Wat de toenemende cyberdreiging van IT-dienstverleners vraagt

Schaal, ervaring en klantkennis essentieel voor succes

ING Research • Januari 2022

Inhoud

De laatste tijd komt het steeds vaker voor: bedrijven en organisaties die slachtoffer worden van een (geslaagde) cyberaanval. Zo werd in 2021 Kaseya, leverancier van remote management tools, slachtoffer van een ransomware-aanval. Hierdoor werden de systemen van vele organisaties via hun IT-dienstverlener besmet. Naast grotere organisaties die in het nieuws komen, zijn ook vele kleinere bedrijven het doelwit van cybercriminelen.

De toename van cyberaanvallen, en daarmee de behoefte aan cyberbeveiliging, roept de vraag op wat de dreiging betekent voor de IT-sector in algemene zin. Natuurlijk voor cyberspecialisten, maar nog interessanter: wat betekent het voor de algemene IT-dienstverlener, zoals managed service providers? Welke kansen liggen er? Wat is er voor nodig om die kansen te verzilveren? En zijn er ook bedreigingen? Op die vragen proberen wij in dit rapport antwoord te geven. De inhoud van dit rapport is naast desk research gebaseerd op interviews met verschillende spelers in de IT- en cybersecuritysector.

Inhoudsopgave

Beste kansen voor IT-dienstverlener met schaal, ervaring en klantkennis

Toenemende dreiging stuwt vraag naar cyberbeveiliging
De dreiging van cyberaanvallen wordt door digitalisering, en vergroting van de aanvalsmogelijkheden door de beweging van organisaties naar de cloud en de toename van het aantal met een netwerk verbonden apparaten gevoed. Daarnaast worden aanvallers steeds professioneler en zetten zij geavanceerde automatisering in. De toenemende cybersecuritydreiging levert in 2025 een Nederlandse cyberbeveiligingsmarkt op met een omvang tot € 11 miljard.

Groeikansen in monitoren uitdijend IT-landschap en bij machines
Na een focus op preventie liggen de komende jaren groeikansen in detectie, opvolging en herstel van de IT-infrastructuur. Vanwege het uitdijende, diverse IT-landschap is de behoefte aan overzicht groot. Daarnaast wordt de beveiliging van fysieke processen en machines belangrijk als steeds meer apparaten met het internet en netwerken verbonden zijn. Samenwerking met vendoren en verzekeraars versterkt daarbij de groeikansen.

Voorwaarden voor invullen behoefte door IT-dienstverlener
IT-dienstverleners kunnen voorzien in de toenemende beveiligingsbehoefte als zij inzetten op het vergroten van kennis en expertise op securityterrein, het zichtbaar maken wat de toegevoegde waarde van security in de totale dienstverlening is en aansprakelijkheid en verwachtingen van klanten managen.

Schaal, ervaring en klantkennis biedt beste kansen
De beste kansen voor succesvolle cybersecurity dienstverlening zijn voor bedrijven met schaal, ervaring en klantenkennis. Schaal is nodig om investeringen te dragen, zoals in een Security Operations Center, om gespecialiseerd personeel te kunnen hebben en als volwaardig partner van vendoren te opereren. Ervaring met security geeft een voorsprong omdat het tijd kost om expertise op te bouwen en partnerships met vendoren te ontwikkelen.

Ten slotte is diepe kennis over klanten een voordeel. Weten in welke richting de producten en dienstverlening van klanten zich ontwikkelt, wat dit betekent voor IT-landschap en specifiek voor de beveiliging ervan.
Deze IT-dienstverleners zijn in staat de juiste security oplossingen te implementeren en daar bovenop extra diensten te ontwikkelen zoals training van personeel en risicobeoordelingen.

Drijvende krachten voor groei van de uitgaven en kansen voor IT-dienstverleners in cybersecurity en de voorwaarden om dit te realiseren

Bron: ING Research

1. De stijgende kosten van cyberbeveiliging

1.1 Cybersecurity draait om bescherming van de hele keten

Cybersecurity beschermt complete keten
Cybersecurity draait om het beschermen en verdedigen van de complete keten van fysieke infrastructuur tot endpoints en mensen. Kern vormt de IT-infrastructuur bestaande uit onderling afhankelijke netwerken als internet, telecom en computer systemen, inclusief aan het netwerk verbonden apparaten en machines (end points). Het gaat daarbij vooral om bescherming tegen cyberaanvallen. Dit zijn aanvallen gericht op individuen of organisaties met als doel het verstoren, platleggen of de controle overnemen van IT-infrastructuur en hieraan gekoppelde operationele technologie (OT, fysieke systemen) of het stelen van informatie.

