WeSecureIT
EEN SCHERPERE BLIK OP CYBERSECURITY

WHITEPAPER

Cybersecurity in het MKB

Heeft u genoeg preventieve maatregelen genomen? In een tijdperk waarin organisaties afhankelijk zijn van automatisering, internet en netwerken is cybersecurity van groot belang. Voor elk bedrijf, ongeacht omvang en sector.

Inhoudsopgave

Inleiding

Digitalisering biedt grote kansen, maar brengt ook risico's met zich mee. Waar grote bedrijven vaak uitgebreide beveiligingsmaatregelen hebben, vormt het midden- en kleinbedrijf (MKB) een aantrekkelijk doelwit voor cybercriminelen. Helaas zijn veel ondernemers zich onvoldoende bewust van de impact die een cyberaanval kan hebben op hun bedrijfsvoering, of zijn in de veronderstelling dat het bedrijf niet interessant genoeg is voor hackers. Automatische hackmachines speuren 24/7 het internet af naar open poorten en kwetsbare systemen. Helaas zien wij hier in de praktijk de vaak desastreuse gevolgen van.

Hoe hoog staat cybersecurity bij u op de agenda? Laat u dit voornamelijk over aan uw externe IT-leverancier of IT-manager? Weet u zeker dat uw IT-leverancier zijn beloftes na kan komen als een gecrasht netwerk niet meer tot leven kan worden gewekt? Zijn uw IT-systemen überhaupt ingericht naar de huidige maatstaven? Doet uw organisatie genoeg om de bescherming van persoonsgegevens te waarborgen en is dit AVG-compliant?

Zie deze whitepaper als een scherpere blik op uw cybersecurity, waarin wij u informeren over de meest voorkomende dreigingen, we praktische handvatten bieden om risico's te verkleinen en we uitleggen wat u moet doen als een aanval zich voordoet.

Een goede beveiliging begint met bewustwording en actie.

Cyberdreigingen: een overzicht

Cybercriminaliteit ligt altijd op de loer. Organisaties die een aanval hebben meegemaakt weten wat de impact is op de continuïteit en reputatie. Cybercriminaliteit kent vele vormen, maar voor het MKB zijn de volgende dreigingen het meest relevant:

Phishing

Criminelen gebruiken misleidende e-mails om gevoelige bedrijfsinformatie en wachtwoorden te stelen. 1 op de 3 datalekken in het MKB begint met een phishing-aanval.

Social engineering

Medewerkers worden gemanipuleerd om toegang te geven tot systemen.

Ransomware

Bedrijfsgegevens worden versleuteld en alleen tegen betaling vrijgegeven.

Fraude

Door onveilige inrichting van systemen mede mogelijk gemaakt of bedrijfsstilstand doordat de continuïteit van kritische systemen onvoldoende geborgd bleek te zijn.

“Toch geeft slechts 40% van de Nederlandse MKB-bedrijven aan actief bezig te zijn met cybersecurity.”

Cyberaanvallen kunnen grote gevolgen hebben, juist ook voor het MKB.

Het aantal cyberincidenten neemt toe en ook de schade wordt groter. We zien bestuurders dagelijks worstelen met de vraag: “doen we genoeg?”

Financiële schade

Herstelkosten en productiviteitsverlies lopen snel op. 60% van de kleine bedrijven die slachtoffer wordt van een cyberaanval, sluit binnen 6 maanden. Gemiddeld kost een cyberaanval in het MKB ca. € 300.000 aan directe en indirecte kosten.

Reputatieschade

Klanten verliezen vertrouwen als blijkt dat hun gegevens zijn gelekt.

Juridische implicaties

Bij het niet naleven van de wetgeving riskeert u hoge boetes.

Waar te beginnen?

Stap 1.

