cegeka

Reduceer cybersecurityrisico's

Detect and response best practices

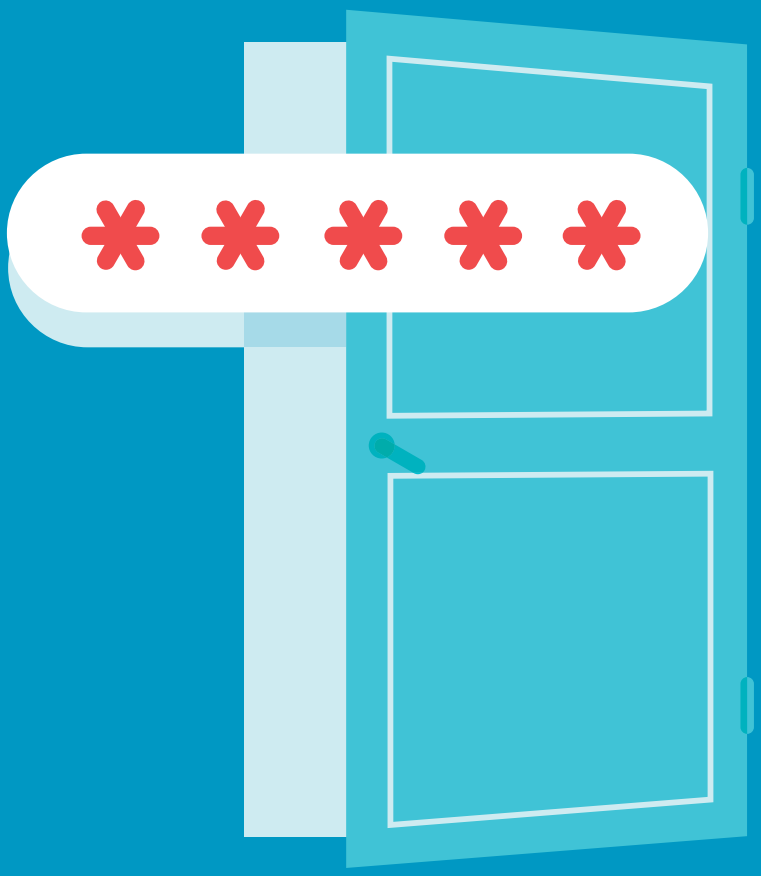
Het duurt gemiddeld 280 dagen voordat een datainbraak onder controle is. Veel bedrijven weten niet eens dat cybercriminelen al lang bij hen ingebroken zijn.

Hoe vermindert u dit aantal dagen? En hoe minimaliseert u de operationele en financiële impact van een computerinbraak en bedreigingen zoals *ransomware*?

In dit e-book vindt u richtlijnen om uw cybersecurityrisico's te reduceren en een stappenplan om op een kostenefficiënte manier een beveiligingsgereedschapskist op te bouwen.

Iedereen is een potentieel doelwit van cybercriminelen. Maar het gereedschap om u te beschermen is ook voor iedereen toegankelijk.

Inhoudsopgave



1

Start met de juiste cybersecurity-aanpak

Cybersecurityrisico's reduceren tijdens vijf fasen

Het Amerikaanse National Institute of Standards and Technology (NIST) geeft in haar Cybersecurity Framework **richtlijnen en best practices** voor organisaties om hun cybersecurityrisico's te reduceren. Cegeka heeft op dit framework voortgebouwd met haar cybersecurity-aanpak. De acties die u als organisatie kunt uitvoeren, zijn met deze aanpak opgedeeld in vijf fasen:

- **Assess:** Inventariseer uw bezittingen, evalueer de bedrijfscontext en krijg inzicht in uw risico's.
- **Prevent:** Bescherm uw bezittingen met procedures en tools.
- **Detect:** Detecteer beveiligingsincidenten zo snel mogelijk.
- **Respond:** Reageer zodra u een inbraak detecteert om de impact minimaal te houden.
- **Recover:** Stroomlijn en versnel het herstel na een beveiligingsincident met de juiste herstelprocedures.

