econocom

De 5 grootste cyber-security uitdagingen van 2022

“Mij overkomt het niet!”

Wist u dat 56% van de organisaties pas maanden later doorheeft dat er iets mis is na een cyberaanval? Of dat 66% van alle bedrijven het voorbije jaar het slachtoffer werd van zo’n aanval? Financieel verlies en imagoschade na een hack kunt u missen als kiespijn. Zeker nu uw IT complexer is en uw data kostbaarder wordt dan ooit tevoren.

De dreiging in cijfers

Sinds de coronacrisis is cybercriminaliteit met

600%

gestegen

De gemiddelde kost van 1 cyberaanval bedraagt

3,5

miljoen euro

Hoelang betaalt een bedrijf na een cyberaanval?

- **67%** in het **eerstre jaar**
- **22%** in het **tweede jaar**
- **11%** in het **derde jaar**

Wat is de oorzaak van cyber-dreiging?

- **51%** externe criminele aanvallen
- **25%** systeemfalen of technische problemen
- **24%** interne menselijke fout

Wat zijn uw 5 grootste cyber uitdagingen?

Ransomware

Ransomware wordt steeds vaker in het computer-netwerk geplant. We spreken zelfs van **double-, triple-, en quadruple extortion,** waarbij criminelen ermee dreigen om uw gegevens op straat te gooien en zelfs uw klanten verwittigen om zo reputatieschade te creëren.

Phishing en spoofing

Niet detecteerbaar door reguliere antivirussoftware en een echte plaag vandaag! De beste verdediging? **Uw eigen medewerkers.**

Professionalisering van cybercriminelen

Door de toenemende professionalisering van **sterk georganiseerde transnationale cybercriminaliteit** ontstaat er een economisch ontwrichtend gevaar.

Toenemende digitalisering

Bedrijven digitaliseren steeds meer. Het gevolg? Cybercriminelen hebben meer doelwitten, waardoor **de kans** én **financiële impact** van een cyberaanval toeneemt.

Tekort aan security professionals

Complexe en geavanceerde malware wordt dagelijks gegenereerd. En dat terwijl er een groot tekort is aan **cybersecurity professionals** om kwaadaardige code te voorkomen of te herstellen.

Hoe ziet cyber-security er in 2022 uit?

De meeste bedrijven voelen aan dat hun huidige cybersecurity niet bestand is tegen de nieuwe uitdagingen.

Bedrijven staan voor een uniek dilemma

- **64%** zegt dat IT in enkele jaren veel complexer is geworden
- **44%** benoemt dat ze te weinig in-house kennis over cyber-security bezitten
- **55%** erkent dat hun data van groot belang is voor het bestaan van hun bedrijf

Bedrijven hebben nood aan een **proactieve aanpak** om hun **data en IT** veilig te stellen. Cybercriminelen spelen namelijk maar al te graag in op de complexe nieuwe IT-realiteit en gaten in uw kennis.

Identify

U kunt uw assets niet beschermen als u niet weet waar ze zich bevinden. Uw verdediging valt of staat bij een volledig en overzichtelijk inzicht in al uw assets.

- Hoe krijgt u overzicht over uw assets? Kunt u dit proces automatiseren?
- Heeft u zowel overzicht over uw data in de cloud, on-premise als bij externe partijen?
- Heeft u voldoende kennis over managed of unmanaged assets? Weet u hoe uw volledige datastructuur eruitziet?
- Welke assets zijn perimeter assets en welke zijn core assets?
- Kunt u correct de waarde van elke asset inschatten?
- Hoe meet u betrouwbaar en herhaaldelijk de sterkte van uw cybersecurity?

Protect

Het bedrijf heeft een steeds evoluerende cybersecurity die door iedereen wordt gedragen. Alle betrokken partijen blijven nadenken over optimalisatie van het systeem.

- Kunnen mensen zich veilig aanmelden met de geïmplementeerde multi-factor authenticatie?
- Hoe zit het met de security hygiene van het systeem? Wordt er voldoende stilgestaan bij tussentijds onderhoud?
- Is er door middel van penetration testing gekeken of de assets voldoende worden beschermd?

Detect

Het bedrijf zet in op detectie van cyberdreiging en houdt de vinger aan de pols bij alle teams.

- Wordt de veiligheid van de assets continu in de gaten gehouden?
- Zijn de methodes om inzicht te krijgen voldoende diepgaand?
- Is de intel die wordt verkregen eenduidig te interpreteren?
- Worden SOC activiteiten geprioriteerd op basis van het risico?

Respond

Het bedrijf en de medewerkers weten wat te doen wanneer cyberdreiging toeslaat.

- Wat is het actieplan na een cyberdreiging? Welke procedures bestaan er wanneer uw cybersecurity wordt bedreigd?
- Hoe wordt de impact van een cyberaanval tot een minimum beperkt?
- Wat wordt van elk team verwacht na een cyberaanval?

Recover

Het bedrijf kan zelfs na een cyberaanval de werking verder zetten en gaat vliegensvlug terug naar normaal.

- Wat is het korte-en langetermijnplan na een cyberaanval?
- Hoe wordt gezorgd dat de werking van het bedrijf ook na een cyberaanval ongestoord verder kan?
- Heeft een cyberaanval een impact voor klanten, partners, externen?
- Is er een back-up van de belangrijkste data en assets?

Cyber resilient werken betekent u volledig **voorbereiden op alle vormen van cyberdreiging** en toch **een daadkrachtig actieplan** hebben voor wanneer het onverwachte gebeurt. Cybercriminaliteit wordt inventiever. Bedrijven moeten dus nog sneller evolueren met hun cybersecurity. Cyber resilience vindt de balans tussen **pro- en reactief.** Actie en reactie. Daarom is het de beste strategie voor bedrijven die willen inzetten op volledige bescherming.

Geef vorm aan uw optimale cybersecurity

Econocom is uw partner in cyber resilience. Uw beste bescherming start met het grondig in kaart brengen van uw security posture. Wij meten daarom voor u:

Uw overzicht over alle assets en waar u kwetsbaarst bent voor cyberdreiging

De kracht van uw huidige cybersecurity

Uw vermogen om dreiging te detecteren en uw inzicht in damage control

De snelheid waarmee u reageert en herstelt van cyberaanvallen

Op basis daarvan geven wij advies op maat van uw bedrijf. Zo geven we samen vorm aan uw sterke actieplan, compleet onafhankelijk van specifieke vendors.

Leer meer met onze cybersecurity audit

- **Intake & installatie**
- **Verzamelen van data**
- **Eindrapport**
- **Rapportering en advies**

MEER INFO

econocom IBM