Gijzelsoftware momenteel grote dreiging
Een groot deel van de geslaagde cyberaanvallen draait om ransomware of gijzelsoftware. Hierbij nemen hackers de controle over van data of IT-infrastructuur van een organisatie. Daarna blokkeren ze de toegang met behulp van encryptie totdat losgeld is betaald. In veel gevallen wordt data ook gestolen, zogenoemde double extortion. Recent waren naast Media Markt ook Colonial Pipeline, JBS Foods, RTL Nederland, Mandemakers, VDL, ROC Mondriaan en honderden andere bedrijven en instellingen slachtoffer.

Vijf hoofdtaken in cyberbeveiliging waar projecten, processen, maatregelen en acties over zijn te verdelen

Vaststellen	Beschermen	Detecteren	Reageren	Herstellen
Bepalen welke processen en assets moeten worden beschermd	Ontwikkelen en implementeren van maatregelen ter bescherming	Ontwikkelen en implementeren van activiteiten om incidenten te ontdekken	Ontwikkelen en implementeren van activiteiten om de impact van incidenten te beperken	Ontwikkelen en implementeren van activiteiten om de processen te herstellen die geraakt zijn door een incident

Bron: NIST, ING Research

Stappen in een cyberaanval vanuit aanvalsperspectief

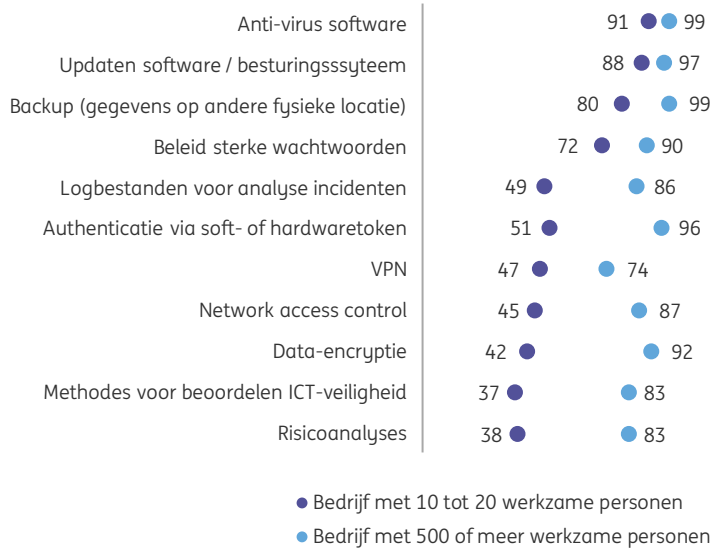
Voor aanval		Tijdens aanval				
Verkennen	**Bewapenen**	**Afleveren**	**Benutten**	**Installeren**	**Beheersen**	**Doelen uitvoeren**
Onderzoeken en selecteren van doelen en zwakheden	Zwakheden benutten door er malware voor te maken	De malware afleveren bij doelwit (bijv.via e-mail)	Toegang tot kwetsbare applicaties en systemen krijgen	Voortdurende toegang tot applicaties en systemen veiligstellen	Bredere controle nemen over het doelwit	Doelen uitvoeren (bijv. data stelen of versleutelen)

Bron: Lockheed-Martin, Cybersprint, ING Research

1.2 Kleinbedrijf minder goed voorbereid op cyberaanvallen

Kleinere bedrijven minder goed voorbereid
Ondanks de toename van cyberdreigingen lijkt een flink deel van het bedrijfsleven onvoldoende voorbereid. Kleinere bedrijven nemen het minst vaak veiligheidsmaatregelen, mede uit gebrek aan kennis, kostenoverwegingen en de inschatting van risico's. Kleine bedrijven denken onterecht dat ze geen doelwit zijn, maar het startpunt voor veel cybercriminelen is het scannen naar zwakheden. Vervolgens kijken ze wat daarmee te halen valt. Bovendien is een groot deel van hen voor cybersecurity afhankelijk van hun IT-leverancier, omdat zij zelf onvoldoende kennis in huis hebben.

Kleine bedrijven nemen minder vaak cybersecurity maatregelen
% van bedrijven dat maatregel neemt, 2020



Bron: CBS, ING Research N.B. groot is > 500 werkzame personen, klein 10 tot 20

1.3 Vijf tot zeven miljard euro uitgegeven aan cybersecurity

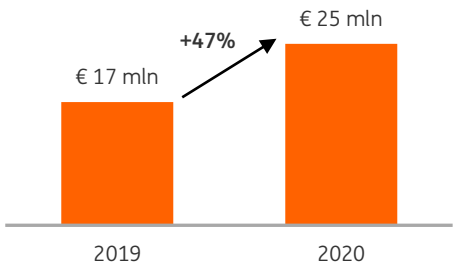
Tot € 7 miljard besteed aan cyberbeveiliging in Nederland
Een cyberaanval is nooit 100% te voorkomen, maar er zijn wel stappen te zetten om de kans op een succesvolle aanval te verkleinen:

