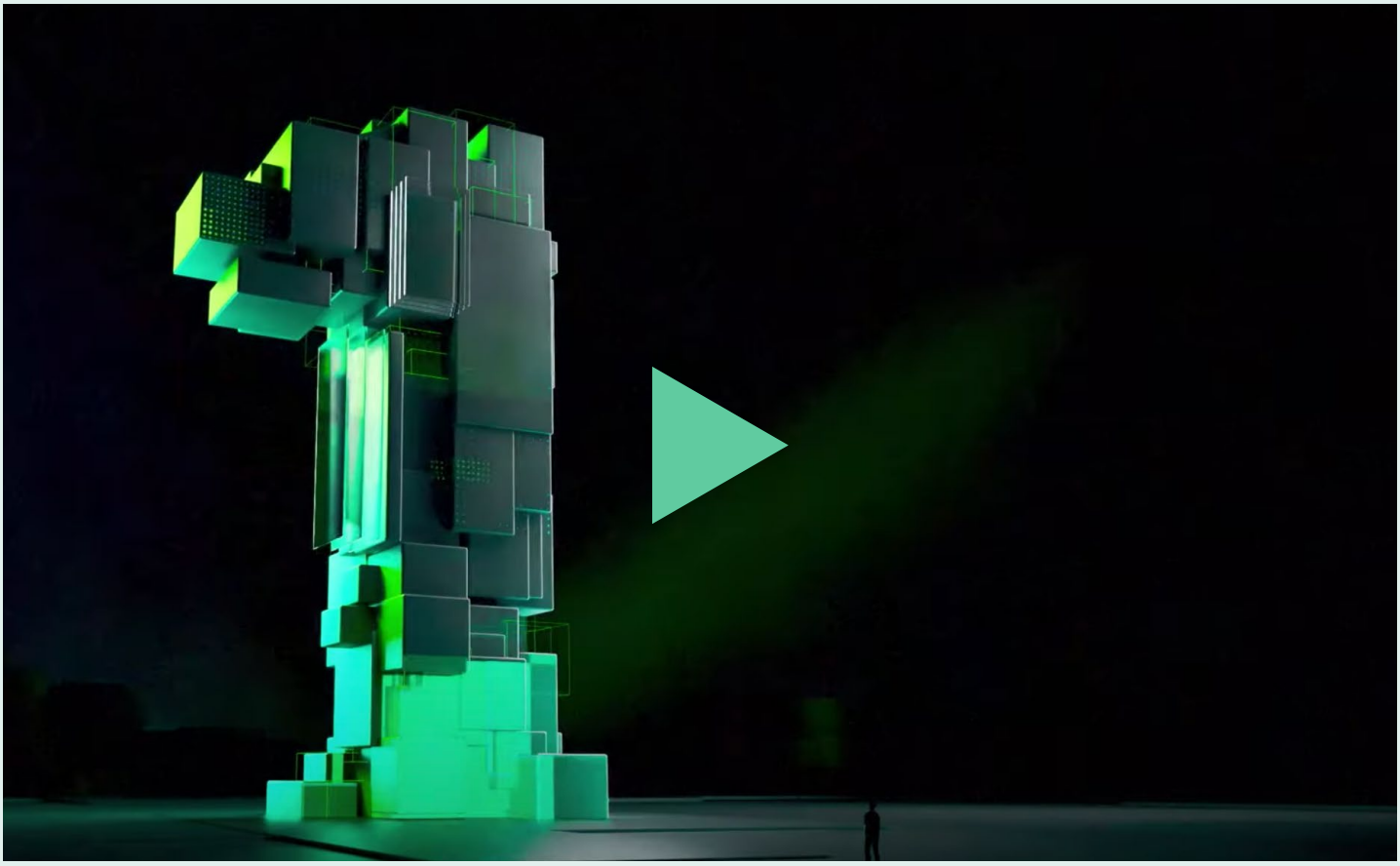
Inzichten over cybersecurity die jij als proactieve, zakelijke besluitvormer moet hebben

Oktober 2021

kaspersky BRING ON THE FUTURE

Inhoud

1. Video "Kaspersky Enterprise Security: Eén cybersecuritypartner ziet het grote plaatje"



2. Voorwoord: Inzicht van experts toevoegen aan geautomatiseerde cybersecurity

APT's, gerichte aanvallen, aanvallen op de supply chain, meer apparaten in gebruik, cloudservices en het 'Internet of Things'... De wereld van cyberdreigingen en aanvalpunten wordt complexer dan ooit en evolueert snel.

Volgens bedrijven vormt een gebrek aan bronnen, regels en expertise het grootste obstakel voor een adequate cyberbeveiligingsstrategie. Traditionele endpointbeveiliging volstaat niet langer om cyberdreigingen snel te detecteren en er juist op te reageren en om de bescherming van de belangrijkste bedrijfsmiddelen te garanderen. Maar wat is essentieel om bedrijven tegen cyberdreigingen te beschermen?

Besluitvormers hebben een actuele, diepgaande en uitgebreide kennis nodig over cyberdreigingen, gerelateerde cyberincidenten en het dreigings-landschap. Moderne bedrijven moeten worden ondersteund door de nieuwste dreigingskennis van overal ter wereld, zodat ze zelfs immuun kunnen blijven voor ongeziene cyberaanvallen. Ze streven naar een verenigde structuur die alles doet: een geïntegreerde toolkit die bedreigingen op verschillende niveaus opspoort, beveiligt meerdere ingangspunten vanuit één plaats.

Besluitvormers van kleine, middelgrote en grote ondernemingen moeten zowel problemen in verband met cyberbeveiliging als hun behoeften binnen hun organisatie proactief aanpakken. Als ze dit niet doen kunnen ze te maken krijgen met een snel groeiend probleem dat moeilijk te controleren valt.

Dit rapport is bedoeld om senior managers te ondersteunen in het sturen van de beveiliging van al hun belangrijke bedrijfsmiddelen. Het presenteert

de nieuwste markttendensen, de voornaamste pijnpunten en een stap-voor-stap-checklist. Geen geekpraat, maar een uitgebreid overzicht met must-have inzichten voor besluitvormers.

Laten we met dit in gedachten aan de slag gaan. Laten we eens een kijkje nemen naar de cybersecuritypartner die het grote geheel ziet, zodat jij je zorgeloos kunt concentreren op innovatie.

Tim de Groot
Territory Manager Benelux & Nordics, Kaspersky

3. Survey Report Europe – Waarom zakelijke besluitvormers cybersecurity proactiever moeten aanpakken

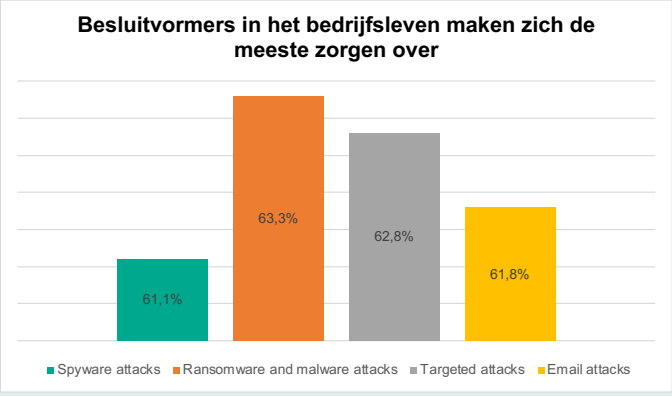
Het instituut voor marktonderzoek Gartner voorspelt dat driekwart van alle CEO's tegen 2024 persoonlijk verantwoordelijk zal worden gehouden voor cyberbeveiligingsincidenten in bedrijven. Dit maakt het onontbeerlijk voor organisaties om beveiligingsmaatregelen tegen cyberdreigingen proactief te versterken.

