nedscaper

// WHITEPAPER

Sterke Security, Tevreden Klanten

Hoe je als MSP beter aan de securityverwachtingen van je klanten voldoet.

NEDSCAPER
MANAGED EXTENDED
DETECT AND RESPOND
SYSTEM AQUIRE

// Inhoudsopgave

// Sterke Security, Tevreden Klanten

Het is de nachtmerrie van elke Managed Service Provider (MSP) en zijn klanten: losgeld moeten betalen aan cybercriminelen om weer toegang te krijgen tot eigen bestanden. De gevolgen zijn enorm en het herstel kan weken, zo niet maanden, duren. Maar hoe zorg je ervoor dat je de juiste kennis en middelen in huis hebt om dit te voorkomen? En nog belangrijker: hoe zorg je dat je klanten beschermd én tevreden blijven, zodat ze niet overstappen naar de concurrent? In deze whitepaper vind je de antwoorden.

De securityverwachtingen van klanten

Als MSP heb je te maken met de verwachtingen van je klanten op het gebied van cybersecurity. Hoewel klanten deze verwachtingen niet altijd expliciet uitspreken, gaan ze ervan uit dat hun systemen en data goed beschermd zijn. Ze verwachten dat alles geregeld is en rekenen erop dat jij de verantwoordelijkheid draagt voor hun digitale veiligheid. Vaak hoor je klanten zeggen: “Mijn IT-leverancier beheert mijn laptops en systemen. Die regelt alles, inclusief security. Maar of ik voldoende beschermd ben tegen ransomware? Geen idee…”

Tegelijkertijd lezen klanten steeds vaker over cyberdreigingen zoals malware, ransomware, CEO-fraude, phishingaanvallen en datalekken. Deze toenemende stroom aan informatie dwingt hen om serieus na te denken over de beveiligingsmaatregelen binnen hun organisatie. Daarnaast hebben ze te maken met wettelijke verplichtingen, zoals de Algemene Verordening Gegevensbescherming (AVG). Echter, het is voor veel klanten niet altijd duidelijk welke specifieke regels op hen van toepassing zijn, zoals de NIS2-richtlijn, wat de inhoud daarvan is en wat de consequenties zijn als ze deze niet naleven.

Waarom MSP’s extra moeten opletten

Als MSP ben je de sleutel tot de IT-omgeving van je klanten. Dit maakt jou een aantrekkelijk doelwit voor cybercriminelen. Als een hacker erin slaagt jouw systemen binnen te komen, kan hij via jouw netwerk eenvoudig toegang krijgen tot de systemen en gegevens van al je klanten. Dit betekent dat een succesvolle aanval op jouw bedrijf verstrekkende gevolgen kan hebben, niet alleen voor jou, maar ook voor alle organisaties die op jouw diensten vertrouwen.

Cybercriminelen richten zich steeds vaker op MSP’s omdat zij de ‘gateway’ zijn naar meerdere klanten tegelijk. In plaats van één bedrijf te hacken, kunnen ze door één MSP te hacken toegang krijgen tot de data van tientallen, zo niet honderden organisaties. Dit maakt het voor jou als MSP cruciaal om je beveiliging op het hoogste niveau te brengen.

// 4 uitdagingen waar MSP's tegenaan lopen

Hoewel een solide cybersecurityaanpak noodzakelijk is, lopen MSP's tegen verschillende uitdagingen aan die het lastig maken om te voldoen aan de verwachtingen van klanten en de eisen van nieuwe wetgeving. Hieronder bespreken we enkele van de grootste obstakels:

1 // Te kort aan personeel en expertise

De vraag naar cybersecurityprofessionals is veel groter dan het aanbod. Dit leidt tot een tekort aan gekwalificeerd personeel, waardoor veel MSP's moeite hebben om hun beveiligingsteams op sterkte te houden. Bestaand personeel raakt overbelast en heeft vaak niet de tijd of focus om beveiligingsincidenten effectief aan te pakken, wat het risico op fouten vergroot.

2 // Complexiteit van moderne cyberdreigingen

Cyberaanvallen worden steeds complexer en geavanceerder. Dit vraagt om gespecialiseerde kennis en tools om nieuwe dreigingen snel te kunnen detecteren en neutraliseren. Veel MSP's beschikken niet over de juiste middelen om deze technologieën bij te houden, waardoor ze kwetsbaarder worden.

3 // Beperkt budget

Niet alle MSP's hebben voldoende financiële middelen om te investeren in uitgebreide beveiligingsinfrastructuur, softwarelicenties, en trainingen voor hun personeel. Hierdoor ontstaat een tekort aan moderne tools en expertise, wat de kans op beveiligingslekken vergroot. Bovendien zijn trainingen en certificeringen vaak duur, waardoor MSP's terughoudend zijn om hierin te investeren.