- **Preventie**: De basis op orde hebben, dus zaken als software-updates, sterke wachtwoorden en multi-factor authenticatie.
- **Detectie en testen**: Monitoren van systemen op aanvallen en controleren hoe sterk de beveiliging is.
- **Trainen**: Specialisten bijscholen en kennis en besef van werknemers over veiligheidsrisico's vergroten.
- **Strategie en respons**: Plannen en backups hebben voor als een aanval toch slaagt.
- **Verzekeren**: De financiële schade van het resterende risico verzekeren.

Ongeveer 9-11% (Deloitte, Hiscox) van IT-budgetten gaat naar cybersecurity. Als percentage van de omzet lopen inschattingen uiteen van 0,2-0,5%. Voor Nederland betekent dit dat er naar schatting van ING Research € 5 tot 7 miljard wordt uitgegeven aan cybersecurity door organisaties (overheid en bedrijfsleven). Dit zijn de kosten van met name preventie, detectie, testen en trainen, los van verzekeringspremies en de schade bij een geslaagde aanval.

Verzekeringskosten beperkt tot € 25 miljoen
De totale door organisaties betaalde premie voor cyberverzekeringen bedroeg in 2020 25 miljoen euro, nog geen 0,2% van de totale premie-opbrengst van verzekeraars. Het aantal bedrijven met een cyberverzekering neemt toe, maar nog altijd is naar schatting maar zo'n 10% van de bedrijven verzekerd. Grotere bedrijven zijn vaker verzekerd. Uit een enquête van Hiscox onder bedrijven met in meerderheid meer dan 50 werknemers bleek dat 1 op de 5 een verzekering heeft. Het wordt voor bedrijven bovendien moeilijker om zich te verzekeren tegen de toenemende cyberaanvallen: dekkingen zijn lager, premies stijgen en voorwaarden worden aangescherpt.

Betaalde premies cyberriscoverzekeringen stijgen met 47%
Premie-omzet voor cyberrisicoverzekeringen in Nederland

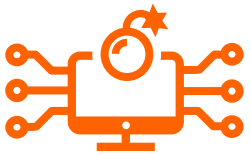


Bron: Verbond van Verzekeraars, ING Research

Schade loopt in de miljarden
De schade van een cyberaanval bestaat uit de kosten gemaakt om te reageren zoals detecteren en escaleren, op de hoogte stellen van en afwikkelen van schade met getroffenen en autoriteiten. De grootste post is echter het verlies aan 'business': omzet, klanten en kosten voor reputatieherstel. Minder concreet, maar wel relevant zijn de opportunity kosten zoals verlies van intellectuele eigendommen en reputatieschade. De hoogte van de schade verschilt sterk per type aanval en van organisatie tot organisatie. McAfee schat de wereldwijde schade van cyberaanvallen op € 830 miljard. Op basis van het aandeel in de mondiale economie komt de schade voor Nederlandse organisaties uit op € 8-12 mld.

8 tot 12 miljard euro

Geschatte schade van cyberaanvallen in Nederland

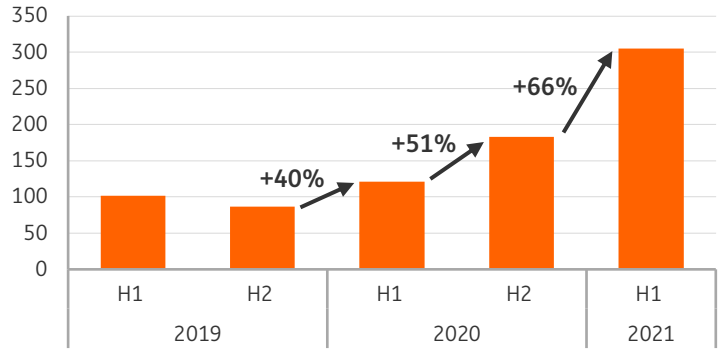


1.4 Stijging cyberaanvallen vraagt om meer uitgaven aan cyberbeveiliging

Dreiging blijft toenemen
Diverse bronnen laten een bijna voortdurende stijging zien in het aantal cyberaanvallen. Daarnaast wordt een toename in de vernuftigheid van aanvallen gerapporteerd. Vanwege de toenemende digitalisering van organisaties is een groter deel van de economie een potentieel doel. De toename van het aantal met internet verbonden apparaten en de groei van de cloud vergroten bovendien het aanvalsoppervlak (mogelijke aanvalspunten). Daarbij drijft de professionalisering van aanvallers, geringe pakkans en automatisering van aanvallen het aantal en de impact ervan op. Gezien de verdere digitalisering (met IoT en cloudgroei) en de financiële mogelijkheden van hackers om technologisch voorop te (blijven) lopen valt in de komende jaren een verdere toename van de cyberdreiging in kwantiteit en kwaliteit te verwachten.