Een recent onderzoek van Kaspersky toont aan dat zakelijke besluitvormers beveiligingsmaatregelen willen versterken, maar nog wel wat werk voor de boeg hebben. Volgens de studie zou 61% van de Europese zakelijke besluitvormers cybersecurity binnen hun bedrijf proactiever wil aanpakken, maar daar niet voldoende gespecialiseerde kennis voor heeft. Verder vormen een gebrek aan bronnen en expertise en de kostendruk vaak een hindernis voor senior managers, omdat ze de nodige investering om het niveau van beveiliging binnen hun bedrijf te verhogen, in de weg staan.

Methodologie: De studie werd in augustus 2021 namens Kaspersky uitgevoerd door Arlington Research. 1500 zakelijke besluitvormers in Europa werden online bevraagd: Duitsland, Groot-Brittannië, Frankrijk, Italië, Spanje en Tsjechië, 250 bevraagden per land. 62% van de bevraagde besluitvormers is tewerkgesteld in kleine en middelgrote bedrijven met 50 tot 999 werknemers; 38% werkt in grote bedrijven met meer dan 1000 werknemers.

3.1. Twee op de drie Europese besluitvormers maken zich zorgen over cyberdreigingen

Bijna twee derde van de Europese zakelijke besluitvormers (62,7%) vreest het slachtoffer te worden van een cyberaanval, ongeacht of ze voor een groot bedrijf (64,6%) of een klein tot middelgroot bedrijf (61,6%) werken.



Gemiddeld zijn managers, wiens bedrijf reeds het slachtoffer is geweest van een cyberaanval, meer geneigd om zich zorgen te maken (tien

procentpunten meer). Meer dan driekwart (78,5%) had namelijk al een of meer aanvallen meegemaakt. Bijna één vijfde (17,8%) geeft aan dat zijn/haar bedrijf tot nu toe gespaard is gebleven aan cyberaanvallen.

3.2. Zakelijke besluitvormers: Staatsbescherming tegen cyberdreigingen ontoereikend

Wanneer we het slachtoffer zijn van diefstal in het echte leven, komt de politie ons meestal redden. Al vele jaren lang bestaan er in Europese landen duidelijke wetten en regels die van toepassing zijn op alle gebieden van het leven en die individuen en bedrijven beschermen.

Helaas is de situatie met cybercrime helemaal anders. Volgens de meest recente studie gelooft bijna twee derde (63%) van de Europese besluitvormers dat door cyberdreigingen getroffen organisaties niet dezelfde bescherming en ondersteuning krijgen als slachtoffers van 'misdaden in het echte leven'.

De Europese Algemene Verordening Gegevensbescherming (AVG) beschermt de persoonsgegevens van klanten, maar legt de verantwoordelijkheid voor de bescherming ervan wel bij het bedrijf. Organisaties van elke omvang gaan een dubbele uitdaging tegemoet: enerzijds bedreigen cyberaanvallen hun eigen bedrijf en klantgegevens, anderzijds maken de richtlijnen van de EU omtrent gegevensbescherming hen verantwoordelijk voor mogelijke beveiligings-incidenten.

- Het is niet verwonderlijk dat 61,2% van de bevraagde zakelijke besluitvormers kritiek had op de ondersteuning van de staat voor bedrijven in hun land.
- Zeven op de tien (70,1%) vindt dat misdaden in de cyberwereld even zwaar gestraft moeten worden als misdaden in het echte leven.
- 62% is bezorgd om de mogelijkheid dat ze in de toekomst te maken krijgen met persoonlijke vervolging omwille van beveiligingsincidenten in hun eigen bedrijf (zie studie van Gartner).

Managers melden ook een gebrek aan interne ondersteuning: meer dan de helft van de bevraagden (55,5%) maakt zich zorgen om de preventie van beveiligingsincidenten binnen hun eigen bedrijf.

"Zakelijke besluitvormers moeten hun gingsmaatregelen tegen cyberaanvallen versterken om hun bedrijf een veilige toekomst te bieden. Een efficiënte manier om dit te bereiken, is door technologie die cyberdreigingen automatisch detecteert en neutraliseert, te combineren met externe ondersteuning van ervaren experts op het gebied van cybersecurity. Dit geeft het interne IT-team de ruimte om zich bezig te houden met de hoofdtaken van het bedrijf."

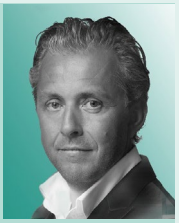
Tim de Groot, Territory Manager Benelux & Nordics, Kaspersky

3.3. Kostendruk en een gebrek aan middelen verhinderen investeringen in cybersecurity

De vraag blijft: Waarom, gezien de complexe dreigingssituatie, gedragen zo veel bedrijven zich passief in de implementatie van proactieve maatregelen voor cybersecurity?

Het antwoord heeft veel te maken met de alomtegenwoordige kostendruk, ongeacht of de respondenten voor grote bedrijven of kleine en middelgrote bedrijven werken.

In de context van de studie bevestigde meer dan de helft van de zakelijke besluitvormers (56,1%) dat ze graag zouden terugvallen op externe experts op het gebied van cybersecurity. Helaas hebben ze niet voldoende middelen om een betrouwbare partner te vinden. Voor 54,3% van de respondenten is het heel moeilijk om budgetten voor verbeterde cybersecurity te krijgen binnen hun bedrijf.



"Er zijn vaak discrepanties tussen de (waargenomen) behoeften van zakelijke besluitvormers en wat IT- en beveiligingsteams werkelijk nodig hebben. Een gebrek aan gespecialiseerde kennis beïnvloedt hier de besluitvorming. De oplossing ligt voor de hand: hoe meer besluitvormers op proactieve wijze investeren in bescherming tegen cyberdreigingen, hoe groter de positieve impact is op de toekomstige veiligheid van het bedrijf."

Tim de Groot, Territory Manager Benelux & Nordics, Kaspersky

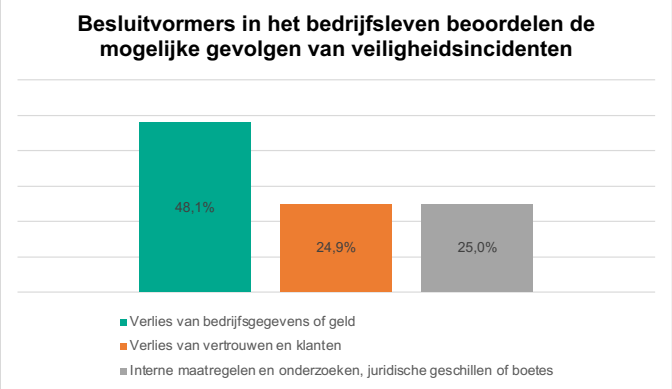
3.4. Cyberaanvallen hebben ernstige gevolgen

Cyberdreigingen worden steeds complexer, evolueren voortdurend en bedreigen de prestaties van bedrijven. Een op de tien beveiligingsincidenten wordt geclassificeerd als ernstig, of het nu gaat om malware, gerichte aanvallen, of aanvallen op bevoorrading.

