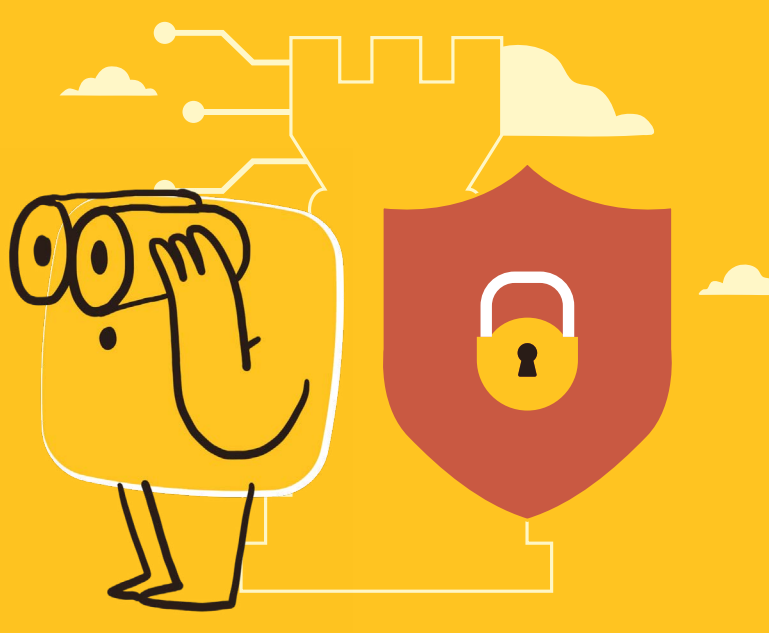
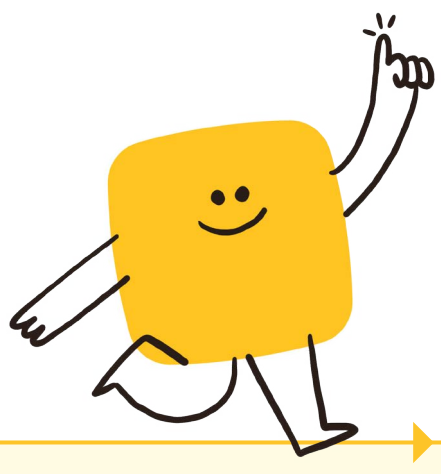
Hoe cyberveilig is jouw bedrijf?



Volg dit 5-stappenplan en waarborg je business continuity



STAP 01

Identificatie van bedreigingen

Meten is weten en dat is niet anders bij cybersecurity. Om jouw bedrijf écht veilig te maken, start je maar beter met een grondige voorbereiding. Weet jij waar het gevaar schuilt, op welke toestellen jouw medewerkers werken, of die apparaten veilig zijn en welke bedrijfsgegevens het best beschermd worden? Twijfel je? Maak je actieplan op en krijg meer inzicht in je IT-infrastructuur en bedrijfskritische gegevens door het opstellen van:

- → **een grondige risicoanalyse doorheen alle lagen van je IT;**
- → **kwetsbaarheidscans: ga op zoek naar de achilleshiel van jouw IT;**
- → **een strategisch risicobeheersplan: welke oplossingen en strategieën implementeer je het best om een mogelijke dreiging te vermijden?**

STAP 02

Bescherming van bedrijfsmiddelen

Je hebt je volledige IT-infrastructuur onder de loep genomen, je kent de zwakke schakels en weet waar die zich bevinden. Tijd om ze ook effectief te beschermen:

BEVEILIGING VAN NETWERK- EN SYSTEEMTOEGANG
Beperk de toegang tot cruciale bedrijfsprocessen en -netwerken en laat enkel geautoriseerde gebruikers toe. Zo voorkom je dat onbevoegde personen toegang krijgen tot gevoelige bedrijfsgegevens of systemen en maak je het hackers moeilijker om je IT-infrastructuur binnen te dringen. Bekende voorbeelden zijn firewalls, VPN's, zero trust en multifactorauthenticatie.

DATA-ENCRYPTIE EN BACK-UPSTRATEGIEËN
Toch gehackt? Met een sterk cybersecuritybeleid hoeft dat niet eens het einde van de wereld te betekenen. Zo maakt data-encryptie je gevoelige bedrijfsgegevens onleesbaar voor onbevoegden, zélfs als data onderschept wordt. En met systematische back-ups herstel je data meteen tot het punt van voor de crash of aanval.

BEWUSTWORDING EN TRAINING VAN MEDEWERKERS
Zijn jouw medewerkers al getraind om mogelijke cybergevaren meteen te detecteren en te voorkomen? Blijf inzetten op coaching zodat jouw team op de hoogte blijft van de nieuwste ontwikkelingen, applicaties en oplossingen binnen cybersecurity. In deze blog ontdek je het belang van teamwork binnen een cyberveilig bedrijf.

STAP 03

Detectie van inbreuken

Geïntegreerde IT-oplossingen, zoals machine learning en AI, analyseren de overvloed aan securitymeldingen en zorgen ervoor dat enkel relevante meldingen zichtbaar worden. Zo wordt mogelijk gevaar sneller en beter opgespoord. Kies voor tools die je IT-infrastructuur 24/7 monitoren, verdachte handelingen melden en meteen uitschakelen:

- → **implementatie van monitoring- en detectietools die je IT-infrastructuur 24/7 monitoren en verdachte handelingen meteen detecteren;**
- → **het opzetten van een Security Operations Center (SOC);**
- → **gebruik van Managed Detection and Response (MDR)-diensten.**

STAP 04

Reageren op incidenten

Gehackt, wat nu? Belangrijk is om snel te reageren en ervoor te zorgen dat iedereen in je organisatie weet wat (niet) te doen:

- → **Maak een hapklaar incident response plan zodat je medewerkers meteen in actie kunnen schieten.**
- → **Communiceer open en transparant naar medewerkers en stakeholders.**
- → **Schrijf een uitgebreid rapport over het incident, de gevolgen en de genomen stappen. Dat maakt het makkelijker om de situatie te begrijpen, mogelijke pijnpunten te achterhalen en een aanval in de toekomst te vermijden.**

STAP 05

Herstel na een cyberaanval

Je bedrijf meteen terug up and running krijgen na een cyberaanval? Implementeer een strategisch disaster recovery-plan om back-upsystemen en herstelprocedures meteen te starten. Vergeet hierbij zeker ook niet om je hersteldoelstellingen te bepalen:

- → **Wat is jouw Recovery Time Objective (RTO) of ook de maximale tijd waarbij een bedrijfsproces offline mag zijn?**
- → **Wat is jouw Recovery Point Objective (RPO) of ook de maximale hoeveelheid data die verloren mag gaan, gemeten in tijd?**

Een cyberveilig bedrijf met Telenet Business

Op zoek naar een partner om jouw cybersecurity-plan uit te tekenen?
Neem contact op met één van onze experts.

Neem contact op

Business