Vooral ransomware groeit sterk
De laatste jaren zien we een toename van ransomware aanvallen. Naast vooruitgang in en de anonimiteit die cryptovaluta biedt bij de ontvangst van losgeld, is het vooral de professionalisering van cybercriminelen die voor een sterke groei zorgt. Het kopen van zero day exploits, een zwakke plek in software die nog onbekend is bij de software-ontwikkelaar, ligt inmiddels ook binnen hun financiële bereik. Er is sprake van een keten, met in elke schakel een specialisatie, waarin wereldwijd miljarden euro's omgaan. Voor organisaties is de schade veel groter dan eventueel betaald losgeld. Bovendien kost een geslaagde ransomware aanval zo'n 10% meer dan de gemiddelde cyberaanval.

Forse stijging ransomware aanvallen sinds 2020
Aantal aanvalspogingen in miljoenen en toename



Bron: SonicWall, ING Research

Toenemende dreiging leidt tot meer uitgaven aan preventie
De toenemende dreiging in het algemeen (en de stijging van relatief kostbare typen aanvallen zoals ransomware) drijven de schade van een geslaagde aanval op. Deze trend is al langer zichtbaar. De gemiddelde kosten van een data-inbreuk liggen in 2021 12% hoger dan in 2015 (Ponemon, 2021). Bovendien leidt dit tot een stijging in de uitgaven aan cyberbeveiliging. Een recente enquête onder chief information officers laat zien dat Nederlandse bedrijven jaarlijks 10% tot 25% extra uitgeven aan beveiliging (FD, 2juli 2021) . Naast inhuur van extra personeel gaat het geld bijvoorbeeld naar het continue monitoren van bedreigingen of verbetering van beveiliging in de cloud.

Ook betaald losgeld stijgt
Ransomware-groeperingen als REvil en Lockbit lijken hun opbrengsten niet alleen door frequentere aanvallen te verhogen. Unit42 van Palo Alto spreekt van stijgingen van de gemiddelde betaling met 171% in 2020 en 82% in de eerste helft van 2021. Het hoogste betaalde bevestigde bedrag in 2021 is $ 11 miljoen door vleesverwerker JBS. De losgeldeis ligt vaak tussen de 0,4% en 2% van de omzet (CVN). Toch maken de kosten van het losgeld maar een klein deel uit van de totale schade. De (financiële) pijn zit vooral in de downtime en het weer op orde krijgen van de systemen, zodat weer normaal zaken gedaan kan worden.

Bron: Cyberveilig Nederland, Palo Alto, Datto,

2. De rol van cybersecurity in de strategie van IT-dienstverleners

2.1 Focus op diensten binnen breed spectrum aan cybersecurity-oplossingen

Veel verschillende aanbieders veiligheidssoftware
De producten en diensten rondom cybersecurity zijn op te delen in software, services en hardware. Binnen software vallen de computerprogramma's die verschillende delen van het cyberlandschap beschermen. Nederland telt weinig grote vendoren van deze veiligheidssoftware, maar heeft met o.a. Compumatica, Guardian360, EclecticIQ en Cybersprint wel kleinere spelers. De mondiale markt is gefragmenteerd. De vele oplossingen van aanbieders leiden binnen afnemers tot een breed palet aan cybersecurity-oplossingen. Hierdoor ligt in het onvoldoende geïntegreerd zijn van cybersecurity software, weer een veiligheidsrisico.

Nederlandse cybersecurity specialisten gericht op diensten
De Nederlandse cybersecuritysector groeit snel. Tussen 2016 en 2021 is het aantal bedrijven in Nederland bijna verdubbeld. De cybersecuritysector is vooral gericht op diensten, zoals managed security services en consultancy. Managed security behelst het op afstand managen en/of monitoren van de IT security taken, informatie en applicaties. Dit gebeurt vaak via een Security Operations Centers (SOC's). Steeds meer organisaties zien veiligheid als integraal onderdeel van het IT landschap. Hierdoor, en vanwege de toenemende behoefte aan beveiliging, is cybersecurity vaker onderdeel van het aanbod van algemene IT-dienstverleners, zoals managed service providers (MSP's).

