

Niet óf. **Maar wanneer.**

Hoe je je bedrijf voorbereidt op een
cyberaanval. Zonder bangmakerij.

Whitepaper 01

OctaOne · Jean de Jongh

Parkweg 37, 4153 XL Beesd

0345 782 500 · help@octaone.nl · octaone.nl

01 — MAANDAGOGHTEND

Kwart voor acht.

Een collega belt. Hij kan niet in de boekhouding. Even later de volgende. Bestanden heten ineens anders. Op het bureaublad staat een tekstbestand. Met een bitcoinadres.

Dat is het moment waarop je ontdekt of je voorbereid bent.

Niet daarvoor.

Ik had hier een pagina vol statistieken kunnen zetten. Stijgende aanvalscijfers, getroffen sectoren, percentages. Ze kloppen vast. Maar je kent ze al. En ze veranderen niets aan je maandagochtend.

Nou en.

Dus geen bangmakerij. Wel wat ik zie werken. En wat ik zie misgaan.

02 — HET GAT

Waarom juist het MKB.

Grote bedrijven hebben een securityteam. Een CISO. Budget.

Het MKB heeft "iemand die er verstand van heeft". Een IT'er die eens per maand langskomt. Of een leverancier die zegt dat Microsoft of Google het allemaal regelt.

Dat is geen verwijt. Het is de realiteit.

Aanvallers weten dat ook. Een MKB-bedrijf is zelden een doelwit. Het is een gelegenheid. Een wachtwoord dat al jaren hetzelfde is. Een laptop die maanden geen update kreeg. Een medewerker die op een overtuigende mail klikt.

En wat ik vaak zie: alle aandacht gaat naar de voordeur. Virusscanner, firewall, klaar. Maar wie merkt het als er toch iemand binnen is? En wie weet wat er dan moet gebeuren?

Daar zit het gat. Niet in de techniek. **In het plan.**

03 — BOUWEN

Vijf bouwstenen.

Cybersecurity is geen product. Je koopt het niet. Je bouwt het. En je blijft bouwen.

1. Weet wat je kroonjuwelen zijn

Begin niet bij techniek. Begin bij je bedrijf. Welke systemen moeten altijd draaien? Welke data mag nooit op straat liggen? Hoeveel uur stilstand overleef je?

Wie dat niet weet, beveiligt alles een beetje. En dus niets goed.

2. Mensen, niet alleen machines

De meeste aanvallen beginnen niet met een hack. Ze beginnen met een mail. Een nepfactuur. Een "directeur" die dringend geld wil laten overmaken.

Train je mensen. Niet één keer per jaar met een saaie presentatie. Kort, regelmatig, met echte voorbeelden en phishingtests. En leg vast wie waarvoor verantwoordelijk is. Klinkt als papierwerk. Is het niet.

Je mensen zijn de zwakste schakel. Of de sterkste.

3. Zien wat er gebeurt

Een virusscanner was ooit genoeg. Die tijd is voorbij.

Je wilt weten wat er op je laptops en telefoons gebeurt. Dat heet EDR: endpoint detection & response. En je wilt signalen uit al je systemen bij elkaar zien. Dat heet SIEM. Niet voor mooie dashboards. Om in te grijpen voordat het escaleert.

Detectie zonder actie is een dure alarmbel.

4. Een netwerk dat je niet ziet

Het netwerk is je ruggengraat. En vaak je voordeur. Deel het op in zones, zodat één besmette laptop niet meteen bij je administratie kan. Behandel thuiswerkers net zo streng als kantoor.

Een goed netwerk merk je niet. Een slecht netwerk wel.

5. Plan het herstel

Laat ik nuanceren. Je kunt veel voorkomen. Niet alles.

Dus de vraag is niet alleen: hoe hou ik ze buiten? Maar ook: hoe snel draai ik weer? Een back-up die je nooit hebt teruggezet, is hoop. Geen back-up. Een herstelplan dat alleen in iemands hoofd zit, is geen plan.

Test het op een rustige dinsdag. **Niet op die maandagochtend.**

04 — MORGEN

Tien dingen die je morgen kunt doen.

Geen geheimen. Gewoon de basis.

- 1 **Zet MFA aan voor iedereen.** Ook voor de directeur. Juist voor de directeur.
- 2 **Laat updates automatisch lopen.** Systemen, apps, besturingssystemen. Uitstellen is uitnodigen.
- 3 **Schrijf je kroonjuwelen op.** Eén A4. Wat moet altijd werken, wat mag nooit lekken.
- 4 **Scheid beheer van dagelijks werk.** Beheerrechten? Dan een apart account, alleen daarvoor.
- 5 **Deel je netwerk op.** Gasten, kantoor, printers en camera's: elk een eigen zone.
- 6 **Vertrouw niemand standaard.** Zero trust: elke toegang wordt gecontroleerd. Ook van binnenuit.
- 7 **Train kort en vaak.** Eén phishingtest zegt meer dan tien presentaties.
- 8 **Versleutel wat gevoelig is.** Laptops, opslag, verzending. Een verloren laptop is dan vervelend. Niet rampzalig.
- 9 **Test je back-up.** Zet echt iets terug. Meet hoe lang het duurt.
- 10 **Laat iemand onafhankelijk meekijken.** Niet degene die het heeft ingericht. Een tweede paar ogen ziet wat het eerste mist.

05 — T O T S L O T

Je kunt dit zelf.

Ik ga je niet vertellen dat je bij mij moet zijn. Deze tien punten kun je zelf. Of met je huidige IT-partner.

Wil je toch een tweede paar ogen? Dan kijk ik graag mee. Gewoon: waar sta je, en wat is de volgende stap.

Strategie eerst. Tech volgt wel.

Jean de Jongh

OctaOne, Beesd

Rust in je IT geeft **ruimte aan je bedrijf.**

Ik geloof dat technologie pas waarde heeft als mensen haar begrijpen en kunnen gebruiken. Daarom begint bij OctaOne alles bij de medewerker. Niet bij het product. En daarom geef ik weg wat ik weet. Deze whitepaper is daar een stukje van.

• Slim werken

• Verbonden blijven

• Beveiligd zijn

• Betrokken blijven

OVER DE SCHRIJVER

Jean de Jongh

Ruim twintig jaar in IT. Mijn eerste bedrijf startte ik op 1 oktober 2001. De afgelopen jaren hielp ik grote organisaties in Nederland, België en Duitsland met security en strategie.

Nu doe ik dat voor het MKB. Vanuit Beesd. Met een voorkeur voor objectief boven subjectief, en voor oplossingen die over vijf jaar nog kloppen.

Strategie eerst. Tech volgt wel.

VOLGENDE STAP

Even sparren?

Plan een gesprek

Geen verkooppraatje. Gewoon kijken waar je staat en wat de volgende stap is. Remote, bij jou op locatie, of bij ons in Beesd.

Afspraak plannen →

octaone.nl/afspraak



Telefoon

0345 782 500



E-mail

help@octaone.nl



Web

octaone.nl

