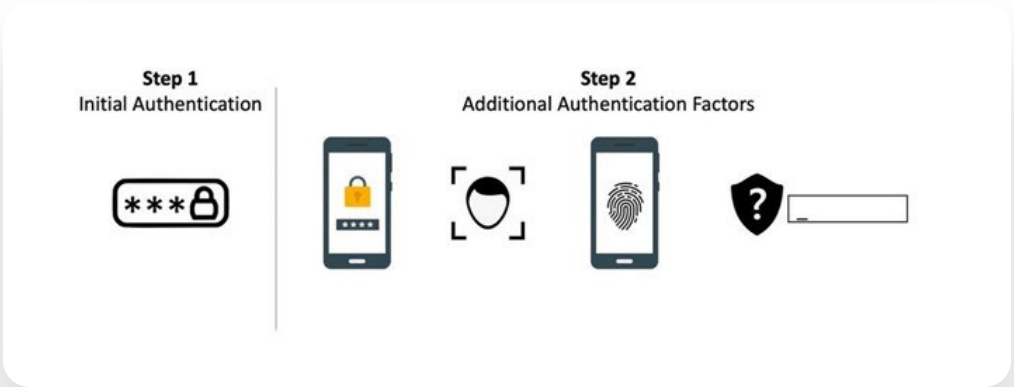
Op basis van een goed securitybeleid kan een organisatie haar toegangsbeleid vormgeven. Wie heeft toegang tot een bepaald bedrijfsnetwerk en tot welke onderdelen? Door middel van authenticatie en autorisatie kan een organisatie garanderen dat gebruikers werkelijk zijn wie ze zeggen dat ze zijn en dat ze de juiste toegang hebben tot bedrijfsgegevens. Die authenticatie en autorisatie kan plaatsvinden op basis van – een combinatie van – gebruikersnamen, wachtwoorden, pincodes, biometrische scans en beveiligingstokens. Zodra een gebruiker is geverifieerd, autoriseert toegangscontrole vervolgens het juiste toegangsniveau en toegestane acties die zijn gekoppeld aan de inloggegevens en het IP-adres van die gebruiker.



Multifactorauthenticatie onmisbaar

Maandelijks worden miljoenen mailboxen gehackt. In 99 procent van de gevallen kan dit worden voorkomen door multifactorauthenticatie (MFA) toe te passen. MFA is een beveiligingsmethode die gebruikmaakt van meerdere identificerende factoren om de identiteit van een gebruiker te verifiëren, in plaats van simpelweg te vertrouwen op de traditionele gebruikersnaam en het traditionele wachtwoord. Het is een combinatie van iets dat je weet – bijvoorbeeld een wachtwoord –, iets dat je hebt – zoals een code die wordt verstuurd via een sms of die wordt getoond in een app of op een token – en iets wat je bent – biometrie of gezichtsherkenning.

MFA moet een ingebed onderdeel zijn van je serviceaanbod om applicaties en gegevens van je klanten te beschermen tegen cyberaanvallen. Azure Multi-Factor Authentication[6] van Microsoft is een goede manier om toegang tot gegevens en apps te beveiligen, zonder het proces heel ingewikkeld te maken voor medewerkers.



6 https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Securitybewustzijn en -trainingen

Cybercriminelen innoveren voortdurend en het aantal aanvallen neemt toe. Maar liefst zestig procent van de aanvallen wordt veroorzaakt door phishing, zo blijkt uit recent onderzoek[7] door Hornetsecurity. In dit onderzoek naar ransomware-aanvallen werden gegevens verzameld van meer dan tweeduizend IT-professionals in verschillende sectoren en over verschillende continenten. Veel aanvallers misbruiken menselijke kwetsbaarheid, want zelfs de beste cyberbeveiliging laat ruimte voor menselijke fouten. Er wordt niet voor niets vaak gezegd dat de mens de zwakste schakel is bij cybersecurity.