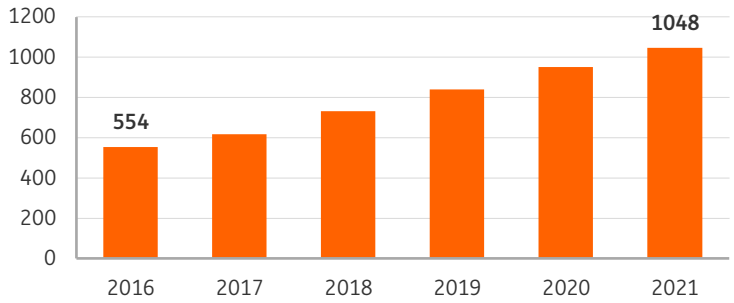
Cybersecurity producten en diensten verdeeld over software, diensten en hardware

	Soort dienstverlening	Voorbeeld
Software	Infrastructure / Network Security	VPN
	Platform / Information Protection	Secure web gateway
	Identity Access Mangement,	Authenticatie app
	Endpoint protection	Anti-virus software
Services	Managed Security Services	Apparaatbeheer
	Consulting	Cybersecurity strategie bepalen, incident response
	Implementation & Hardware support	Helpdesk
Hardware		Hardware firewall, proxy server

Bron: ING. Klik op de figuur voor uitleg van de termen.

Verschil in expertiseniveau securitydiensten
Er zijn grote verschillen in het expertiseniveau van securitydiensten. Basis security diensten zoals configureren, inregelen van zaken als firewall en authenticatie vragen een lager expertise niveau dan bijvoorbeeld continue monitoring, advisering en incident response. De basisdienstverlening is daarom toegankelijker voor algemene IT-dienstverleners.

Aantal cybersecuritybedrijven bijna verdubbeld
Aantal vestigingen van cybersecuritybedrijven



Bron: KvK, ING Research

2.2 Cybersecurity steeds vaker onderdeel van strategie van IT-dienstverleners

Strategie relevant voor eigen beveiliging en die van klanten
Cybersecurity is voor de strategie van IT-dienstverleners, zoals managed service providers (MSP's), vanuit zowel intern als extern perspectief relevant:

1. Security is een groeisegment, dus commercieel en financieel aantrekkelijk (extra omzet, hoge marges);
2. Steeds meer klanten verwachten dat cybersecurity integraal onderdeel is van het dienstenaanbod, en
3. Het is zeker voor IT-dienstverleners zaak de eigen, interne cyberveiligheid op orde te brengen en/of te houden.

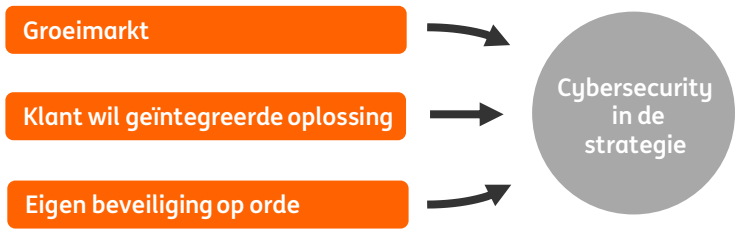
Dat laatste interne punt heeft ook weer een uitwerking op de beveiliging van klanten. Een aanval op de MSP kan immers leiden tot de besmetting van haar klanten, zoals bij de Kaseya en SolarWinds aanval gebeurde (ketenaanval). Cloud service providers krijgen bovendien te maken met regulering van cybersecurity voor clouddiensten (zie kader).

Levering cybersecurity diensten geen vanzelfsprekendheid
De eigen beveiliging moet altijd onderdeel zijn van de strategie, zoals voor elke andere organisatie geldt. Of cybersecurity ook onderdeel wordt van het dienstenaanbod is een tweede vraag. Er zijn namelijk verschillen tussen cybersecurity en het beheer van IT, waardoor de kennis, expertise, mensen en kijkwijze tussen beide verschilt. Bij cybersecurity ligt de focus op risico-inschattingen en veiligheid, terwijl het beheer van het IT-landschap vooral gericht is op de technische ondersteuning van de business en continuïteit. Dit maakt cybersecurity niet voor iedere IT-dienstverlener toegankelijk.

Bovendien kost het tijd en geld om te voldoen aan kennis- en andere vereisten die leveranciers stellen om hun beveiligingssoftware te mogen implementeren bij klanten.

MKB klanten rekenen op MSP voor hun beveiliging
Naast een sterke groei in de vraag naar cybersecuritydiensten en de noodzaak de eigen beveiliging op orde te hebben maken verwachtingen van klanten cybersecurity vaker onderdeel van de strategie. Klanten vragen namelijk om complete IT-oplossingen, inclusief cybersecurity. Hier liggen kansen voor de MSP. Vanwege de digitale transformatie en ook door thuiswerken zijn MKB-klanten in toenemende mate afhankelijk van hun MSP. Ze kijken ook naar de MSP voor security want ze kunnen dit meestal niet zelf. Hier is wel een verschil tussen MSP met MKB klanten en IT-dienstverlener voor grootbedrijf: Bij grotere organisaties is meer ruimte voor eigen security specialisten.