Prevent: Hoe u digitale risico's kunt verkleinen

Zonder IT zouden onze dagelijkse activiteiten en operationele business volledig blokkeren. Gezien deze afhankelijkheid zou IT-bescherming hoog op de agenda moeten staan. Hackers en cybercriminelen passen hun methodieken continu aan. Zijn uw cybersecuritymaatregelen dynamisch genoeg om de digitale dreiging het hoofd te bieden?

1. Basismaatregelen:

- Gebruik sterke, unieke wachtwoorden en tweestapsverificatie (MFA)
- Zorg voor regelmatige updates van software en systemen.
- Maak back-ups en test deze regelmatig.
- Zorg dat u als bestuurder bewuste keuzes kunt maken. Laat u goed informeren en weet waar u in investeert of juist niet.
- Voer een jaarlijkse risicoanalyse uit. Start met de vraag welke IT-middelen nodig zijn voor de primaire / kritische bedrijfsprocessen.

2. Bewustwording:

- Train medewerkers in het herkennen van phishing.
- Bespreek cybersecurity regelmatig binnen uw bedrijf.
- Blijf op de hoogte van wet- en regelgeving zoals NIS2.

3. Technologische oplossingen:

- Installeer beschermingsmiddelen zoals: firewalls, endpoint security, EDR.
- Monitor actief de beschermingsoplossingen. Bij verdachte activiteiten dient snel actie te kunnen worden ondernomen.

4. Organisatorisch:

- Zorg voor gedocumenteerde contracten en afspraken met dienstverleners en leveranciers.
- Zorg voor een intern overzicht van alle assets.
- Laat periodieke audits uitvoeren door experts, zoals WeSecureIT. (cybersecurity is een vak apart en vergt andersoortige kennis dan automatisering alleen.

Nu ontdekken wat u achteraf graag had willen weten (preventief, Cyber Security Audit en Cyber RI&E)

Next

Stap 2.
Perform: Cybersecurity als onderdeel van uw bedrijfsvoering

Perform draait om gestructureerd bezig zijn met cybersecurity. Bedrijfsprocessen en IT-afhankelijkheden goed in kaart hebben, evenals kritieke punten herkennen. Dat betekent de optimale balans vinden tussen gebruikersgemak, cybersecurity en budget.

- Informatiebeveiligingsbeleid: Stel beleid en protocollen op en evalueer dit periodiek.
- Incident response plan: Wees voorbereid op onverwachte situaties. Verwacht het onverwachte en speel daar op in.
- Samenwerking: een specialist die met u meekijkt om meer ROI te behalen door het gebruik van slimme oplossingen en gestructueerd werken.
- Continuïteit: Zorg voor doorlopend toezicht en optimalisatie van uw beveiliging.

Next

Stap 3.
React: Wat te doen na een cyberaanval

Zelfs met goede beveiliging kan een aanval plaatsvinden. Of het nu gaat om een gehackt mailaccount, malware op een systeem of dataverlies na een harde schijf crash. Vele experts en collega's gingen ons voor in deze uitspraak: "Het is niet zozeer de vraag of uw organisatie te maken krijgt met een incident, maar wanneer." Is uw organisatie voorbereid en weet u hoe te handelen als u toch slachtoffer wordt?

1. Eerste stapen:

- Koppel getroffen systemen los van het netwerk (isoleer het incident)
- Pak het IRP erbij. Verzamel de juiste mensen bij elkaar. Denk aan proceseigenaren, bestuurders en managers. Formeer een crisiteam.

2. Forensisch onderzoek:

- Meld het incident bij relevante instanties en stakeholders.
- Laat vaststellen wat er is gebeurd, welke gegevens zijn aangetast en of er nog ongewenst gedrag op het netwerk plaatsvindt.

3. Communicatie:

- Informeer medewerkers, klanten en partners eerlijk en transparant.

4. Herstel en preventie:

- Herstel de schade en neem maatregelen om herhaling te voorkomen.