De zakelijke besluitvormers die voor de studie zijn geïnterviewd, beoordelen de mogelijke gevolgen van beveiligingsincidenten op een verschillende manier:

- Een op de twee beschouwt het verlies van bedrijfsgegevens of -geld (48,1%) als het ergste gevolg van een mogelijke cyberaanval. Volgens een vierde van de respondenten (24,9%) is het verlies van vertrouwen en klanten het zwaarste gevolg. Ongeveer evenveel respondenten (25%) zien interne maatregelen en onderzoeken, juridische geschillen of boetes als het ergste gevolg van een beveiligingsincident

- Slechts een derde (36,7%) van de zakelijke besluitvormers is ervan overtuigd dat de interne beveiligingsmiddelen volstaan om cyberdreigingen succesvol af te weren. 61,8% van de deelnemers aan het onderzoek denkt dat hun organisatie ten minste voor een deel moet vertrouwen op de hulp van externe experts in het geval van een beveiligingsincident



3.5. Hoe zakelijke besluitvormers vandaag proactief reageren op cyberdreigingen

Dit is een andere reden waarom besluitvormers zichzelf moeten afvragen of hun investering in de preventie van cyberaanvallen groot genoeg is om het hoofd te bieden aan alle dreigingen. En of ze geen probleem hebben met het feit dat ze achterstaan op het gebied van state-of-the-arttechnologie.

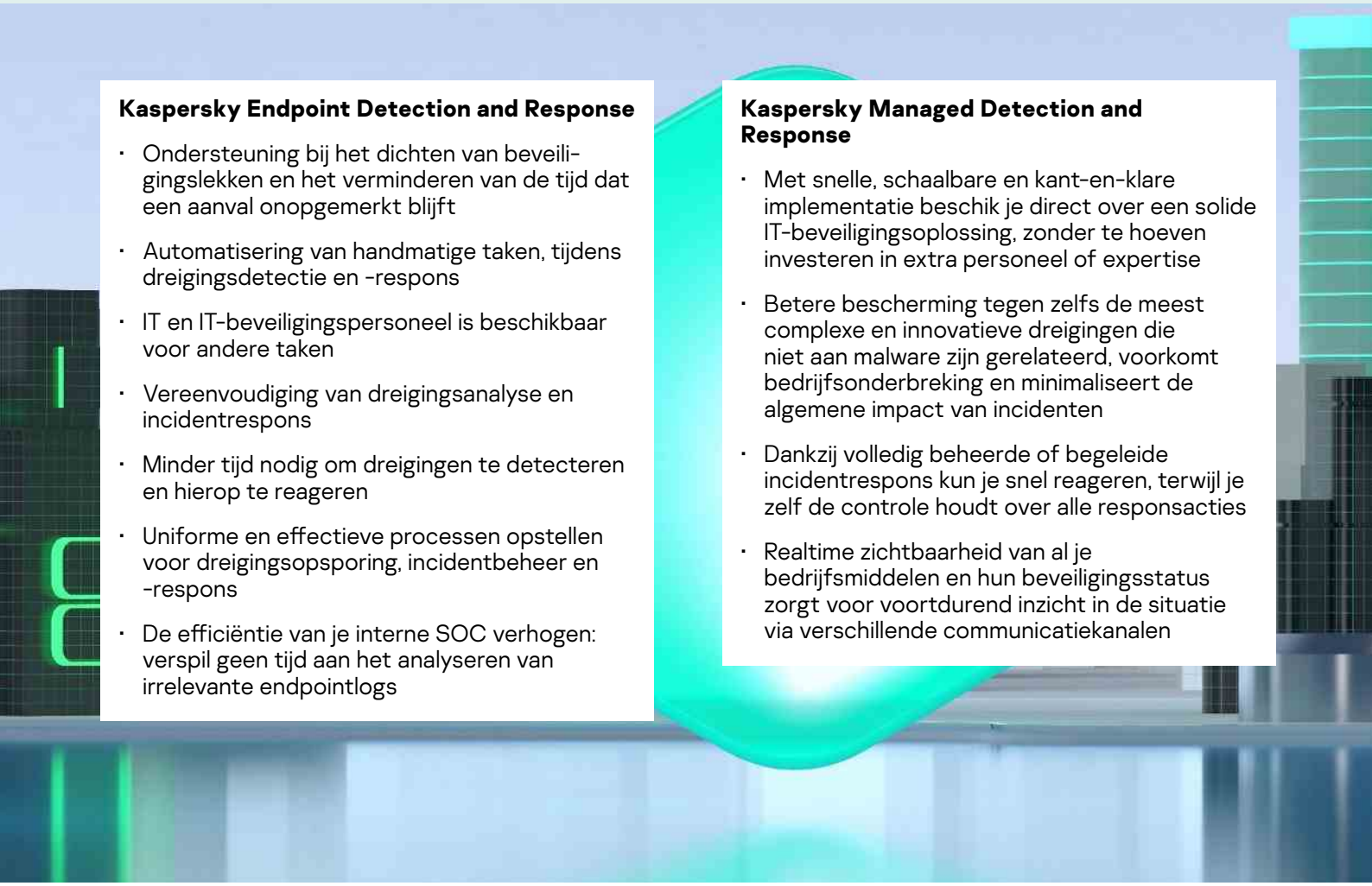
In de studie geeft meer dan een vijfde van de besluitvormers (23,1%) toe dat hun bedrijf niet voldoende investeert in preventieve maatregelen voor cybersecurity. Meer dan de helft (56,6%) is tevreden met de bestaande investeringen, maar

ongeveer een vijfde (20,4%) denkt te veel te investeren. Kort gezegd moeten bedrijven opnieuw nadenken over hoe ze investering in cybersecurity zien. Het draait niet om geldbesparing door een oplossing te gebruiken, maar om de beveiliging van alle middelen van een organisatie.

Het is bewezen dat het de moeite loont om te investeren in externe beveiligingsoplossingen: volgens de studie worden de organisaties die vertrouwen op de ondersteuning van professionele experts op het gebied van cybersecurity, minder getroffen door aanvallen dan de organisaties die werken met interne cybersecurity-oplossingen (bijna tien procentpunten minder).

Zakelijke besluitvormers van bedrijven van alle omvang die hun organisatie op een proactieve en allesomvattende manier willen beschermen tegen cyberdreigingen, moeten dus voordeel halen uit de professionele ondersteuning van een externe dienstverlener met ongeëvenaarde ervaring in cybersecurity. Ze moeten het thema cybersecurity op een proactieve manier aanpakken en investeren in de juiste oplossingen en diensten. Zo niet, zullen ze achter raken op de concurrentie.

