De kracht van een geïntegreerde Zero Trust-oplossing

inetum

Een hoeksteen om aan de NIS2-richtlijn te voldoen

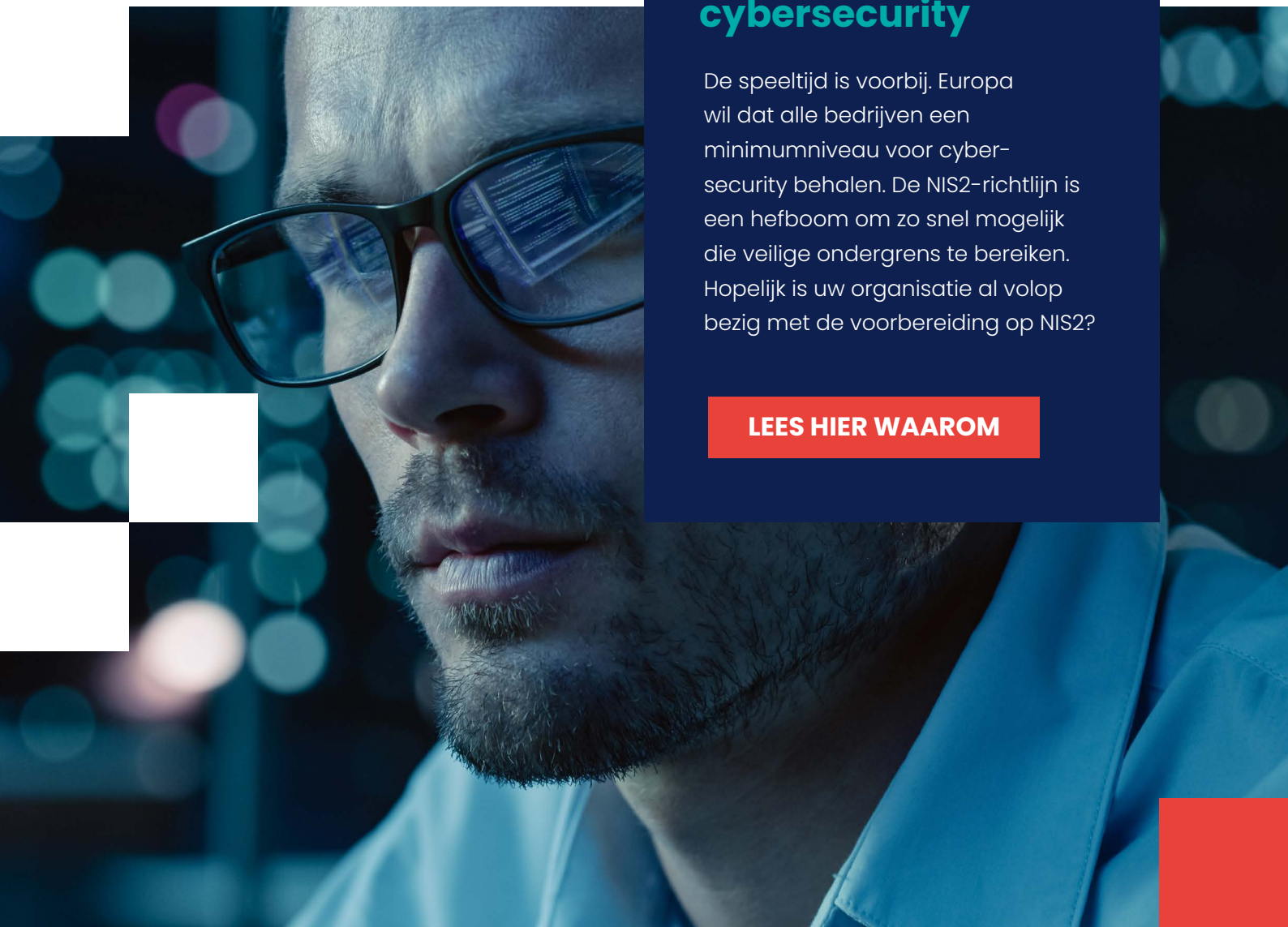
Terwijl de NIS2-richtlijn de lat voor cybersecurity hoger legt binnen de EU, biedt een Zero Trust-benadering een solide fundament om te voldoen aan die nieuwe normen. Ontdek hoe Zero Trust-principes niet alleen een duurzame beveiliging van uw digitale ecosystemen verzekeren, maar ook waarom het een essentieel onderdeel is om als organisatie aan de NIS2-richtlijn te voldoen

