Is uw bedrijf cyberweerbaar?

6 redenen waarom sommige bedrijven cyberaanvallen beter doorstaan

centric

Business IT Solutions

Cyberaanvallen treffen elke dag bedrijven van alle groottes. Toch is de impact lang niet overal even groot. Hoe komt het dat sommige organisaties snel herstellen, terwijl anderen wekenlang platliggen of zelfs volledig ten onder gaan?

In deze whitepaper ontdek je de zes cruciale factoren die het verschil maken. Inclusief zes praktische tips om zelf aan de slag te gaan met cybersecurity, op maat van je KMO.

centric

1. Een sterk incident response plan

Een goed voorbereid bedrijf weet precies wat te doen wanneer het misgaat.
Een incident response plan beschrijft wie welke stappen onderneemt bij een cyberincident: wie verwittig je, hoe verzamel je bewijsmateriaal, en hoe zorg je dat kritieke processen zo snel mogelijk weer draaien? Door vooraf scenario's te oefenen en medewerkers te trainen, voorkom je paniek en chaos op het moment zelf.

> Een duidelijk communicatie plan – zowel intern als extern.

Waarom dit werkt:

Snelheid is cruciaal bij een cyberaanval. Elke minuut telt. Bedrijven met een plan beperken schade én reputatieverlies.

centric

2. Regelmatige en geteste back-ups

Back-ups maken is één ding. Ze testen en vlot kunnen terugzetten is iets anders.
Wie back-ups systematisch en geautomatiseerd uitvoert én af en toe test of ze effectief werken, staat veel sterker bij dataverlies door ransomware, menselijke fouten of systeemstoringen.
Bewaar ook minstens één up-to-date kopie op een externe locatie, zodat je ook bij brand of diefstal beschermd bent.

Waarom dit werkt:

Een recente back-up is je reddingsboei. Zonder ben je overgeleverd aan hackers of verlies je weken aan werk.

centric

3. Een stevige basisbeveiliging

Cybersecurity begint bij de basis
• Digitale voetafdruk: weet waar uw informatie staat, zorg deze gelabeld is en zorg voor goede Governance rules en security
• Werk met up-to-date software en besturingssystemen
• Gebruik sterke wachtwoorden en pas ze regelmatig aan
• Activeer multi-factor authenticatie (MFA) waar mogelijk

Waarom dit werkt:

Hackers zoeken altijd de makkelijkste ingang. Wie zijn digitale voordeur stevig sluit, maakt het hen een pak moeilijker.

"Nog te veel bedrijven hebben geen volledig zicht op waar hun informatie zich bevindt, wie er toegang toe heeft, welke data ze precies bezitten of wat hun systemen allemaal doen."

centric

4. Hoge bewustwording bij medewerkers

Een groot deel van de cyberaanvallen begint met een klik op een foute link. Door medewerkers regelmatig te trainen in het herkennen van phishing, verdachte mails en andere vormen van misleiding, verhoog je de digitale alertheid binnen je organisatie. Zo bouw je stap voor stap aan een sterkere cyberweerbaarheid en verhoog je de digitale waakzaamheid binnen je organisatie.

Waarom dit werkt:

Menselijke fouten blijven de zwakste schakel in de beveiligingsketen. Door te investeren in cybersecurity awareness maak je van je medewerkers een eerste verdedigingslinie tegen aanvallen.

centric

5. Brandoefening voor cyberaanvallen (Pentesten)

Voorbereid zijn is één ding. Testen of je écht klaar bent, is nog iets anders.
Sommige bedrijven organiseren regelmatig een gesimuleerde cyberaanval – zoals een DDoS-aanval – zonder dat de medewerkers vooraf op de hoogte zijn. Zo wordt duidelijk hoe iedereen reageert, of het incidentplan goed gevolgd wordt, en waar bijgestuurd moet worden.

Na zo'n oefening (ook wel pentest of stresstest genoemd) breng je samen met IT en management de zwakke plekken in kaart. Denk aan wat er gebeurt als een cruciale applicatie uitvalt of gevoelige data uitlekt. Op basis daarvan kun je gerichter beveiligen en schade beperken bij een echte aanval.

Waarom dit werkt:

Net als een brandoefening zorgt een pentest voor betere paraatheid. Het maakt van cyberveiligheid geen papieren plan, maar een concrete reflex. En dat is precies wat nodig is bij een echte aanval.