4 // Compliance en regelgeving

Met de komst van de NIS2-richtlijn en andere wet- en regelgeving wordt het steeds lastiger voor MSP's om aan alle eisen te voldoen. De verplichtingen rondom risicobeoordelingen, incidentmeldingen en het nemen van passende beveiligingsmaatregelen vereisen veel kennis en inzet. MSP's die hier niet tijdig op inspelen, lopen het risico op sancties of boetes.

// Wat is NIS2 en waarom krijgt het nu extra aandacht?

In het licht van de toenemende digitale dreigingen is er binnen de Europese Unie gewerkt aan een aangescherpte richtlijn voor netwerk- en informatiesystemen: de NIS2-richtlijn. Deze richtlijn is gericht op het vergroten van de digitale en economische weerbaarheid van Europese lidstaten. Voor MSP's betekent dit dat zij verantwoordelijkheden krijgen, niet alleen voor hun eigen beveiliging, maar ook voor de beveiliging van hun klanten.

De NIS2-richtlijn is ontwikkeld om de digitale weerbaarheid van organisaties in Europa te versterken en wordt in Nederland in 2025 geïmplementeerd als de Cyberbeveiligingswet (Cbw). Deze wet legt organisaties, waaronder MSP's, nieuwe verplichtingen op, zoals risicobeoordelingen, passende beveiligingsmaatregelen en een meldplicht bij incidenten binnen 24 uur. De Rijksoverheid adviseert organisaties om nu al maatregelen te treffen, zoals het uitvoeren van een risicoanalyse, het nemen van passende maatregelen en het inrichten van procedures voor incidentenbeheer, zodat ze beter voorbereid zijn op deze wetgeving en huidige dreigingen.

NIS2 in het kort:

- Europese richtlijn voor versterking van cyberbeveiliging.
- Uitbreiding naar bredere sectoren, inclusief digitale diensten.
- Meer cyberdreigingen, noodzaak voor strengere beveiligingsmaatregelen.
- Verhoogde focus op risicobeheer en incidentrespons.
- Sancties en verplichtingen maken naleving kritischer voor bedrijven.

// 4 stappen om aan de security-verwachtingen van je klanten te voldoen

Om als MSP te voldoen aan de toenemende securityverwachtingen van klanten én wetgeving zoals de NIS2, moet je verschillende strategische stappen ondernemen. Dit begint bij inzicht in de risico's waarmee je klanten te maken hebben en het implementeren van passende beveiligingsmaatregelen.

1 // Ken je klant en hun risico's

Om een effectieve beveiligingsaanpak te bieden, moet je de specifieke behoeften en risico's van je klanten begrijpen. Dit begint met een risicoanalyse. Vraag jezelf af:

- Welke waardevolle gegevens en systemen moeten beschermd worden?
- Wat zijn de potentiële dreigingen en hoe verhoudt hun huidige beveiliging zich daartoe?
- Welke compliance-eisen zijn van toepassing op deze klant?

Met een risicoanalyse kun je beveiligingsmaatregelen aanpassen aan de behoeften van je klant, en zorg je ervoor dat je oplossingen biedt die écht relevant zijn.

2 // Zorg voor een solide basis in cybersecurity

Beveiliging begint bij de basis. Als MSP moet je ervoor zorgen dat je klanten de juiste fundamenten hebben voor hun beveiligingsstrategie. Hieronder volgen enkele essentiële maatregelen die je kunt implementeren:

- **Multi-factorauthenticatie (MFA):** implementeer MFA om het voor ongeautoriseerde gebruikers aanzienlijk moeilijker te maken om toegang te krijgen tot gevoelige gegevens of systemen.
- **Automatische detectie en respons (XDR):** maak gebruik van geavanceerde security-tools voor automatische detectie van verdachte activiteiten en het uitvoeren van tegenmaatregelen.
- **Security Service Edge (SSE):** implementeer een oplossing voor veilige toegang tot websites en applicaties, zodat je klant beschermd blijft, ook buiten hun eigen netwerk.

3 // Monitor continu je digitale omgeving

Cyberdreigingen zijn voortdurend in ontwikkeling, dus het is van cruciaal belang dat je klantensystemen 24/7 worden gemonitord. Door realtime monitoring kunnen beveiligingsexperts onmiddellijk ingrijpen wanneer een dreiging wordt gedetecteerd, waardoor de schade beperkt blijft.

4 // Transparante communicatie over security

Klanten willen de zekerheid dat hun data veilig is en dat hun continuïteit geborgd is. Zorg er daarom voor dat je duidelijk communiceert over welke maatregelen je neemt en waarom deze noodzakelijk zijn. Door transparantie te bieden, vergroot je het vertrouwen van je klant en voorkom je misverstanden.