Kaspersky is hiervoor de ideale partner. Het bedrijf biedt een combinatie van geautomatiseerde beveiligingsoplossingen (Endpoint Detection & Response) en MDR-systemen (Managed Detection and Response), waarin menselijke beveiligingsexperts bedrijven ondersteunen om zo vroeg mogelijk cyberaanvallen te identificeren en neutraliseren. Bovendien verhogen ook het Security Operation Center (SOC) en de introductie van Security Information and Event Management (SIEM) het beveiligingsniveau van grote bedrijven. Kaspersky heeft zich bewezen met zijn oplossingen voor endpointdetectie en zijn dreigingsintelligentie in de opsporing en detectie van alle soorten cyberdreigingen, gebaseerd op meer dan 20 jaar ervaring van de toonaangevende expertgroep GReAT (Global Research and Analysis Team). Dit maakt van Kaspersky de ideale partner van bedrijven om een allesomvattende, toekomstbestendige bescherming in te voeren.



Kaspersky Endpoint Detection and Response

- Ondersteuning bij het dichten van beveiligingslekken en het verminderen van de tijd dat een aanval onopgemerkt blijft
- Automatisering van handmatige taken, tijdens dreigingsdetectie en -respons
- IT en IT-beveiligingspersoneel is beschikbaar voor andere taken
- Vereenvoudiging van dreigingsanalyse en incidentrespons
- Minder tijd nodig om dreigingen te detecteren en hierop te reageren
- Uniforme en effectieve processen opstellen voor dreigingsopsporing, incidentbeheer en -respons
- De efficiëntie van je interne SOC verhogen: verspil geen tijd aan het analyseren van irrelevante endpointlogs

Kaspersky Managed Detection and Response

- Met snelle, schaalbare en kant-en-klare implementatie beschik je direct over een solide IT-beveiligingsoplossing, zonder te hoeven investeren in extra personeel of expertise
- Betere bescherming tegen zelfs de meest complexe en innovatieve dreigingen die niet aan malware zijn gerelateerd, voorkomt bedrijfsonderbreking en minimaliseert de algemene impact van incidenten
- Dankzij volledig beheerde of begeleide incidentrespons kun je snel reageren, terwijl je zelf de controle houdt over alle responsacties
- Realtime zichtbaarheid van al je bedrijfsmiddelen en hun beveiligingsstatus zorgt voor voortdurend inzicht in de situatie via verschillende communicatiekanalen

4. Op-ed: De economie van EDR en MDR - Waarom investeringen in detectie- en responsoplossingen de moeite lonen

Door Oliver Schonschek, security-analist en IDG-influencer

Hoe effectief zijn investeringen in cybersecurity? Beveiligingsmanagers moeten deze vraag regelmatig beantwoorden wanneer ze hun budgetgebruik rechtvaardigen of 'bewijs' verzamelen voor hun volgende budgetaanvraag.

Maar het is helemaal niet makkelijk om de doeltreffendheid van cybersecurity te meten, want het is geen winstgenererende investering, maar een investering die verlies voorkomt.

Erger nog: de implementatie van bescherming is geen garantie voor succes. Zelfs wanneer robuuste veiligheidsmaatregelen van kracht zijn, kunnen cyberaanvallen zich voordoen. Een recent onderzoek door cybersecuritybedrijf Kaspersky toont aan dat 38% van de grote bedrijven aan minstens één gerichte cyberaanval leed in 2020.

En dit terwijl meer dan de helft (52%) van hen een speciale afdeling voor IT-beveiliging heeft en 20% een intern Security Operations Center (SOC) heeft dat verantwoordelijk is voor de voortdurende bewaking van en reactie op beveiligingsincidenten.

Voor sommige ondernemingen wekt dit niet alleen de vraag op hoeveel budget ze zouden moeten investeren in cybersecurity, ze vragen zich ook af of beveiligingsinvesteringen hun vruchten afwerpen.

"Vele klanten investeren miljoenen in basis IT-bescherming, maar slagen er dan niet om hun investering volledig te benutten", legt Uwe Kissmann, Managing Director, Cyber Defence Service Accenture EMEA, uit. "Eigenlijk is dit een puur economische discussie: Hoe zorg ik ervoor dat de investeringen in cybersecurity die we al hebben gedaan, hun gehele potentieel kunnen ontwikkelen, en hoe kunnen we garanderen dat toekomstige investeringen optimaal presteren?"

Om dit te bereiken, raadt beveiligingsexpert en voormalig CISO Kissmann het volgende aan:

"Het is van essentieel belang om niet alleen te investeren in statische bescherming, maar ook middelen, processen en technologie te voorzien die de naadloze detectie van mogelijke toegangspoorten mogelijk maakt. Dit betekent ook dat men een duidelijke responsstrategie voor

eventuele aanvallen moet ontwikkelen. Het oprichten van beveiliging die even statisch als dynamisch is, dient om de voordelen van investeringen in cybersecurity te maximaliseren."

4.1. Detectie en respons: Bescherming moet proactiever worden

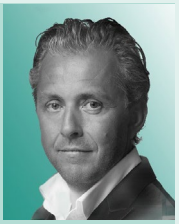
Een succesvolle cyberaanval op een bedrijf betekent niet dat investeringen in cybersecurity zinloos zijn. Dit is een verkeerd idee over beveiliging.

Het is belangrijk om te onthouden dat elk bedrijf ooit kan en waarschijnlijk zal leiden aan een succesvolle aanval. Cybersecurity moet daarom niet worden beperkt tot de bescherming tegen aanvallen, maar ook de detectie ervan en verdediging ertegen omvatten.

Het doel van cybersecurity bestaat erin succesvolle cyberaanvallen zo snel mogelijk te detecteren en hun mogelijke gevolgen te minimaliseren.

Volgens de internationale studie van Kaspersky "IT Security Economics 2021: Managing the trend of growing IT complexity[1]" , bedragen de gemiddelde kosten van gegevenslekken momenteel $ 106.577 voor kleine en middelgrote bedrijven.

Grote bedrijven kunnen nog hogere verliezen verwachten. De in de studie onderzochte bedrijven meldden bijvoorbeeld dat een IT-beveiligingsincident hun gemiddeld $ 1,06 miljoen kost op bedrijfsniveau.



"Onze studie toont een welkome trendomkering: bedrijven zijn beter en sneller geworden in de detectie van cyberbeveiligingsincidenten. Hoewel er in geval van schade nog steeds heel veel opvolgingskosten zijn, kunnen deze worden geminimaliseerd door betere en vroegere detectie. Dit kan worden bereikt door externe IT-beveiligingsexperts te betrekken en geschikte oplossingen te gebruiken."

Tim de Groot, Territory Manager Benelux & Nordics, Kaspersky.

Er is echter ook goed nieuws. Vorig jaar was de impact aanzienlijk, zelfs wanneer beveiligings-incidenten onmiddellijk werden ontdekt. Wanneer een IT-beveiligingsincident een week lang onopgemerkt bleef, stegen de kosten ook sterk.

Om een incident te detecteren en zich ertegen te beschermen in een vroeg stadium en hierbij de kosten laag te houden, moeten bedrijven zorgen dat ze over een robuust detectie- en responsvermogen beschikken. Vooral rond endpoints, want deze zijn de focus van de meeste cyberaanvallen.