Veel van de acties zullen gelijktijdig plaatsvinden.
Schakel onze **digitale noodhulp in** om u hierin te begeleiden

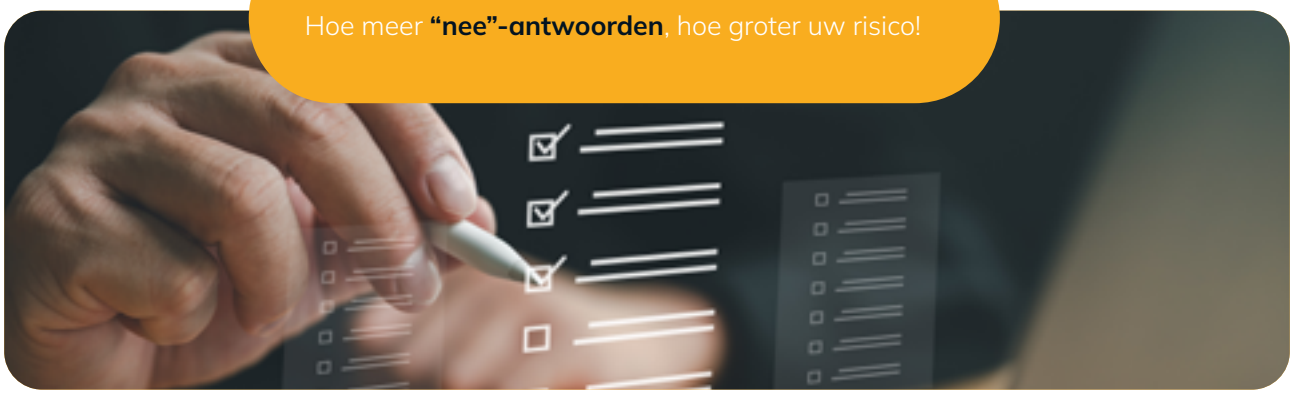
Zelfscan 10 cruciale vragen om uw risico te bepalen

Gebruik deze ja/nee-vragen om te beoordelen hoe goed uw bedrijf is beveiligd:

1. Heeft u uw maximaal aanvaardbare downtime en financiële schade in kaart gebracht?
2. Heeft u een actueel informatiebeveiligingsbeleid?
3. Zijn al uw software en systemen up-to-date?
4. Worden er regelmatig back-ups gemaakt en worden deze actief getest?
5. Zijn uw medewerkers getraind in het herkennen van o.a. phishing?
6. Zijn alle systemen voorzien van next-gen endpoint protectie / EDR / firewall?
7. Heeft u een incident response plan (IRP)?
8. Worden uw netwerken en systemen regelmatig gecontroleerd op kwetsbaarheden?
9. Heeft u inzicht in wie wanneer toegang heeft tot welke systemen?
10. Heeft u uw IT-omgeving wel eens laten testen door een onafhankelijke deskundige?

Bonusvraag:
Heeft u als eindverantwoordelijke bij het beantwoorden van vragen aannames gedaan?
Zo ja, plan eens een **vrijblijvende brainstormsessie** in met één van onze experts!

Hoe meer **“nee”-antwoorden**, hoe groter uw risico!



Conclusie

De digitale dreiging is enorm toegenomen. De afhankelijkheid van automatisering is ook toegenomen. Organisaties worden door digitale criminelen met één druk op de knop out-of-business gezet. Volautomatische hackmachines speuren het internet af op zoek naar kwetsbare systemen en zwakke wachtwoorden. De kans om gehackt te worden (een digitale inbraak) is 50 keer groter dan de kans op een bedrijfsinbraak!

Cybersecurity is cruciaal voor elk MKB-bedrijf. Deze whitepaper heeft u inzicht gegeven in de dreigingen, maatregelen om risico's te beperken en hoe u kunt handelen na een aanval. De belangrijkste boodschap: wacht niet tot het te laat is. Neem vandaag nog actie.

WeSecureIT
085 – 4012 740
contact@wesecureit.nl
www.wesecureit.nl