Veel bedrijven focussen zich op de tweede fase van het beveiligingsframework: **Prevent**. Ze installeren beveiligingssoftware om hun gegevens en IT-systemen te beschermen. Maar dat volstaat niet: de andere fasen zijn even essentieel.

NIST Cybersecurity Framework

Lees meer over het
NIST Cybersecurity Framework op
www.nist.gov/cyberframework

2

Eerst inzicht, dan bescherming

Weet wat u moet beschermen

Het is verleidelijk om onmiddellijk naar de tweede fase van uw cybersecurityaanpak te gaan: Prevent. Maar om uw IT-systemen kostenefficiënt te beschermen, is het belangrijk dat u eerst identificeert welke bezittingen u wilt beschermen en wat de risico's exact zijn. Al uw beveiligingsinspanningen beginnen bij **Assess**.

Met andere woorden: wat zijn de kroonjuwelen van uw bedrijf? Welke gegevens wilt u zeker niet verliezen? En welke gegevens wilt u zeker niet publiek of op het dark web verkocht zien?

Wat zijn uw kroonjuwelen?

Maak eens een lijst met de belangrijke gegevens in uw bedrijf die u zeker moet beschermen. Denk daarbij aan:

- Personeelslijst
- Loonstroken
- Klantenlijst
- Gegevens van klanten
- Bankrekeningnummers
- Wachtwoorden
- Offertes

Stel u de vraag wat de impact op uw bedrijf is als u deze gegevens verliest of als ze publiek worden.

Ken uw vijand

Om de risico's correct te kunnen evalueren, is het belangrijk dat u uw vijand kent: de cybercriminelen die het op uw gegevens of infrastructuur gemunt hebben. Een van hun meest gebruikte wapens is tegenwoordig **ransomware**.

Met ransomware versleutelen cybercriminelen uw gegevens. Daardoor zijn die gegevens niet meer leesbaar voor u en ligt uw bedrijf stil. Alleen al daarmee verliest u heel wat omzet. De cybercriminelen vragen dan **losgeld om uw gegevens weer leesbaar te maken.**

Afpersing

Maar zelfs al heeft u een back-up, kunt u uw gegevens herstellen én slaagt u erin om uw hele IT-infrastructuur opnieuw op te bouwen zodat de cybercriminelen niet meer binnen kunnen, u bent niet meer veilig.

Zodra de cybercriminelen in uw systemen ingebroken zijn, hebben ze immers ook uw gegevens gestolen. Daarmee persen ze u af: ze dreigen om die gegevens te publiceren, wat uw bedrijf heel wat schade zal berokkenen. Als bewijs dat ze uw gegevens hebben, tonen ze u een deel, of lekken ze een deel aan het publiek.

Drie fundamentele risico's voor uw bedrijf

Er zijn drie fundamentele soorten risico's waartegen u uw bedrijf wilt beschermen:

Operationeel

Als uw IT-systemen lam liggen, kan uw bedrijf geen orders meer verwerken, geen producten of diensten meer leveren en geen herinneringen voor facturen meer sturen. Dan verliest u omzet.

Financieel

De financiële gevolgen gaan verder dan alleen het omzetverlies. U betaalt de cybercriminelen losgeld om te voorkomen dat ze uw gegevens publiek maken. Het herstel van uw IT-systemen kost ook geld, evenals het inhalen van de achterstand. Klanten en leveranciers kunnen u aanklagen of compensaties eisen als hun informatie gelekt is, en er kunnen u boetes opgelegd worden. Dit alles brengt ook juridische kosten met zich mee. En wat als uw offertes of vertrouwelijke R&D-documenten zijn gepubliceerd en uw concurrenten die kunnen inzien?