Gepersonaliseerde training belangrijk

Veel aanbieders van cyberbeveiligingsverzekeringen eisen dat organisaties hun medewerkers regelmatig een security awareness training laten volgen. Daarbij is het belangrijker dat elke medewerker precies die training krijgt die nodig is. De Employee Security Index (ESI) helpt daarbij. Deze benchmark, ontwikkeld door IT-Seal[8], maakt het beveiligingsbewustzijn van individuele medewerkers meetbaar. Het kan honderden verschillende gesimuleerde aanvallen met verschillende moeilijkheidsgraden volautomatisch genereren en verzenden. Zo krijgt elke deelnemer een andere e-mail, wat voorkomt dat medewerkers elkaar informatie kunnen influisteren bij de koffiemachine. Dat zou immers een vertekend beeld geven van de uitkomst. Zo'n geautomatiseerde training geeft niet alleen een heel waarheidsgetrouw beeld, het is ook eenvoudig en onderhoudsarm. Zo worden alle aspecten van de bewustzijns-preventie-detectiecyclus behandeld.

7 https://www.portland.eu/formulier-hornetsecurity-ransomware-attacks-analyse
8 https://it-seal.de/en/awareness-technology/employee-security-index/

3. DETECTEREN

In het kort

De pijler ‘Detect’ betreft het snel detecteren van beveiligingsincidenten en het verzamelen van bewijs. Dit gebeurt door het monitoren van de IT-omgeving op afwijkend gedrag of ongebruikelijke gebeurtenissen, en het inrichten van een proces voor het detecteren van beveiligingsproblemen. Hierdoor kan een organisatie snel reageren op bedreigingen en ervoor zorgen dat aanvallen niet onopgemerkt blijven of dat er te laat wordt ingegrepen.

Anomalie- en gebeurtenisdetectie

Het is belangrijk voor een organisatie afwijkend gedrag en ongebruikelijke gebeurtenissen in de IT-omgeving tijdig te detecteren. Hierdoor kan worden voorkomen dat aanvallen onopgemerkt blijven of dat er te laat wordt ingegrepen.

Continu bewaking van de beveiliging

Het monitoren van een IT-omgeving van een organisatie moet 24/7 plaatsvinden, zodat eventuele beveiligingsproblemen snel kunnen worden opgemerkt en opgelost, ook buiten reguliere werktijden.

Proces voor detectie

Dit gaat over het inrichten van het juiste proces voor het opsporen van beveiligingsproblemen. Hierdoor kan een organisatie efficiënt en effectief reageren op cyberbedreigingen.

De waarde van tools voor monitoring en beheer op afstand

Het gebruik van tools voor monitoring en beheer op afstand (RMM) heeft veel voordelen. Het helpt je als MSP bij je dagelijkse activiteiten en biedt onder andere inzicht en zorgt voor preventieve monitoring. Niet alleen stelt het je in staat meerdere organisaties tegelijkertijd te bewaken en beheren, het helpt je potentiële problemen in een vroeg stadium te diagnosticeren en zelfs al op te lossen, vaak voordat de klant zich zelfs maar realiseert dat er een probleem is. Zo kun je betere service leveren en eenvoudig je servicegebied regionaal en nationaal uitbreiden.

4. REAGEREN

In het kort

In de vorige stappen zijn de risico's geïdentificeerd en de IT- omgeving in kaart gebracht (Identify) beschermende maatregelen zijn genomen (Protect), net als maatregelen om incidenten te identificeren (Detect). Nu is het tijd voor actie (Respond). Immers, hoe goed je een organisatie ook beschermt, een ongeluk zit in een klein – virtueel – hoekje. Wat doe je als een beveiligingsincident zich toch voordoet? Hoe help je een organisatie dan snel en efficiënt te reageren en de schade tot een minimum te beperken? Deze pijler bevat best practices, regels en richtlijnen met betrekking tot de juiste reactie op beveiligingsincidenten en het herstellen van de normale bedrijfsvoering.

Incidentresponseplan

Een incidentresponseplan beschrijft hoe een organisatie moet reageren op beveiligingsincidenten. Dit plan geeft duidelijkheid over de rollen, verantwoordelijkheden en procedures die moeten worden gevolgd bij een incident, om zo een tijdige en adequate reactie op gedetecteerde cyberbeveiligingsincidenten te garanderen. Jay McBain, Chief Analyst Channels, Partnerships & Ecosystems van Canalys, doet een aantal voorspellingen voor de toekomst van de technologie-industrie[9]. Daarbij geeft hij onder andere aan dat detectie en reactie van vitaal belang zijn om het hoofd te bieden aan cyberdreigingen.