Drie belangrijke drivers voor cybersecurity in de strategie van een IT-dienstverlener



Invulling Europese regels rondom cybersecurity van clouddiensten stuit op bezwaren
ENISA het cyberveiligheidsagentschap van de EU heeft in concept gedetailleerde regels voor certificering van clouddiensten opgesteld. Deze regels worden op termijn verankerd in wetgeving, maar stuiten op bezwaren vanuit Nederland. Zo gaan ze niet uit van internationaal gangbare cloud beveiligingsstandaarden, maar de specifieke aanpak in Frankrijk en Duitsland. Verder worden drie niveaus van beveiliging beoogd: basis, hoog en substantieel. In de praktijk zal het lastig werken zijn met een certificering lager dan substantieel. Voor een aanbieder is het op beveiligingsniveau van de cloud voor verschillende klanten differentiëren namelijk niet haalbaar, waardoor het basisbeveiligingsniveau al snel afvalt. Bovendien beperkt een lager dan het hoogste beveiligingsniveau de kansen bij (publieke) aanbestedingen. De gedetailleerde regels drijven daarnaast de kosten van het auditen op. Verwacht wordt dat bestaande certificeringen zoals ISO relevant blijven. De precieze impact op cloud service providers hangt af van hoe de regels uiteindelijk precies ingevuld worden, maar voor kleinere spelers lijkt het moeilijker te worden hun diensten aan te bieden.

2.3 In de komende jaren cybersecurity integraal onderdeel van strategie

Cybersecurity integraal onderdeel dienstverlening MSP
Cybersecurity krijgt de komende jaren een prominente rol in de strategie van IT-dienstverleners. Nu zijn zaken als uptime van systemen en de beschikbaarheid van het netwerk de standaard diensten. Straks verwachten MKB-klanten dat de MSP bijvoorbeeld ook risico's kan identificeren en indammen. MSP's die cybersecurity niet in hun strategie meenemen, vergroten hun kennisachterstand op het vlak van cyberbeveiliging of weten niet de juiste partners aan te haken. Hierdoor verwachten klanten meer dan er geleverd kan worden.

Succesvolle MSP's van de toekomst richten zich op security als integraal deel van de dienstverlening om zo hun MKB-klanten goed te bedienen. Voor IT-dienstverleners die grotere klanten bedienen ligt uitbreiding naar levering van efficiënte basis security voor de hand. Daarbij moeten ze waken voor overschatting van eigen kunnen. Indien de expertise en tools ontbreken (en niet opgebouwd kan worden), is samenwerking met security specialisten nodig. Dit geldt met name voor beveiligingsdiensten met een hoger expertiseniveau.

Uitdaging om MKB-klant toegevoegde waarde van security te tonen
Centrale uitdaging voor MSP's is de klant duidelijk te maken waar deze precies voor betaalt. Het toevoegen van security diensten verhoogt immers de kosten (en prijs) voor eindgebruikers. Als klanten niet inzien dat ze beter beschermd zijn en wat dit hen oplevert, accepteren ze de hogere prijs niet. Een prijskopende / -gevoelige klant gaat dan mogelijk verloren aan MSP met een minder veiligheidsaanbod en een scherpere prijs. Daarbij speelt ook nog een paradox: Als je bedreigingen buiten de deur houdt, is het misschien wel lastiger om waarde te tonen.

In elk geval moet de IT-dienstverlener duidelijk maken wat wel en niet beveiligd is, welke oplossingen mogelijk zijn en dat daarbij een afweging tussen enerzijds kosten of operationele beperkingen en anderzijds extra beveiliging nodig is. Multifactor authenticatie leidt bijvoorbeeld tot een hoger veiligheidsniveau, maar ook tot extra handelingen voor werknemers. Vervolgens moeten afspraken en afwegingen goed worden vastgelegd, ook om aansprakelijkheid in te perken. MSP's zijn namelijk al met succes aansprakelijk gesteld voor schade uit cyberaanvallen op klanten.

93% van de MSP's overweegt security dienstverlening uit te breiden

Bron: Kaspersky

3. IT-dienstverlener kan in toenemende behoefte aan cyberveiligheid voorzien

3.1 Dreiging, digitalisering en connectiviteit leiden tot uitgavengroei cybersecurity

Groter risico betekent intensivering beveiliging

De professionalisering en automatisering van cyberaanvallen leiden tot een verbreding van de groep potentiële slachtoffers. In combinatie met verdere digitalisering is het onvermijdelijk dat de risico's op een cyberaanval stijgen. De toename in dreiging en in meer succesvolle aanvallen leiden tot meer uitgaven aan preventie. Incidenten bij de organisatie zelf en/of bij andere bedrijven werken als een trigger om meer te investeren in beveiliging. Zo geeft in een onderzoek van Kaspersky bijna een kwart van de bedrijven aan dat zij klant werden van een MSP als gevolg van gegevensdiefstal.