Reputatie

Onderschat ook de reputatieschade niet als uw bedrijf het slachtoffer wordt van cybercriminelen. Willen klanten nog bij u kopen als er bij u ingebroken is? Zeker als hun eigen gegevens publiek zijn gemaakt, denken ze wel twee keer na. U verliest klanten, en het kost heel wat geld om hun vertrouwen te herwinnen en nieuwe klanten aan te trekken.

Kosten-batenanalyse

Maak de berekening eens voor enkele scenario's als de drie fundamentele risico's (operationeel, financieel en reputatie) realiteit worden in uw bedrijf. Hoeveel kost het dan om uw bedrijf weer operationeel te krijgen? En hoeveel kost het om uw bedrijf tegen die risico's te beschermen?

3

Detecteer en reageer

Alarmsysteem

Na Prevent komt **Detect**. Als uw beschermingsmaatregelen niet hebben gewerkt, merkt u dan of er ingebroken is?

Vergelijk het met een alarmsysteem voor fysieke inbraken. Als inbrekers de ronde doen in uw straat, weet u zonder alarmsysteem niet wanneer ze aan uw deur morrelen.

Bedrijven installeren doorgaans wel een fysiek alarmsysteem. Waarom dan geen IT-alarm?
Uw IT-systemen vormen immers het hart van uw bedrijf, zelfs als u geen IT-bedrijf bent.

Wacht niet op een inbraak voor u een alarmsysteem installeert

Veel mensen en zelfs bedrijven installeren pas een alarmsysteem wanneer er in de buurt ingebroken wordt. Ook in de digitale wereld gebeurt dat: men denkt vaak dat een cyberinbraak hen niet overkomt. Maar iedereen is een potentieel doelwit van cybercriminelen, zowel grote als kleine bedrijven. Wacht niet tot u het slachtoffer wordt van ransomware, maar wees voorbereid.

Reageer

Het heeft geen zin om een alarmsysteem met camera's in uw bedrijf te installeren als niemand de camerabeelden bekijkt.

Op dezelfde manier bent u niets met een detectiesysteem voor cyberincidenten zonder systeem om erop te reageren. Na Detect komt immers **Respond**.

Een Security Operations Center (SOC) is daarom essentieel. De analisten in deze 'meldkamer' houden het alarmsysteem van uw IT 24/7 in de gaten en reageren snel op mogelijke inbreuken.

De security-analisten hebben ervaring met allerlei soorten incidenten. Ze zijn daarom goed geplaatst om u te helpen als u moet beslissen welke stappen u dient te nemen in het geval van een beveiligingsincident.

Een goed uitgerust SOC wordt ook bijgestaan door systemen die automatisch reageren op gedetecteerde bedreigingen.

280

dagen onveilig

Het duurt gemiddeld 280 dagen voordat een data-inbraak onder controle is[1]. Gemiddeld duurt het 207 dagen om de inbraak vast te stellen en nog eens 73 om ze op te lossen. Met een detectiesysteem vermindert u dit aantal dagen en verlaagt u dus ook de impact voor uw business.

1. Bron: 2020 Cost of a Data Breach Report van het Ponemon Institute en IBM Security

4

Managed Detection & Response: uw flexibele beveiligingsgereed-schapskist

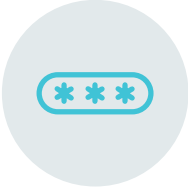
Managed Detection & Response

Het equivalent van een alarmsysteem met meldkamer voor fysieke inbraken is in de IT-wereld MDR: Managed Detection & Response. Dit bestaat uit de volgende onderdelen:

- De analisten van een **Security Operations Center (SOC)** monitoren uw organisatie op mogelijke cyberbeveiligingsinbreuken.
- Een **Security Information & Event Management (SIEM)** verzamelt logs van allerlei bronnen en levert realtime analyses en meldingen op van verdachte gebeurtenissen.
- **Network Detection & Response (NDR)** analyseert netwerkverkeer, bepaalt het risiconiveau, detecteert afwijkingen en kan door middel van integraties met andere systemen deels automatisch daarop reageren. De SOC-analisten evalueren de meldingen van de NDR en reageren daarop als dat nodig is.
- **Endpoint Detection & Response (EDR)** monitort het gebruik van endpoints (computers of mobiele apparaten), detecteert afwijkend gedrag en kan deels automatisch daarop reageren. Op de endpoints installeert u daarvoor End Point Protection (EPP). Het laat de SOC-analisten toe om rechtstreeks met de endpoints te verbinden, informatie op te vragen en in te grijpen waar nodig.