Communicatieplan

Een communicatieplan beschrijft hoe een organisatie communiceert met interne en externe stakeholders – inclusief wetgevingsinstanties – als beveiligingsincidenten zich voordoen.

9 https://www.canalys.com/resources/Canalys-outlook-2023-predictions-for-the-technology-industry

Analyse

Doet een cyberincident zich voor, dan moet een gedegen analyse plaatsvinden. Wat is de oorzaak van het incident, wat is de omvang en hoe groot is de impact? Waar komt de aanval vandaan en welke gegevens of systemen zijn aangetast? Een organisatie moet bij analyse de volgende stappen ondernemen:

- Verzamelen van informatie over het incident
- Evaluatie van de informatie om de oorzaak en impact te bepalen
- Identificatie van de aanvallers
- Beoordeling van de ernst van het incident
- Bepaling van welke gegevens of systemen zijn aangetast
- Identificatie van eventuele verdere risico's

Op basis van de analyse wordt besloten welke maatregelen nodig zijn om het incident op te lossen en verdere risico's te vermijden.

Mitigatie ofwel schadebeperking

Mitigatie gaat over de acties die een organisatie kan ondernemen om de gevolgen van een incident te beperken of te voorkomen dat het incident zich verder verspreidt. Het omvat de volgende stappen:

- Isoleren van het geïnfecteerde end-point, systeem of (deel van het) netwerk om te voorkomen dat de dreiging zich verder verspreidt.
- Uitschakelen van de dreiging door bijvoorbeeld het verwijderen van malware of het blokkeren van verdachte IP-adressen.
- Herstellen van de normale werking door het back-up- en disaster-recovery-plan uit te voeren.
- Verwijderen van de oorzaak van de dreiging door bijvoorbeeld het aanpassen van beveiligingsinstellingen.

- Implementeren van maatregelen om soortgelijke incidenten in de toekomst te voorkomen door bijvoorbeeld het installeren van updates of het opleiden van gebruikers.

Verbeterstappen nemen

Na elk incident moeten verbeterpunten worden geïdentificeerd en geïmplementeerd om toekomstige incidenten beter te kunnen afhandelen, met als doel om de effectiviteit en efficiëntie van het incidentresponseplan te verhogen. Zo wordt de kans dat een cyberincident zich voordoet steeds kleiner en komt een organisatie sneller tot een oplossing. Denk daarbij aan de volgende stappen:

- Evaluatie van de processen in het incidentresponseplan om te bepalen waar knelpunten zich bevinden.
- Identificatie van knelpunten en verbeterpunten door op basis van data-analyse.
- Aanbrengen van veranderingen in procedures en mogelijk het – beter – opleiden van medewerkers.
- Monitoring van de effectiviteit van de veranderingen door bijvoorbeeld het bijhouden van incidentdata.