Endpoint Detection and Response (EDR) verwijst naar endpointbeveiligingsoplossingen die systeem- en gebruiksgegevens van gemonitorde endpoints verzamelen, aggregeren, opslaan en analyseren. De endpointanalyse geeft een indicatie van verdachte gebeurtenissen en waarschuwt voor mogelijke IT-beveiligingsincidenten, zoals een hackpoging op een endpoint.

EDR detecteert potentiële aanvallen niet op basis van handtekeningen zoals een klassieke anti-malware doet, maar bepaalt hiervoor het verwachte gedrag van individuele endpoints en monitort of ze anomalieën vertonen. Dit maakt het ook makkelijker om aanvaltechnieken op te sporen die eerder onbekend waren, aangezien ze het gedrag van endpointprocessen, -functies en -applicaties veranderen. Beheerde diensten voor EDR worden Managed Detection and Response (MDR) genoemd.

"De risico-omgeving voor bedrijven is steeds complexer geworden in de nasleep van digitale transformatie-inspanningen en veranderingen op het gebied van de werkplek die de pandemie heeft teweeggebracht", zegt Bob Bragdon, SVP/ Managing Director van CSO, die de behoefte aan nieuwe benaderingen omtrent beveiliging bestudeert. "Organisaties die blijven reageren op hun beveiligingsrisico's, zullen een directe positieve impact op hun bedrijfsresultaten merken, die altijd zwaarder zullen doorwegen dan de kosten van de voorafgaande investering in goede beveiliging.

Bob Bragdon raadt bedrijven aan om "te focussen op de basis: Houd je technologie up-to-date,

1 De Kaspersky Corporate IT Security Risks Survey (ITSRS) is een globaal onderzoek bij IT-besluitvormers. Het werd gevoerd in mei en juni 2021 en in totaal werden 4303 interviews afgelegd met bedrijven met meer dan 50 werknemers. Kaspersky voert het onderzoek elk jaar.

zorg ervoor dat deze geconfigureerd is zoals dat hoort, en hanteer een op risico's gebaseerd model om investeringen in technologie te bevorderen. Aangezien de meeste aanvallen op de endpoint zijn gericht, is het een goede eerste stap om gebruik te maken van EDR, MDR en externe expertise."

4.2. Naleving: Incidenten sneller identificeren helpt je aan rapportvereisten te voldoen

De studie Cyber Security 2020+ van IDC rapporteert toenemende budgetten voor cybersecurity tijdens de coronapandemie.

Ook problemen met de naleving van regels zetten bedrijven ertoe aan om hun beveiligingsbudgetten te verhogen. "Dat is ten minste wat we bij onze klanten observeren, niet alleen op het gebied van IT-beveiliging, maar ook met betrekking tot gegevensbescherming, bevoorradingswetten, KYC-controles enz", vertelt advocate Mareike Gehrmann, gespecialiseerd in IT-recht.

EDR en MDR maken het mogelijk om aanvallen, en in het bijzonder inbreuken inzake gegevensbescherming, te detecteren en af te weren in een vroeg stadium. Dit vermindert of vermijdt ook sancties en boetes die zijn vastgesteld in de AVG (Algemene Verordening Gegevensbescherming), als een inbreuk inzake gegevensbescherming te laat of helemaal niet wordt gemeld.

In geval van een inbreuk inzake gegevensbescherming zijn de sancties en boetes van de AVG hoog genoeg om de leefbaarheid van mkb's in het geding te brengen. Toeziende autoriteiten kunnen bijvoorbeeld boetes opleggen die kunnen oplopen tot 20 miljoen euro of tot 4% van het totale jaarlijkse inkomen dat in het vorige boekjaar is gegenereerd, afhankelijk van welk van beide het hoogst is.

4.3. Externe ondersteuning om gebrek aan vaardigheid te bestrijden en werklast beheerbaar te houden

De behoefte aan nieuwe benaderingen van beveiliging is ook elders zichtbaar. Cyberaanvallen worden steeds complexer en verfijnder, terwijl bedrijven een gebrek aan beveiligingsprofessionals ervaren en duidelijk beperkte kennis hebben over het dynamische dreigingslandschap. Dit geldt voor zowel middelgrote bedrijven als grotere ondernemingen.

Om het gebrek aan beveiligingsprofessionals en expertise aan te pakken doen bedrijven steeds vaker een beroep op aanbieders van cybersecuritysservices.

"Voor zowel detectie als respons zijn experts met een hoge specialisatiegraad en vooral voortdurend geactualiseerde informatie erg gewild", vertelt beveiligingsexpert Uwe Kissmann. "Een professionele hacker handelt vaak onder de radar. Hackers doen een verdedigende zet om ongedetecteerd te blijven, voordat ze het risico lopen betrapt te worden. En dan, op een of ander moment, zijn bedrijven verwonderd wanneer ze ontdekken dat onbekende mensen hun systemen al jarenlang onopgemerkt aan het roamen zijn."

Maar aanvallen kunnen zeker worden gedetecteerd, volgens Kissmann, want: "Vaak worden de indicatoren over het hoofd gezien of verkeerd geïnterpreteerd. Experts die systemen het hele jaar door 24/7 monitoren en een up-to-date en zeer gespecialiseerde kennis hebben, kunnen hier te hulp schieten."

4.4. Externe ondersteuning werpt vruchten af: Detectie en respons optimaliseren

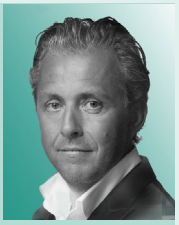
Externe ondersteuning in beveiliging is vooral zinvol waar detectie van en verdediging tegen cyberaanvallen kunnen worden geoptimaliseerd en versneld.

Managed Detection and Response (MDR) geeft middelgrote bedrijven toegang tot 'externe experts op het gebied van cybersecurity', die het mogelijk maken om bijkomende beveiligingsmaatregelen te implementeren zonder dat nieuwe werknemers moeten worden aangeworven.

Detectie en respons uitbesteden kan middelgrote en grote organisaties helpen hun detectie en verdediging te verbeteren: MDR beschermt ook tegen geavanceerde dreigingen via 24/7 proactieve monitoring en expertenkennis en via externe dreigingsintelligentie.

Kaspersky Managed Detection and Response biedt alle belangrijkste voordelen van een uitbesteed Security Operations Center (SOC). Het vereist geen gespecialiseerde vaardigheden van interne teams voor de detectie van dreigingen en de analyse van incidenten, wat het bijzonder relevant maakt voor middelgrote bedrijven.