Door de automatische reacties en de reacties van de SOC-analisten wordt eventuele **schade van een inbraak tot een minimum beperkt.** Iedereen is dus gebaat bij een MDR.

Alarmsysteem op maat



MDR-systemen bestaan in talloze smaken, van eenvoudig tot complex. Voor een **kostenefficiënte inzet** van MDR is het belangrijk dat u een systeem kiest op maat van uw bedrijf.

De belangrijkste factor in deze keuze is dat u voldoende aandacht besteedt aan de fase Assess in uw cybersecurityaanpak.

Als u zonder onderscheid al uw logs door uw SIEM laat verzamelen, wordt u overspoeld door meldingen en ziet u daardoor de echt belangrijke meldingen niet.

Als u daarentegen weet wat u moet beschermen, als u weet wat de kroonjuwelen van uw bedrijf zijn, kunt u zich op die gegevens en systemen focussen. Dan:

- beperkt u de door het SIEM verzamelde logs tot de **belangrijke systemen;**
- installeert u EPP op bedrijfskritische **endpoints;**
- neemt u het **netwerkverkeer van en naar essentiële servers** en industriële systemen waar geen endpointbeveiliging mogelijk is onder de loep met NDR.

De SOC kan zich op deze manier focussen op de bedreigingen die belangrijk zijn voor uw bedrijf.

Start met EDR

Heeft u nog geen SIEM, dan is EDR de eerste stap om u tegen cybercriminelen te beschermen. Deze technologie is de meest kostenefficiënte, en het geeft u vanaf het begin ook de mogelijkheid om snel te reageren op cyberbedreigingen.

Heeft u al wel een SIEM, dan is de meest kostenefficiënte volgende stap dat u deze aanvult met EDR. Dat verhoogt de zichtbaarheid van bedreigingen en geeft een antwoord op de toenemende inbreuken op endpointsystemen. Bovendien kunt u zo sneller reageren op cyberaanvallen, wat de operationele impact vermindert.

Start met de basis, breid later uit

Met MDR kunt u met de basis starten en uw beveiligingsgereedschapskist gaandeweg uitbreiden, naarmate u meer ervaring opdoet met uw beveiligingsaanpak. Afhankelijk van hoe u begint, zijn er twee paden mogelijk:

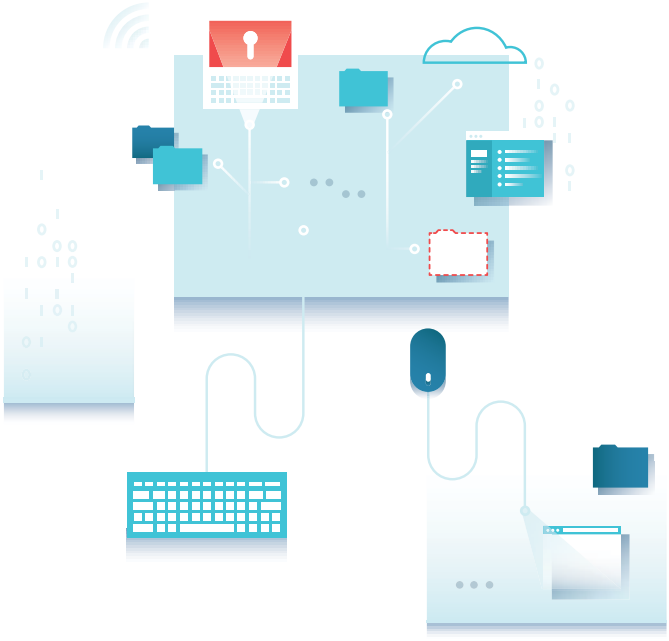
- **U begint met een SOC en SIEM:** u vult dit eerst aan met EDR op de endpoints en breidt dit tot slot uit met NDR voor het netwerkverkeer.
- **U begint met een SOC en EDR:** u breidt de zichtbaarheid uit met SIEM en voegt tot slot het netwerkperspectief toe met NDR.