5. HERSTELLEN

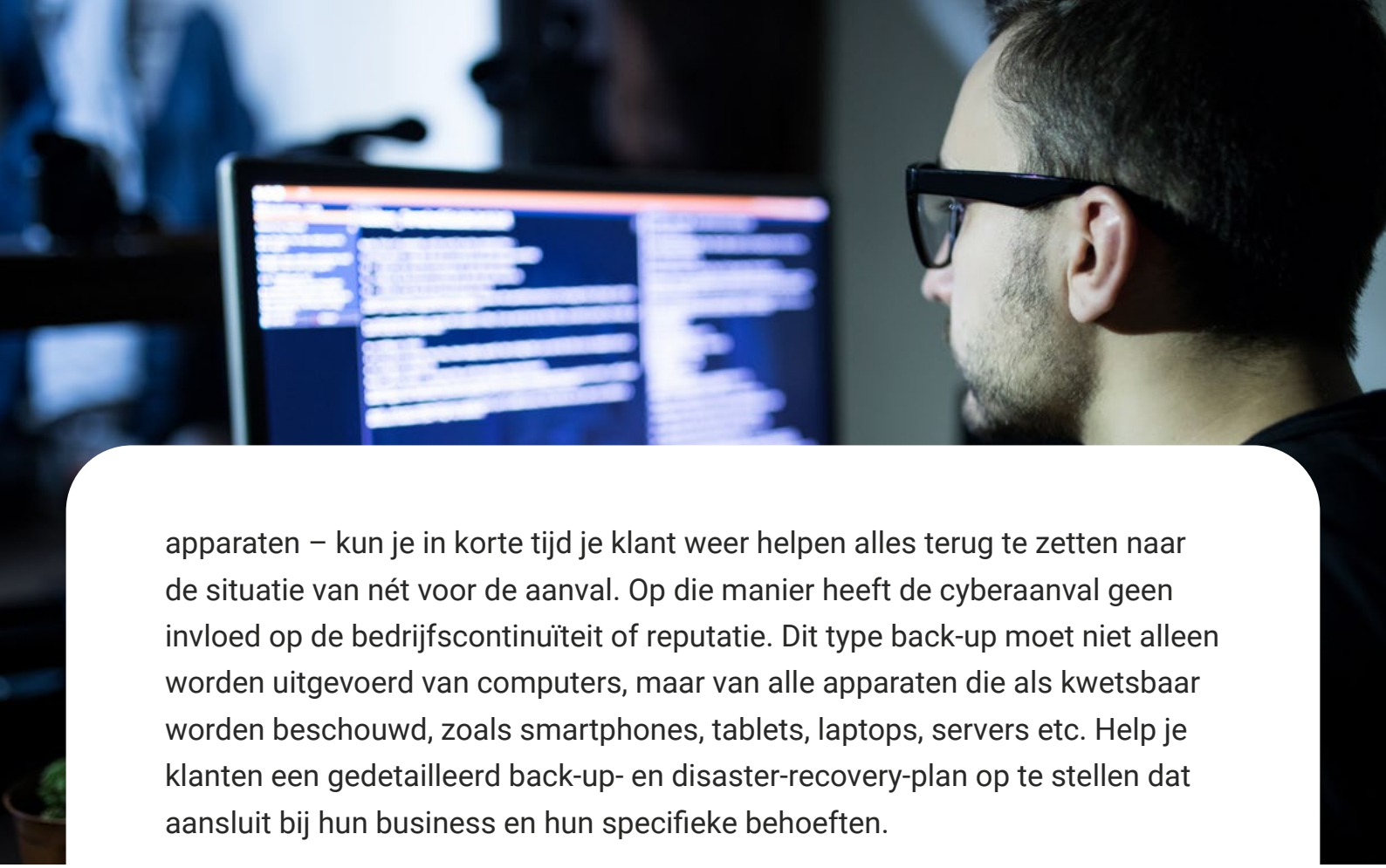
In het kort

De pijler ‘Recover’ gaat over het zo snel en efficiënt mogelijk herstellen van de bedrijfsvoering na een beveiligingsincident, het zover mogelijk beperken van de impact en het verbeteren van de beveiligingsmaatregelen om toekomstige incidenten te voorkomen.

> *Als één medewerker die gevonden usb-stick die op de parkeerplaats lag even in de computer steekt, kan het al bal zijn.*

Herstelplan

We weten allemaal dat er soms toch iets misgaat. Hoe stevig het beveiligingsbeleid ook is en hoe goed een bedrijfsnetwerk ook is beveiligd, als iemand zijn inloggegevens cadeau geeft of die usb-stick die op de parkeerplaats lag even in de computer steekt, kan het bal zijn. Dan is er een ding dat je kan helpen: een goed back-up- en disaster-recoveryplan. Als zich toch een ramp voordoet, kan het hebben van goede BDR-ondersteuning de downtime verminderen en de impact van een ramp op een organisatie verminderen. Met een – bruikbare – back-up van het hele systeem – inclusief alle gegevens, inclusief telefoons, laptops, desktops, servers en andere



apparaten – kun je in korte tijd je klant weer helpen alles terug te zetten naar de situatie van nét voor de aanval. Op die manier heeft de cyberaanval geen invloed op de bedrijfscontinuïteit of reputatie. Dit type back-up moet niet alleen worden uitgevoerd van computers, maar van alle apparaten die als kwetsbaar worden beschouwd, zoals smartphones, tablets, laptops, servers etc. Help je klanten een gedetailleerd back-up- en disaster-recovery-plan op te stellen dat aansluit bij hun business en hun specifieke behoeften.