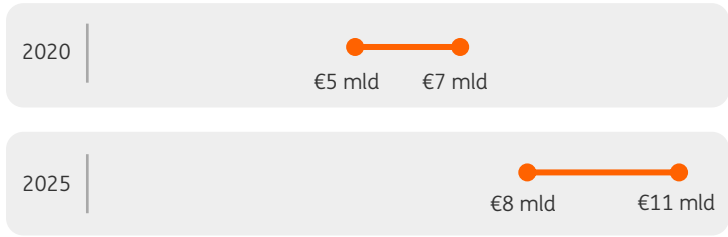
Bestedingen aan cybersecurity stijgen

De komende jaren nemen de bestedingen aan cyberbeveiliging verder toe. In 2025 geven bedrijven en andere organisaties in Nederland naar schatting € 8 tot 11 miljard uit aan hun beveiliging, tegen € 5 á 7 miljard in 2020. Drijvende krachten achter de hogere uitgaven zijn, naast een stijgende dreiging:

- de verdere digitalisering van de samenleving en specifiek beweging naar (opslag van data in) de cloud;
- de toename van het aantal met internet verbonden apparaten, zoals sensoren en industriële machines.

Uitgaven aan cybersecurity in Nederland stijgen naar € 8-11 miljard in 2025

Schatting omvang bestedingen aan cyberbeveiliging door Nederlandse organisaties*



* Omvang in 2025 gebaseerd op groeivoet van 10%, die is afgeleid van groeiramingen voor de (wereldwijde) cybersecuritymarkt van verschillende onderzoeksbureaus zoals bijv. Gartner.
Bron: ING Research

3.2 Groei via samenwerking en het betreden van nieuwe markten

Voor IT-dienstverleners liggen groeikansen in verbreding van de markt en het aanboren van nieuwe markten. MSP's versterken daarbij hun groeikansen door samenwerking met vendoren en verzekeraars te zoeken.

Monitoren van uitdijend IT-landschap biedt groeikansen
De security dienstverlening groeit de komende jaren sneller dan die van producten (software) omdat organisaties vaker hun beveiliging uitbesteden. De afgelopen jaren lag de focus bij organisaties, zeker in het MKB, op preventie. Voor detectie, opvolging en herstel was minder aandacht. Groeikansen liggen daarom in het (voortdurend) managen en monitoren van applicaties en onderdelen van de IT-infrastructuur op kwetsbaarheden. Vanwege het uitdijende, diverse IT-landschap is de behoefte aan overzicht groot.

Cybersecurity van industriële machines nieuwe markt
Waar nu de nadruk veel op beveiliging van IT ligt, komt daar de komende jaren de beveiliging van operationele technologie (OT) bij. Deze beveiliging van fysieke processen en machines wordt relevanter nu steeds meer apparaten met het internet en netwerken verbonden zijn. Daarbij komt dat software op machines minder vaak wordt geupdate (gepatcht), uit vrees processen stil te moeten leggen. Dit maakt bedrijven kwetsbaar voor aanvallen via machines. Het marktsegment cybersecurity van industriële apparaten is nu nog klein, maar zal de komende jaren groeien. Machinebouwers zelf zijn ook actief op deze markt, maar integratie van machinebeveiliging in de totale cyberbeveiliging is daarbij een uitdaging.

Fijnmazig netwerk kracht van MSP
Grote vendoren verbreden hun aanbod door meer functionaliteiten toe te voegen aan bestaande producten en zo uiteindelijk complete security platformen aan te bieden (zie kader). Dit verbrede aanbod is een antwoord op de wens van klanten om minder verschillende soorten security software te gebruiken (vendor consolidation). Het voorkomt dat de klant zelf de verschillende security oplossingen moet integreren en zorgt voor meer overzicht. Voor MSP's en andere IT-dienstverleners betekent dit dat partnerships met grote vendoren belangrijker worden. Zelf platformen ontwikkelen lijkt geen haalbare kaart. Zij bezitten echter wel het fijnmazige netwerk om MKB klanten direct te bedienen (waar het vendoren aan ontbreekt) en zo de platform oplossing van de vendor en hier op gebaseerde eigen diensten aan te bieden.