NDR geeft u meer inzicht in de bedreigingen op uw netwerk. Het is een krachtig sluitstuk van uw MDR.

Managed EDR

Door uw EDR uit te besteden aan experts, bespaart u kosten en profiteert u van de schaalgrootte van de aanbieder.

Zelfs als u al een systeem voor endpointbeveiliging heeft, is het de moeite waard om oplossingen voor managed EDR te bekijken. Vaak is het goedkoper om uw eigen EPP in te ruilen voor een managed EDR (waarin de endpointbeveiliging EPP inbegrepen is). Op deze manier maakt u eenvoudig budget vrij dat u kunt investeren in uw beveiligingsstrategie.



5

Conclusie

Conclusie

Om uw cybersecurityrisico's te reduceren, begint u met uw kroonjuwelen te identificeren en de risico's van cybercriminelen in kaart te brengen. Daarna kunt u een kosten-batenanalyse maken om uw bedrijf tegen die risico's te beschermen.

Beschermingsmaatregelen alleen zijn niet voldoende: u moet ook weten wanneer er ingebroken is, en erop kunnen reageren. Het duurt gemiddeld 280 dagen voordat een data-inbraak onder controle is. Hoe meer u dit aantal dagen kunt verminderen, hoe meer u de operationele en financiële impact minimaliseert.

Dat kan met Managed Detection & Response (MDR). Als u voldoende aandacht besteed heeft aan het identificeren van uw kroonjuwelen, kunt u zich met MDR vrij snel en kostenefficiënt focussen op de bedreigingen die belangrijk zijn voor uw bedrijf. Start met de basis en breid uw beveiligingsgereedschapskist gaandeweg uit, naarmate u meer ervaring opdoet met uw beveiligingsaanpak.

Het resultaat? U elimineert cyberbedreigingen zo snel mogelijk en de operationele impact blijft beperkt.

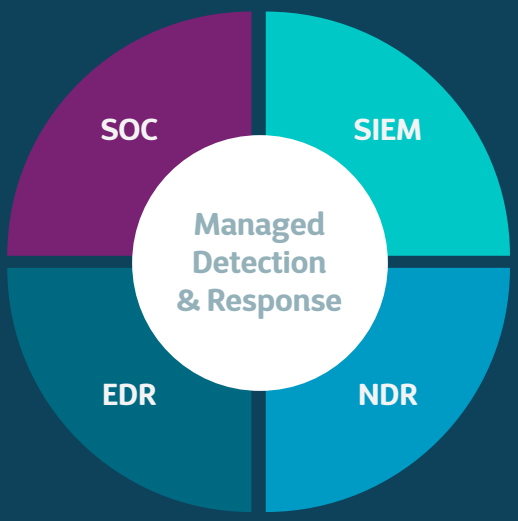
Managed Detection & Response bij Cegeka

Cegeka biedt een modulair MDR-portfolio aan, waarbinnen er een combinatie is voor elke behoefte, elke organisatie en elk budget.

Met de geavanceerde Threat & Brand Intelligence van Cegeka MDR heeft u toegang tot een belangrijke bron van informatie om snel en accuraat beveiligingsproblemen in uw omgeving op te sporen.

Door de modulaire aanpak stapt u in een toekomstgerichte dienstverlening die meegroeit met uw budget en in lijn met de uitvoering van uw beveiligingsplan.

Door de as-a-service-aanpak betaalt u alleen voor wat u echt gebruikt en houdt u de kosten onder controle.



index

WWW.CEGEKA.COM