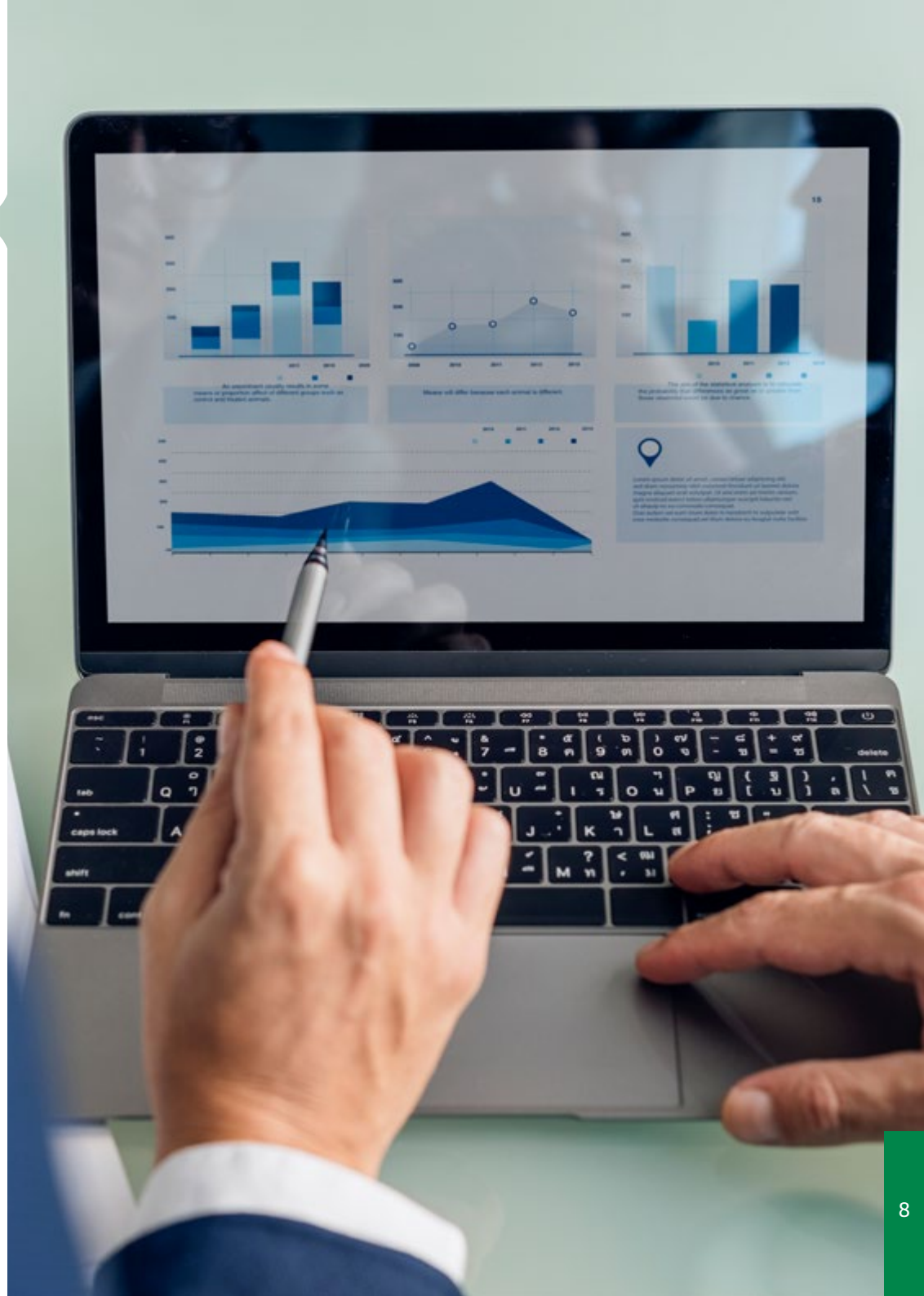
centric

6. Continue monitoring van je systemen

Detecteer problemen voor ze escaleren.
Bedrijven die hun systemen continu monitoren – via software of externe dienstverleners – kunnen afwijkingen zoals ongebruikelijke inlogpogingen snel opsporen en actie ondernemen nog voor de schade groot is.

Waarom dit werkt:

Vroegtijdige detectie betekent: sneller ingrijpen, minder schade, minder kosten.