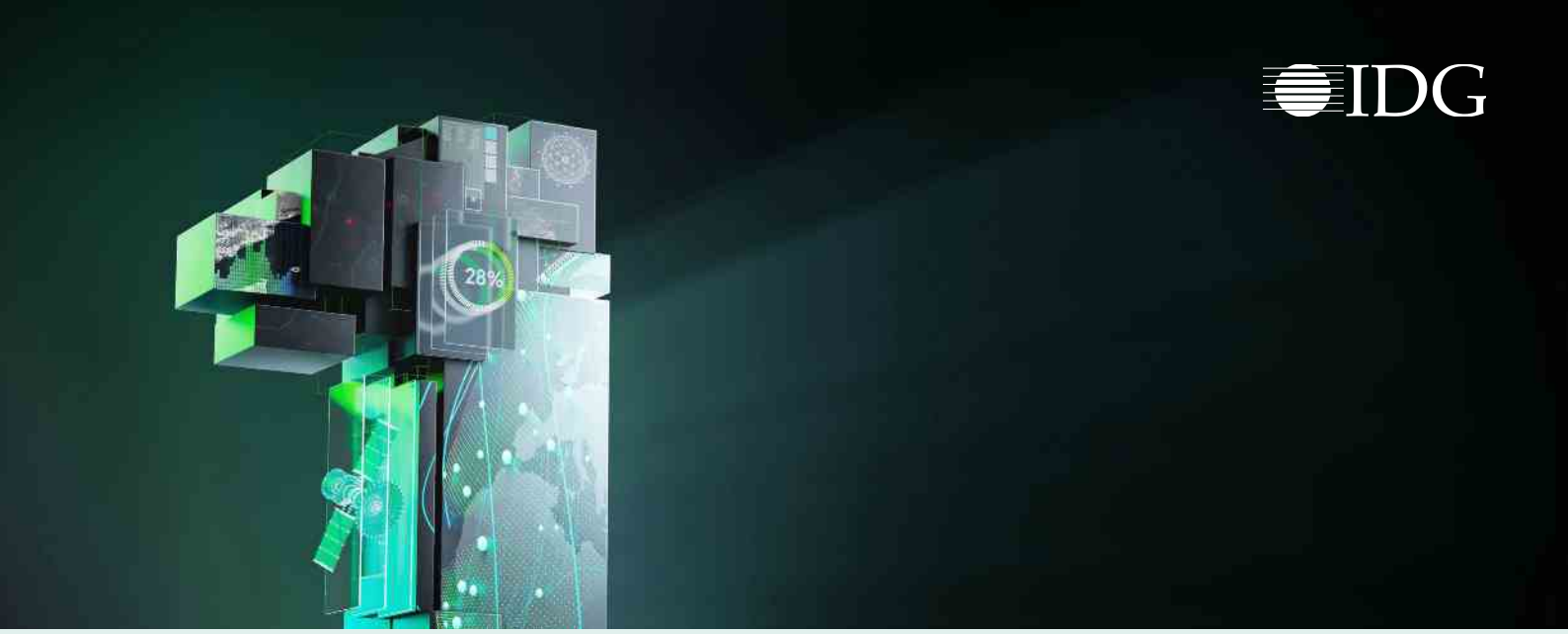
De dienst wordt aangevuld door detectie-technologieën, uitgebreide kennis over de opsporing van dreigingen en incidentrespons van beveiligingsexperts. Bovendien is de dienst uitgerust met de AI-analyseoplossing, die automatisch aanvallen evalueert, waardoor SOC-analisten zich kunnen concentreren op de belangrijkste waarschuwingssignalen.



"Organisaties zonder een toegewijd beveiligingsteam zouden moeten overwegen om te investeren in EDR-oplossingen en MDR", raadt Tim de Groot, Territory Manager Benelux & Nordics, Kaspersky aan. "Externe SOC-professionals met diepgaande expertise in het detecteren en onderzoeken van gerichte aanvallen, merken verdachte activiteit op het bedrijfsnetwerk op, analyseren het en melden een incident. Dit betekent dat een aanval wordt gedetecteerd in een vroeg stadium en de klant wordt bespaard van bijvoorbeeld het rampenscenario van een potentiële ransomwareaanval."

Bedrijven met een in-house SOC kunnen ook voordeel halen uit Managed Detection and Response: "Een MDR-service kan een tweede mening geven, ook al heeft de organisatie al een eigen SOC-team", Tim de Groot, Territory Manager Benelux & Nordics, Kaspersky.

Voor grote organisaties wordt het uitbesteden van detectie en respons vaak beschouwd als een uitbreiding van het interne Security Operations Center (SOC) of de interne beveiligingsafdeling. Het interne SOC heeft altijd een beperkt inzicht, omdat zijn beveiligingsintelligentie is gebaseerd op zijn eigen gemonitorde infrastructuur en beveiligingssensoren.



5. Uitdaging van ROSI-analyse: Hoe meet je de kosten van cybersecurity?

Volgens ENISA, het agentschap voor cybersecurity van de EU, biedt **ROSI** alvast één mogelijk antwoord.

ROSI staat voor het rendement op investeringen in beveiliging (return on security investment).

Daarom wordt een investering in beveiliging winstgevend geacht als het effect van de risicobeperking groter is dan de verwachte kosten.

Effecten van risicobeperking brengen de voordelen van investering in beveiliging aan het licht. Eenvoudig gezegd is het een 'vermindering van risicolopende waarden' die afkomstig is van de beperking van het risico dat is gerelateerd aan financiële waardevermindering, volgens ENISA.

De ROSI-formule is ontwikkeld door een team van de universiteit van Idaho onder leiding van onderzoeker Huaqiang Wei. Het team gebruikte bestaande statistieken met betrekking tot investering in informatiebeveiliging, combineerde die met enkele van hun eigen theorieën en wees waarden toe aan alle factoren, van tastbare tot ontastbare middelen.

ROSI = R - (R-E) + T
of
ROSI = R – ALE

R: Jaarlijkse onkosten om alle veiligheidsgerelateerde incidenten aan te pakken.

E: Jaarlijkse financiële besparingen dankzij de vermindering van het aantal veiligheidsgerelateerde incidenten door de implementatie van de veiligheidsoplossing.

T: Jaarlijkse kosten van de investering in beveiliging.

ARO: De kans dat een risico in een bepaald jaar voorvalt (Annual Rate of Occurence)

SLE: Het bedrag dat een bedrijf naar verwachting verliest als een risico voorvalt (Single Loss Expectancy)

ALE: Het verwachte verloren bedrag per jaar (Annual Loss Expectancy)

ALE = SLE*ARO

Een eenvoudige berekening:

Het bedrijf Muster GmbH overweegt te investeren in een beveiligingsoplossing. Elk jaar wordt Muster GmbH getroffen door vijf cyberaanvallen (ARO=5). De beveiligingsmanager schat dat elke aanval ongeveer 15.000 euro verlies veroorzaakt (SLE=15.000). Stel dat de beveiligingsoplossing minstens 80% van de aanvallen afweert (beperkingspercentage=80%) en 25.000 euro per jaar kost (licentiekosten van 15.000 euro + 10.000

euro voor opleidingen, installatie, onderhoud enz.). Voor deze oplossing wordt het rendement op investering in beveiliging dan als volgt berekend:

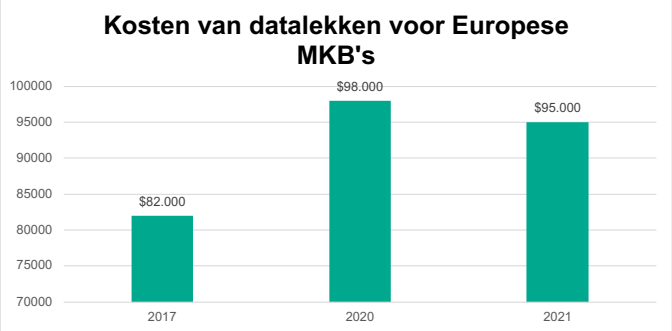
ROSI = ((5 * 15,000) * 0.8 – 25,000) / 25,000 = 140%

Volgens de ROSI-berekening is de beveiligings-oplossing een kosteneffectieve oplossing en dus financieel haalbaar.