Via verzekeraar klantengroep uitbreiden
Verzekeraars en hun tussenpersonen kunnen belangrijke partners zijn in de groei op cybersecurity gebied. Zij kopen voor polishouders incident response diensten in bij cyberspecialisten. Daarnaast stimuleren zij het op orde brengen van security van klanten doordat polisvoorwaarden minimale security vereisten bevatten. Als een bedrijf niet aan de eisen voldoet, moet dit opgelost worden of er is bijvoorbeeld een bredere cyberrisico-inschatting nodig. Verzekeraars kiezen er gezien de benodigde specialistische expertise vaak voor om samen te werken met een leverancier van cybersecurity diensten. De samenwerking met verzekeraars werkt twee kanten op omdat klanten van de MSP op cybervlak met restrisico's zitten die ze kunnen laten verzekeren.

Vendoren zetten in op verbreding en platformisering
Grotere vendoren van security software proberen vaker een geïntegreerd aanbod van software en diensten te leveren. Dat aanbod wordt tegelijkertijd breder doordat stand alone producten, zoals een firewall, meer functionaliteiten, bijvoorbeeld een scan op malware, toevoegen. In de meest verregaande vorm wordt een platform aangeboden dat een range aan voorheen individuele security producten van anti-virus tot analyse tools en geautomatiseerde probleemoplossingen integreert.

XDR (extended detection and response) is een volgende stap in verbetering van dreigingsdetectie en snelheid van opvolging. Het vergelijkt data en alerts uit verschillende beveiligingslagen en levert zo een centraal overzicht van incidenten en de mogelijkheid te reageren, waardoor de hele attack surface gemonitord wordt.

Bronnen

Acunetix, Web application attack
Allied Market Research (2020), Cyber Security Market - Global Opportunity Analysis and Industry Forecast, 2020-2027
CBS (2020), Cybersecuritybedrijven in Nederland
CBS (2021), Cybersecuritymonitor 2020
Crowdstrike, Cybersecurity 101
CyberSecurity Raad (2021), Adviesrapport Integrale Aanpak Cyberweerbaarheid
Cyberveilig Nederland, Whitepaper Ransomware
Computer Economics (2021), IT Spending and Staffing Benchmarks
Deloitte (2021), Reshaping the cybersecurity landscape
ENISA (2021), ENISA Threat Landscape 2021
FD (2021), Spionage uit China en Rusland jaagt IT-kosten bedrijven omhoog
Gartner (2021), Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021
Hisxcox (2019), Cyber Readiness Report
Hisxcox (2020), Cyber Readiness Report
Hisxcox (2021), Cyber Readiness Report
IDC (2021), Europe IT Security Spending to Jump 8.3% in 2021, According to IDC
Infocyte, Cybersecurity 101
Kaspersky (2021), MSP market focus in 2021
McAfee (2020), The Hidden Costs of Cybercrime
Mordor Intelligence (2021), Global Cybersecurity Market (2021-2026)
NCTV (2021), Cybersecuritybeeld Nederland
Palo Alto / Unit 42 (2021), Extortion Payments Hit New Records as Ransomware Crisis Intensifies
Ponemon (2021), Cost of a Data Breach Report 2021
Simmons, Shiva, Singh Bedi en Dasgupta (2014), AVOIDIT: A Cyber Attack Taxonomy,
Sonic Wall (2021), Cyber Threat Report
The Hague Center for Strategic Studies (2016), Dutch Investments in ICT and Cybersecurity
Technavio (2020), Global Information Security Products and Services Market 2021-2025

Dit kan u ook interesseren

AI vindt zijn weg naar alle sectoren
Artificiële intelligentie biedt meeste waarde voor de IT-sector

Further efficiency gains vital to limit electricity use of data
How to limit the climate impact of an increasingly data-hungry world

Digitalisering in het hoger onderwijs
Niet voor de kosten, wel voor de kwaliteit

Meer weten?

Sector Banker TMT/ICT
Samantha Reilly
+31 630529129
samantha.reilly@ing.com

Senior econoom / Auteur van de publicatie
Ferdinand Nijboer
ING Research
+31 65185 2971
ferdinand.nijboer@ing.com

Met dank aan

Beate Zwijnenberg	ING
Sebastiaan Bosman	Cybersprint
Pieter Jansen	Cybersprint
Vincent Thiele	Cybersprint
Petra Oldengarm	Cyberveilig Nederland
Dave Maasland	ESET Nederland
Fred Streefland	Hikvision
Emiel Havinga	MKB Fonds
Pim Takkenberg	Northwave
Michiel Steltman	Online Trust Coalitie, DINL
Wilco de Haan	Schouten Zekerheid
Eugène Tuijnman	SLTN

Redactieraad

Katinka Jongkind	ING
Maurice van Sante	ING
Lex Hoekstra	ING

Kijk op ing.nl/kennis en volg ons op Twitter