centric

6 PRAKTISCHE TIPS VOOR EEN VEILIGE IT-OMGEVING

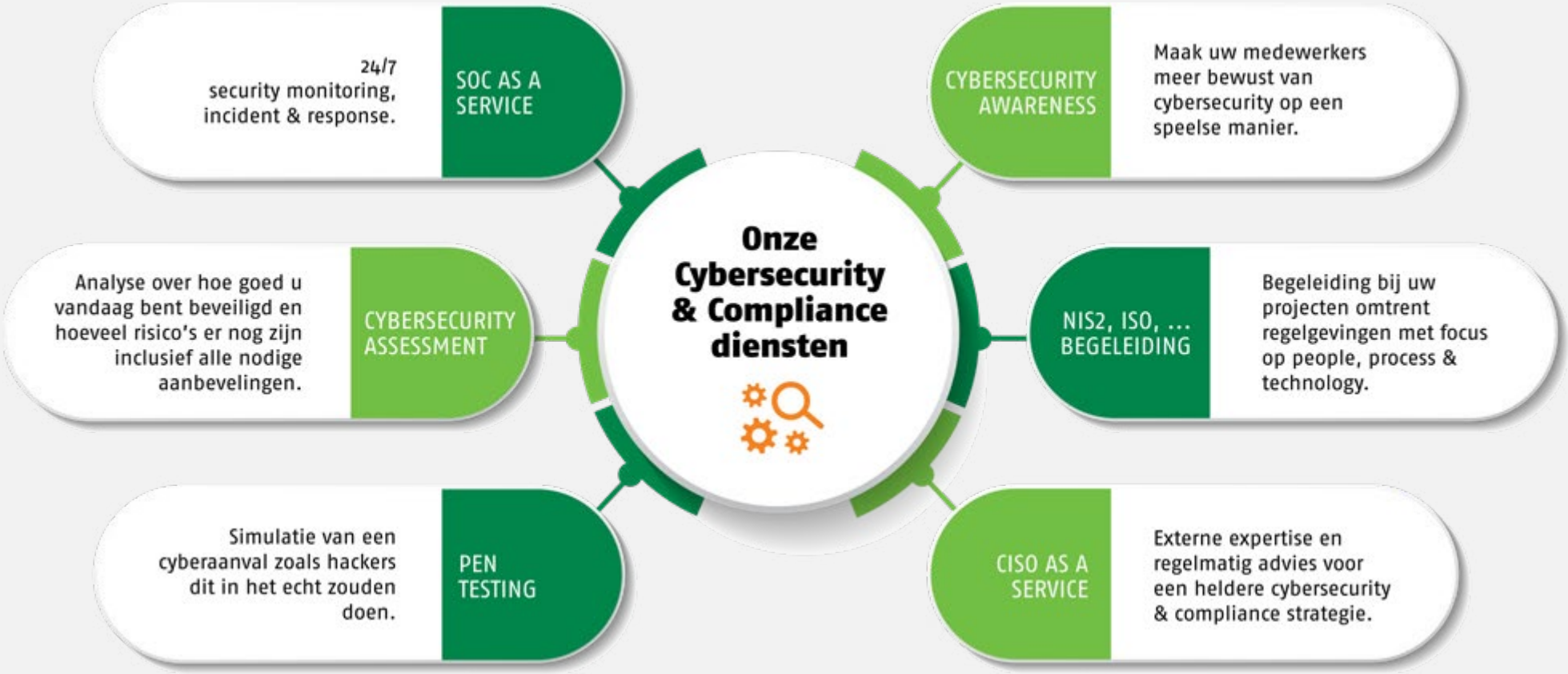
Wil je meteen stappen zetten? Begin met deze 6 basistips:	
1.	Maak back-ups (automatisch én regelmatig)
2.	Installeer updates van software en systemen
3.	Gebruik antivirussoftware en houd die actueel
4.	Activeer tweefactorauthenticatie (2FA) voor je accounts
5.	Bescherm wachtwoorden met een wachtwoordmanager
6.	Werk een incidentplan uit en hou het up-to-date

ONZE DIENSTEN

Wij bieden diensten aan om jouw beveiliging te optimaliseren om je zo meer weerbaar te maken tegen cyberdreigingen. Dit kan gaan van een initiële assessment tot het permanent monitoren van uw security. We bieden ook alle nodige begeleiding om je te laten voldoen aan alle nodige regelgevingen.

Waarom Centric?

- Begeleiding en advies op maat
- Persoonlijke aanpak
- Lokale partner
- Betrouwbaar
- Team van experten 24/7



BESLUIT

Cybercriminaliteit is een reëel risico, maar met de juiste voorbereiding en basismaatregelen kun je je bedrijf aanzienlijk weerbaarder maken. KMO's hoeven geen fort te bouwen, maar wel slim en doordacht te handelen.

Wil je weten hoe jouw organisatie ervoor staat? Of zoek je hulp bij het opstellen van een incidentplan of het beveiligen van je IT?

Neem gerust contact met ons op. We denken graag mee.

Your guiding partner in IT.

Contacteer ons:
Siemenslaan 12 | 8020 Oostkamp | Belgium
T +32 50 83 33 33 | sales.bel@centric.eu | www.centric.eu

centric