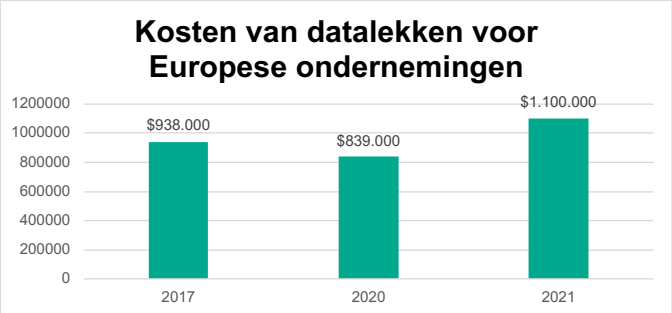
5.1. Hoe hoog zijn de kosten veroorzaakt door IT-beveiligings-incidenten in vergelijking met de uitgaven die we ertegenover stellen?

De gemiddelde kosten van IT-beveiligingsincidenten voor middelgrote bedrijven en grote ondernemingen volgens het internationale onderzoek van Kaspersky "IT Security Economics 2021: Managing the trend of growing IT complexity" [2], worden hieronder aangeduid.

Sinds 2017 bedragen de kosten per gegevenslek voor mkb's:



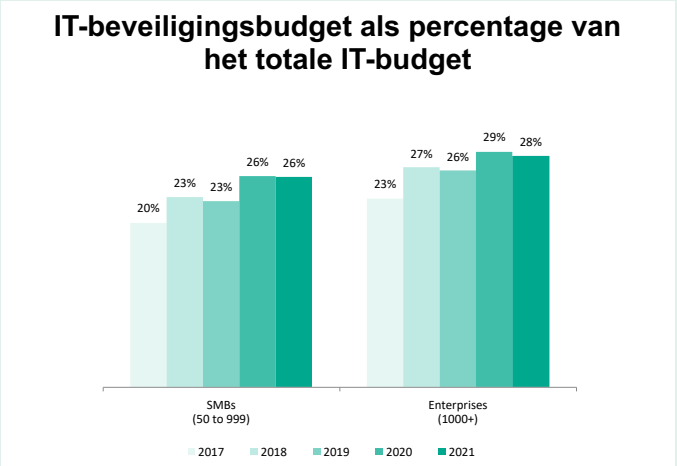
Voor grote ondernemingen zien de kosten er zo uit:



"Onze studie toont aan dat state-of-the-art-benaderingen van beveiliging, zoals EDR en MDR, werken. Voor de bevraagde bedrijven zijn de opvolgingskosten van IT-beveiligingsincidenten afgenomen in vergelijking met vorige jaren. De toenemende investeringsbereidheid van de afgelopen jaren toont aan dat er een positief effect is, aangezien de financiële schade van een cybersecurity-incident succesvol wordt verminderd."

Tim de Groot, Territory Manager Benelux & Nordics, Kaspersky.

Sinds 2017 stijgen budgetten voor IT-beveiliging wereldwijd in de mkb- en ondernemingssectoren. Ze bestrijken nu meer dan een kwart van het totale IT-budget.



"Het is essentieel voor mkb's en grote ondernemingen om strategische investeringen te maken zodat ze kunnen overleven in een steeds complexer wordend dreigingslandschap. Ze moeten investeren in externe expertise en diensten, geavanceerde oplossingen zoals EDR of MDR en beveiligingslagen zoals cloudbe-scherming die passen bij hun specifieke situatie."

Tim de Groot, Territory Manager Benelux & Nordics, Kaspersky.

2 De Kaspersky Corporate IT Security Risks Survey (ITSRS) is een globaal onderzoek bij IT-besluitvormers. Het werd gevoerd in mei en juni 2021 en in totaal werden 4303 interviews afgelegd met bedrijven met meer dan 50 werknemers. Kaspersky voert het onderzoek elk jaar.

Sommige CISO's gebruiken de ROSI-methode en anderen kiezen om dat niet te doen. Uiteindelijk is het een individuele beslissing.

"Aangaande strategische consultancy op C-niveau is ROSI een van de benaderingen die de kern vormen van de discussie", zegt Accenture-manager Uwe Kissmann. "In vele gevallen willen de deelnemers de doeltreffendheid en efficiëntie van hun cybersecuritystrategie in cijfers zien, in een Excel-bestand. Zo kunnen ze gemakkelijk bepalen in welke mate budgetten voor cybersecurity effectief zijn toegekend voor de lange termijn."

Kissmann legt het belang van het economische perspectief uit: "Cybersecurity pak je het beste aan door de voornamelijk technologische mindset te voeden met een financieel oogpunt. ROSI is hier een grote hulp en creëert de economische basis voor altijd efficiënte bescherming. We moeten echter in gedachten houden dat kwantificerende methoden vaak ontoereikend zijn in het cybergebied. De benadering moet dus op een betekenisvolle manier worden aangevuld."

Stefan Wittjen, CISO bij Vivantes Netzwerk für Gesundheit GmbH, heeft een ander standpunt: "Voor mij is het ROSI-debat te academisch en ik ben blij dat ik meestal niet zulke rekenoefeningen hoef te doen. Als onze ziekenhuizen hun deuren moeten sluiten omwille van incidenten die worden veroorzaakt door ontoereikende beveiligings-maatregelen, zal niemand zich zorgen maken om welke investeringen financieel zinvol zouden zijn geweest."

"Investeringen in cybersecurity, en in het bijzonder in detectie en respons, lonen echt de moeite. Ze kunnen ook op kosteneffectieve wijze uitbesteed worden aan beveiligingsexperts als wij." Tim de Groot, Territory Manager Benelux & Nordics, Kaspersky. "Dit legt minder druk op beveiligings-budgetten, terwijl de detectie van cyberdreigingen betrouwbaarder is en sneller gebeurt, wat schade beduidend vermindert."

6. Checklist: Belangrijkste stappen om je bedrijfsmiddelen te beschermen

De juiste benadering hanteren op het juiste moment is cruciaal om bedrijfsmiddelen op proactieve wijze te beschermen en zakelijke cybersecurity te verbeteren. Om te zorgen dat zakelijke besluitvormers het landschap van cyberdreigingen kunnen verkennen en de geschikte bescherming en processen kunnen invoeren door een cybersecuritypartner te vinden, stelt Kaspersky de volgende zes belangrijke stappen voor succes voor.

6.1. Beoordeel en begrijp de risico's

Om je bedrijfsmiddelen te beschermen, moet je elk mogelijk risico kennen dat je middelen kan treffen. Om het landschap van cyberdreigingen van je bedrijf te begrijpen, heb je een bedrijfsbreed zicht nodig op alles wat er binnen het netwerk gaande is. Dit vraagt om een geïntegreerde benadering van technologie en expertise.