Verbeteringen

Dit gaat over het verbeteren van de processen rondom incidentmanagement, met het doel om de effectiviteit en efficiëntie van de incidentrespons te verhogen. Dit omvat het evalueren van incident respons processen, identificeren van knelpunten en verbeterpunten en implementeren van veranderingen om knelpunten op te lossen.

Communicatie

Dit gaat over het communiceren met betrokken partijen zoals medewerkers, klanten, toezichthouders en andere belanghebbenden over het incident en de maatregelen die worden genomen om het incident op te lossen. Dit omvat het opstellen van communicatieplannen, het informeren van betrokken partijen over de status van het incident en het verstrekken van richtlijnen voor het herstel van de normale werking.

De basismaatregelen, maar dan simpel

We weten uit ervaring dat het voor veel kleinere organisaties onhaalbaar is om zich te certificeren voor NIST of ISO 27001. Het kost niet alleen heel veel tijd en energie, het gaat ook flink in de papieren lopen. Dan hebben we het nog niet gehad over het jaarlijks onderhouden van je certificering. Gelukkig zijn er meerdere wegen die naar Rome leiden en dat weet ook de overheid. Met de volgende basismaatregelen[10] kom je al een heel eind.

1. Zorg voor voldoende loginformatie

Logbestanden zijn cruciaal bij het detecteren en oplossen van cyberincidenten. Bepaal welke logbestanden je nodig hebt – systeem-, netwerk-, applicatie- en/of cloudlogging. Wil je direct op de hoogte zijn van dreigingen, zorg dan dat je notificaties ontvangt. Bepaal hoelang je de logbestanden wil bewaren en zorg dat ze in een apart netwerksegment worden opgeslagen, zodat ze intact blijven als je te maken krijgt met een cyberaanval.

2. Pas multifactorauthenticatie toe

Dit komt overeen met de pijler 'Protect' van NIST, zoals beschreven in paragraaf 2.

3. Bepaal wie toegang heeft tot je data en diensten

Zorg dat je medewerkers alleen bij die data en systemen kunnen die ze daadwerkelijk nodig hebben om hun werk te kunnen doen. Zie ook de pijler 'Protect' van NIST, zoals beschreven in paragraaf 2.

10 https://www.ncsc.nl/onderwerpen/basismaatregelen

4. Verdeel je netwerk in segmenten

Als je je netwerk in verschillende zones verdeeld, kan een virus zich niet verder verspreiden dan dat ene netwerksegment.

5. Versleutel gevoelige data

Versleutelde data is niet in te zien als je de sleutel niet hebt. Door harde schijven, laptops, mobiele apparaten en usb-sticks met gevoelige informatie te versleutelen, kunnen kwaadwillenden er niets mee.

6. Sta toegang tot het internet alleen toe als dit noodzakelijk is

Plaats apparaten die vanaf het internet bereikbaar zijn in een apart netwerksegment. Pas multifactorauthenticatie toe voor accounts die via het internet te gebruiken zijn.

7. Maak back-ups

Met een goed back-up- en disaster-recoveryplan ben je snel weer ‘up and running’ als zich onverhoopt toch een cyberincident voordoet. Zie ook de pijler ‘Herstellen’ van NIST, zoals beschreven in paragraaf 5.

8. Installeer software-updates

Softwareleveranciers brengen regelmatig updates uit waarmee kwetsbaarheden in hun applicaties kunnen worden verholpen.

TENSLOTTE: NEEM JE SECURITY STACK GOED ONDER DE LOEP

Hoe belangrijker security, hoe meer tools. Ongetwijfeld dragen alle tools bij aan het behalen van je doelen, maar de regie houden en efficiënt werken terwijl je van scherm naar scherm springt is nauwelijks te doen. Kijk naar je bestaande MSP tech stack en laat je informeren over hoe je die optimaliseert en juist integreert met de beste securitytools. Vooral 24/7/365 SOC- of MDR-diensten worden steeds crucialer in het afweren van cybercrime. Zo hou je controle.