RECAP

NIS2: hefboom en accelerator voor cybersecurity

De speeltijd is voorbij. Europa wil dat alle bedrijven een minimumniveau voor cyber-security behalen. De NIS2-richtlijn is een hefboom om zo snel mogelijk die veilige ondergrens te bereiken. Hopelijk is uw organisatie al volop bezig met de voorbereiding op NIS2?

LEES HIER WAAROM



Cybersecurity roadmap

NIS2 stelt duidelijke eisen voor een brede waaier aan veiligheidsaspecten die de algehele weerbaarheid van organisaties verhogen. Het gaat onder andere om het effectief aanpakken van incidenten, het vormgeven van een stevige cybersecuritystrategie, en het waarborgen van de veiligheid van infrastructuur en software.

Bij Inetum bieden we een gestructureerde aanpak om prioriteiten te stellen en te navigeren door de vereisten van NIS2 via onze Cybersecurity Roadmap. In drie stappen brengen we de cyberveiligheidsmaturiteit van uw organisatie in kaart, identificeren we mogelijke zwakke plekken specifiek gerelateerd aan uw NIS2-implementatie en bieden we gerichte optimalisatievoorstellen aan.

De roadmap omvat zowel technische aspecten die via een grondige datascan opgehaald worden, als niet-technische aspecten die verzameld worden door een gerichte vragenlijst tijdens een workshop. Dit tweeledige proces zorgt ervoor dat elke dimensie van uw cybersecuritystrategie wordt geëvalueerd en versterkt.

Basishygiëne in cyberveiligheid

Artikel 89 is een cruciaal onderdeel van de NIS2-richtlijn. Het benadrukt het belang van 'Basic Cyber Hygiene', een verzameling kernpraktijken die cruciaal zijn voor het verbeteren van de veiligheid van een organisatie. **Het gaat onder andere om:**

BEVEILIGING VAN NETWERKEN EN SYSTEMEN

Het toepassen van maatregelen om de veiligheid en de weerbaarheid van netwerken en informatiesystemen te waarborgen.

RISICOANALYSE EN -BEHEER

Organisaties moeten regelmatig hun cyberbeveiligingsrisico's beoordelen en beheersmaatregelen implementeren op basis van deze risicoanalyse.

INCIDENTBEHEER

Het ontwikkelen en implementeren van procedures voor het effectief detecteren, melden en afhandelen van cybersecurityincidenten.

CONTINUÏTEIT VAN DE BEDRIJFSVOERING

Het waarborgen van de continuïteit van de dienstverlening, inclusief herstelplannen en -procedures na cyberaanvallen.

GEBRUIKERSBEWUSTZIJN EN TRAINING

Het regelmatig opleiden en bewust maken van medewerkers over cyberbeveiligingsrisico's en best practices.

BEVEILIGING VAN DE TOELEVERINGSKETEN

Het waarborgen van de beveiliging van de toeleveringsketen, inclusief de beveiligingseisen voor leveranciers en partners.

Zero Trust als basishygiëne

Het Zero Trust-principe speelt een belangrijke rol 'Basic Cyber Hygiene'. Deze benadering, die uitgaat van het principe "vertrouw nooit, verifieer altijd", is essentieel voor het creëren van een veilige digitale omgeving.

Zero Trust is een strategisch framework dat organisaties helpt om toegang tot hun netwerken en systemen te controleren en te beperken, ongeacht of de toegangspoging intern of extern plaatsvindt:

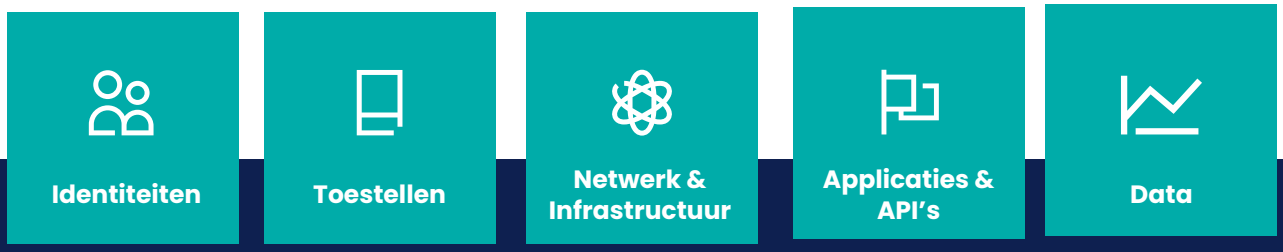
1.