Cyberdreigingen zijn vandaag divers en verfijnd en variëren van ransomware en APT's tot aanvallen op bevoorrading en gegevenslekken. Maar als we gegevens en bedrijfsmiddelen integraal willen beschermen, moeten we ook weten dat niet alleen cyberdreigingen enorme financiële en reputatiegevolgen kunnen hebben. Ook ontevreden werknemers, voormalige werknemers en zelfs klanten kunnen een risico vormen, als je niet de juiste processen en bewakingsoplossingen hebt geïmplementeerd om gegevens en bedrijfsmiddelen te beschermen.

Om de omvang van het probleem aan te tonen als het niet serieus wordt genomen, voerde Kaspersky onlangs een studie uit. Hieruit bleek dat een gegevenslek dat een week na een cyberaanval wordt ontdekt, ondernemingen in Europa een half miljoen Amerikaanse dollar kost (minder voor mkb's, namelijk $ 122.963). Bedrijven die een aanval onmiddellijk detecteren, zouden daarentegen 213.737 Amerikaanse dollar betalen (mkb's zouden $ 97.817 kwijt zijn).

6.2. Stel de juiste vragen

Met dit in gedachten is het vervolgens van cruciaal belang om de juiste vragen te stellen over cybersecurity. Zo weet je zeker dat je geen middel onbeproefd laat en dat het juiste type plan wordt gecreëerd. Dit begint bij het begrijpen van de belangrijkste zakelijke processen en technologieën waarvan je het meest afhankelijk bent, voordat je het gaat hebben over budgetten en oplossingen.

Hoe wordt de netwerkinfrastructuur momenteel beheerd en beveiligd? Welke zakelijke processen zijn onmisbaar voor de missie en waar zou uitvaltijd leiden tot verloren inkomsten en beschadigde relaties? Welke beveiligingsexpertise is er op werknemersniveau? Hoe hebben we beveiligings-incidenten in het verleden aangepakt en hoe hebben we erop gereageerd? Waar hebben we te weinig kennis en vaardigheden?

Met behulp van een resultaatgerichte benadering kunnen de juiste prioriteiten en investeringen worden vastgesteld op basis van de beschermingsniveaus die op de verschillende plaatsen in het bedrijf nodig zijn.

6.3. Creëer bewustzijn en een gevoel van eigenaarschap

Een cultuur waar beveiliging op de eerste plaats komt, is cruciaal om cybersecurityniveaus overal in het bedrijf te verbeteren. Dit kan echter alleen worden bereikt als iedereen in de organisatie zijn of haar rol en verantwoordelijkheden begrijpt. Aangezien de helft van alle inbreuken inzake beveiliging worden veroorzaakt door dreigingen van binnenuit, is het vaak te wijten aan een gebrek van bewustzijn of menselijke fout.

Opleidingen rond bewustzijn en regelmatige volgoefeningen om te testen of advies wordt omgezet in actie, zijn daarom essentieel op alle niveaus, van de meest junior werknemers tot senior executives. Dit kan online gebeuren en moet best practices behandelen, zoals wachtwoordbeheer, e-mailbeveiliging en veilig surfen op het web. Mensen moeten niet alleen de risico's begrijpen, ze moeten ook weten bij wie ze terecht kunnen als ze een probleem hebben en over duidelijke richtlijnen en aanbevelingen beschikken om een gevoel van eigenaarschap te ondersteunen.

6.4. Investeer in intelligentie

Naast vaardigheden aanreiken om een aanval te herkennen en te vermijden, is het essentieel om het bedrijf voor te bereiden op de toekomst met state-of-the-art-, robuuste bescherming tegen cybercriminaliteit. Deze holistische aanpak kan alleen worden bereikt wanneer men het juiste niveau van dreigingsintelligentie heeft en in staat is om big data-analyse toe te passen op beveiliging. Dankzij in acties omzetbare inzichten over dreigingen voor bedrijven, kunnen plannen en processen evolueren op basis van betekenisvolle gegevens om te voorkomen dat bedrijven in de toekomst in aanvaring komen met bedreigingen of beveiligingsincidenten. Om de essentiële laag van geautomatiseerde intelligentie te verkrijgen, moeten zakelijke besluitvormers de juiste partner met een bewezen staat van dienst vinden die dreigingsintelligentie ook kan automatiseren voor nog snellere respons-vermogens.

Kaspersky ondersteunt bedrijven met toegang tot de nieuwste dreigingsintelligentie via ons Threat Intelligence Portal. Dit verstrekt uitgebreide gegevens over cyberaanvallen en intelligentie, die onze experts al meer dan 20 jaar lang verzamelen.

6.5. Wees voorbereid om snel te reageren

Aanvallers zijn tegenwoordig bekwame, verfijnd te werk gaande stiekemerds. Ze gebruiken alles wat nodig is om voorbij de verdediging te raken. Preventie op zich is niet voldoende. Organisaties moeten ook in staat zijn om snel en beslissend te reageren. Plannen, oefenen en ervoor zorgen dat de juiste beveiligingstools aanwezig zijn, is cruciaal.

Oplossingen als Kaspersky Endpoint Detection and Response en Kaspersky Managed Detection and Response kunnen helpen bij het identificeren, onderzoeken en snel oplossen van incidenten bij alle werknemerendpoints. Dit is in het bijzonder waardevol nu BYOD (bring your own device) vaak wordt gebruikt, vooral als gevolg van de pandemie en lange perioden van thuis werken.

6.6. Beoordeel en herzie plannen

Externe en interne beveiligingsdreigingen evolueren voortdurend, wat betekent dat je plannen en processen dat ook moeten doen om bij te blijven. Beveiligingsplannen moeten regelmatig worden herzien en geüpgraded om beveiligingsdreigingen af te weren en te herstellen.

Werken met externe experts kan ervoor zorgen dat plannen actueel en toekomstbestendig blijven naarmate bedrijven groeien en het dreigings-landschap blijft veranderen.

Met een cybersecuritypartner die het volledige plaatje kan zien dankzij deskundig inzicht, je ondersteunt met de nieuwste dreigingsintelligentie en een verenigde structuur biedt die alles doet, kun je je zorgeloos concentreren op innovatie.

7. Welke bescherming past het beste bij je bedrijf?

	Geautomatiseerde EDR	EDR Optimum	MDR	XDR-EDR-expert
Status quo van je IT-resources	Je IT-resources zijn beperkt.	Je hebt werknemers binnen je IT-afdeling die de infrastructuur operationeel houden en bovendien verantwoordelijk zijn voor beveiliging en analyse indien nodig.	Je IT-resources zijn beperkt.	Naast de klassieke IT-afdelingen heb je een speciaal IT-beveiligingsteam.
Status quo van je beveiligings-expertise	Je hebt geen toegewijde werknemer voor IT-beveiliging en er zijn geen plannen om beveiligingsexpertise op te bouwen.	Je hebt al een beetje ervaring in de analyse van incidenten of bent je eigen beveiligings-expertise aan het opbouwen binnen je bedrijf.	Je wilt geen eigen IT-beveiligings-expertise opbouwen, noch op dit moment, noch op de lange termijn. Toch wil je deze taak uitbesteden aan een 24/7-dienst om het best mogelijke beschermingsniveau te behalen.	Je werknemers hebben goede tot zeer goede beveili-gingsexpertise. Je bent een toegewijd team van experts aan het bouwen of hebt het onderwerp detectie en verdediging reeds georganiseerd in een SOC.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

kaspersky.com