// Werk samen met een securitypartner

Als je als MSP niet over de middelen of expertise beschikt om alle cybersecuritydiensten zelf aan te bieden, overweeg dan een samenwerking met een gespecialiseerde securitypartner. Door een partner zoals Nedscaper in te schakelen, krijg je toegang tot geavanceerde beveiligingsoplossingen zoals Managed Extended Detection en Response (MXDR). Dit zorgt ervoor dat je klanten altijd goed beschermd zijn, zonder dat je zelf grote investeringen hoeft te doen in eigen beveiligingsteams of infrastructuur. Een samenwerking biedt je:

- **Directe toegang tot expertise:** je hoeft geen dure interne beveiligingsexperts aan te nemen of op te leiden. Een ervaren partner neemt deze taak van je over.
- **24/7 monitoring en respons:** met een gespecialiseerde partner kunnen je klanten rekenen op constante monitoring en snelle actie bij incidenten.
- **Toekomstbestendige oplossingen:** partners zoals Nedscaper benutten de nieuwste technologieën en methodes, waardoor je klanten altijd up-to-date beveiligd zijn tegen nieuwe dreigingen.

Waarom Nedscaper's dienstverlening aansluit op de behoeften van MSP's

In een wereld waar cyberdreigingen steeds complexer worden en de druk om te voldoen aan regelgeving toeneemt, hebben MSP's behoefte aan betrouwbare, schaalbare oplossingen. Het tekort aan personeel en expertise, gecombineerd met de complexiteit van moderne dreigingen, maakt het voor veel MSP's moeilijk om aan de verwachtingen van hun klanten te voldoen. Hier komt Nedscaper in beeld. Met onze Managed Extended Detection and Response (MXDR) oplossing bieden wij de ondersteuning en tools die MSP's nodig hebben om hun klanten te beschermen en compliant te blijven.

Managed Extended Detection en Response van Nedscaper

Bij Nedscaper leveren we MSP's en hun klanten een volledig geïntegreerde cyberbeveiligingsoplossing, aangedreven door de toonaangevende tools van Microsoft. Ons Managed XDR-platform biedt 24/7 preventie, detectie van bedreigingen en respons, ondersteund door AI en een team van meer dan 80 beveiligingsspecialisten. Dit stelt je in staat om continu kwetsbaarheden te detecteren en direct in te grijpen wanneer dit vereist is, terwijl je klanten beschermd blijven tegen de steeds veranderende dreigingen in het cyberlandschap.

Wij zijn de grootste Microsoft-only Managed Security Services Provider (MSSP) in Nederland, wat ons een unieke positie geeft. Met onze Microsoft Verified Managed XDR Solution-status benutten we optimaal alle mogelijkheden van Microsoft. En mocht je onze samenwerking ooit willen beëindigen, dan blijf je toegang houden tot je zorgvuldig ingerichte Microsoft-omgeving.

// Conclusie: versterk je beveiliging en bescherm je klanten

Als MSP sta je voor de uitdaging om aan steeds hogere securityverwachtingen van klanten te voldoen en tegelijkertijd de toenemende eisen van wet- en regelgeving, zoals de NIS2-richtlijn, te navigeren. Door nu proactieve maatregelen te nemen, kun je ervoor zorgen dat je niet alleen je klanten optimaal beschermt, maar ook je eigen bedrijf future-proof maakt. Of je nu kiest voor een interne aanpak of samenwerkt met een gespecialiseerde securitypartner, het belangrijkste is dat je voorbereid bent op de steeds veranderende cyberdreigingen.

Cybersecurity is niet langer een optie, maar een noodzaak. Investeren in de juiste oplossingen en expertise is essentieel om het vertrouwen van je klanten te behouden en je concurrentiepositie te versterken

// Meer weten?

Ben je klaar om je cybersecurityaanpak naar een hoger niveau te tillen en je klanten nóg beter te beschermen? Nedscaper biedt gespecialiseerde beveiligingsoplossingen en ondersteuning om je daarbij te helpen. Neem vandaag nog contact op voor een vrijblijvend gesprek en ontdek hoe onze Managed Extended Detection en Response (MXDR) je kan helpen om voorop te blijven lopen.

+31 (0)20 299 9848

connect@nedscaper.com

// Over Nedscaper

Nedscaper is een gespecialiseerd cybersecuritybedrijf dat Managed Security Services biedt op basis van Microsoft-technologie, actief in Europa en Afrika. Met het eigen Managed XDR-platform en geavanceerde AI-gestuurde dreigingsdetectie beschermt Nedscaper bedrijven en overheidsorganisaties 24/7 tegen cyberdreigingen. Het MKB wordt bediend via haar partnernetwerk.

Nedscaper verzamelt beveiligingsgegevens uit hybride omgevingen, zoals on-premises infrastructuren, cloud, apparaten en gebruikers, en levert zo een naadloze, realtime verdediging tegen cyberaanvallen. Naast security-oplossingen biedt Nedscaper ook consultancy en zet het zich in voor de opleiding van jong talent, met een sterke focus op Zuid-Afrika.

Met kantoren in Amsterdam, Kaapstad en Johannesburg, en ondersteund door een breed partnernetwerk, blijft Nedscaper wereldwijd uitbreiden en draagt het bij aan een veiligere digitale wereld.