Met de toename van remote werken, cloud computing en mobiele toegang, biedt Zero Trust een nieuwe manier van beveiliging. Door elke gebruiker en elk apparaat te verifiëren voordat toegang wordt verleend, minimaliseren organisaties het risico op datalekken en cyberaanvallen.

2.

Daarnaast stimuleert Zero Trust een cultuur van beveiligingsbewustzijn. Door constante monitoring en evaluatie van toegangsverzoeken en gebruikersgedrag, kunnen organisaties sneller reageren op verdachte activiteiten en potentiële bedreigingen.

De architectuur achter Zero Trust berust op 5 pijlers:



Wil je meer weten over die 5 pijlers van Zero Trust?

LEES DAN ONZE WHITEPAPER

Zero Trust-oplossingen van HPE Aruba

Geen enkele leverancier of oplossing kan alle cyberbeveiliging bieden die een organisatie nodig heeft. Om die reden kan het interessant zijn om te starten met een netwerk dat een ingebouwde basis biedt voor Zero Trust-beveiliging. Zo beperkt u het aantal tools die nodig zijn om aan de NIS2-vereisten te voldoen. **HPE Aruba heeft op dat vlak een interessant aanbod:**

1. NETWERK-SEGMENTATIE

Via HPE Aruba's Dynamic Segmentation kunnen organisaties netwerkverkeer scheiden op basis van identiteit en bijbehorende toegangsrechten, van edge tot cloud.

2. IDENTITEITS- EN TOEGANGSBEHEER

Met oplossingen zoals HPE Aruba Networking Central en ClearPass, biedt HPE Aruba AI-gestuurde zichtbaarheid en profilering van gebruikers en apparaten, waardoor organisaties een nauwkeurig beeld krijgen van wie en wat verbinding maakt met hun netwerken. Dit omvat authenticatie van een breed scala van identiteitsbronnen en gedetailleerde toegangsprivileges die de gebruiker en het apparaat volgen over alle soorten netwerken.

3. ZERO TRUST-BEVEILIGINGSPRINCIPES

HPE Aruba Networking bouwt op Zero Trust-principes, van edge tot cloud. Deze principes omvatten uitgebreide zichtbaarheid, authenticatie en autorisatie, minimaal noodzakelijke toegangsrechten, continue monitoring en beleidshandhaving.

4. SOFTWARE-UPDATES EN APPARAATCONFIGURATIES

HPE Aruba Networking Central vereenvoudigt de workflow voor het configureren van beheerde apparaten door beheerders in staat te stellen een set apparaten in groepen te combineren en te beheren, hetgeen zorgt voor efficiëntie en naleving van de nieuwste veiligheidsstandaarden.

Ervaar de kracht van een geïntegreerde Zero Trust-oplossing

Bij Inetum erkennen we de complexiteit en de uitdagingen die de NIS2-richtlijn met zich meebrengt voor organisaties. Het implementeren van Zero Trust-principes is niet alleen een fundamentele stap om te voldoen aan de NIS2-richtlijn, maar gidst uw organisatie ook naar een duurzame, veilige digitale omgeving.

Wij moedigen u aan om niet af te wachten, maar proactief te werk te gaan. De voorbereiding op NIS2 vereist tijd en aandacht voor detail, van het uitvoeren van een grondige cybersecurity assessment tot het ontwikkelen van een strategische roadmap die uw organisatie begeleidt naar een versterkte beveiligingsinfrastructuur.

NEEM CONTACT OP

Inetum
A. Vaucampslaan 42
1654 Huizingen, Belgium
+32 2 801 55 55
www.inetum-realdolmen.world

inetum | HPE aruba networking