SOC-AS-A-SERVICE

Hackers slapen nooit, dus moet ook de cyberbeveiliging van een organisatie 24/7 alert zijn. Een Security Operations Center (SOC) dat altijd actief is, is dan ook een waardevolle bron voor alle bedrijven, ongeacht de branche en omvang. Het vanaf scratch bouwen van een 24/7 SOC-team kost gemiddeld ongeveer 2,3 miljoen dollar. Er zullen maar weinig organisaties zijn die het budget en het talent in huis hebben om een SOC op te zetten. Hier is een mooie rol voor jou als MSP weggelegd. Door met een 24/7 SOC-team van een betrouwbare partner samen te werken, kun je jouw klanten de gemoedsrust en bescherming van een SOC bieden, zonder het hoge prijskaartje.

MANAGED DETECTION AND RESPONSE

Het belangrijkste voordeel van MDR is dat het helpt om de impact van bedreigingen te identificeren en snel te beperken zonder zelf extra personeel in dienst te nemen. Leveranciers van MDR-services kijken letterlijk over jouw schouder mee. Niet incidenteel, maar 24 uur per dag, 7 dagen in de week en 365 dagen per jaar. MDR-serviceproviders bieden een kant-en-klare ervaring,

gebruikmakend van een vooraf gedefinieerde tech stack die gebieden bestrijkt zoals endpoint-, netwerk- en cloud-services. Zo worden relevante logboeken, gegevens en contextuele informatie verzameld. Deze telemetrie wordt binnen het platform van de provider geanalyseerd met behulp van verschillende technieken. Dit proces maakt onderzoek mogelijk door experts die bekwaam zijn in het opsporen van bedreigingen en incidentbeheer, die bruikbare resultaten opleveren.

VAN IT-DIENSTVERLENER NAAR MODERNE MSP

Steeds meer IT-dienstverleners en Value Add Resellers (VAR's) willen doorgroeien naar een rol als Managed Service Provider (MSP). Om van een reactieve naar een proactieve of zelfs een moderne MSP door te groeien, is de keuze voor de juiste tools cruciaal. Zo moet je de beschikking hebben over een goed ingerichte PSA- en RMM-omgeving. Je moet een responsief team hebben, dat zowel vóór een probleem zich aandient als bij acute calamiteiten direct hulp weet te bieden. Je monitort hybride IT-omgevingen en applicaties consequent en 24/7. Zero trust, schaduw-IT en een goed back-up- en disaster-recoveryplan hebben geen geheimen voor jou. Wij hebben een preselectie gemaakt van tools van de beste fabrikanten die specifiek software en clouddiensten ontwikkelen voor MSP's. Scheelt jou tijd. Wel zo makkelijk.

OOK JE KLANTEN HELPEN BIJ HET BESCHERMEN VAN HUN DATA?

Doing business is teamsport, daar geloven wij heilig in bij Portland. Het NIST-framework vertelt je wel wat een organisatie moet doen, maar niet voor welke oplossing ze moeten kiezen. Dat is waar jij je klanten bij kunt helpen en waar wij jou bij kunnen adviseren. Ben je geïnteresseerd in het optimaliseren van

jouw cybersecurity stack? Wij helpen je graag met het optimaliseren van je aanbod en selecteren van de meest passende SOC- of MDR-oplossing. Eén die 24/7/365 over je schouder meekijkt. Dus ook als je slaapt! Benieuwd hoe we dat doen? Neem vrijblijvend contact met ons op.

OVER PORTLAND

Taking care of your Managed Services en Reseller Business

Dat is wat wij doen, al 25 jaar. Portland helpt MSP's en VAR's om hun bedrijf efficiënt, productief en winstgevend in te richten. Wij zijn een platte organisatie met duidelijke en heldere lijnen, verantwoordelijkheden en verwachtingen. Wij blinken uit in persoonlijke aandacht. Het is onze missie het team te zijn achter de succesvolle IT-dienstverlener, die mkb'ers in de Benelux een cyberveilige werkplek biedt en blij maakt met slimme en gebruiksvriendelijke softwarediensten.

PLAN EEN ADVIESGESPREK

Leidsevaartweg 99
2106 AS Heemstede
Nederland

+3120 2144000
info@portland.eu
https://www.portland.eu

portland