Ik maak me zorgen over mijn cybersecurity. Hoe sta ik ervoor?

Checklist voor MKB-ondernemers

Cybersecurity hoeft niet je hoofdtaak te worden. Je moet er wel grip op hebben. Met deze checklist zie je in een paar minuten waar je staat. Beantwoord elke vraag eerlijk met ja of nee.

Vraag	Ja	Nee
KOERS EN REGIE		
1. Ik weet wat ik met cybersecurity wil bereiken. Bijvoorbeeld: klantgegevens goed beveiligen, zonder dat het werk onwerkbaar wordt. Met een helder doel kies je makkelijker welke maatregelen nodig zijn, en welke niet.	☐	☐
2. Er is één persoon die cybersecurity in mijn bedrijf in de gaten houdt. Dat hoeft geen IT'er te zijn. Wel iemand die afspraken bewaakt, vragen verzamelt en weet wie er gebeld moet worden.	☐	☐
3. Ik weet wat mijn IT-leverancier voor me regelt, en wat niet. Wie maakt de back-ups, wie installeert updates, en staat beveiliging in het contract? Ga er niet van uit dat het geregeld is omdat je bedrijf klein is.	☐	☐
JE HUIS OP ORDE		
4. Ik weet welke apps en systemen we gebruiken, en welke gegevens erin staan. Klantgegevens, administratie, offertes: staan ze in de cloud, op een laptop of bij een leverancier? Je kunt alleen beschermen wat je kent.	☐	☐
5. Ik weet wie toegang heeft tot welke apps. Medewerkers, maar ook oud-collega's, stagiairs, freelancers en je IT-leverancier. Iedereen met een account is een mogelijke ingang.	☐	☐
6. Als iemand vertrekt, heeft die daarna geen toegang meer. Accounts die blijven bestaan na vertrek zijn een van de makkelijkste ingangen voor misbruik. Toegang intrekken hoort standaard bij elk vertrek.	☐	☐
7. We hebben een wachtwoordbeleid, een wachtwoordmanager en tweestapsverificatie (MFA). Sterke, unieke wachtwoorden onthoudt niemand, een wachtwoordmanager wel. En met MFA is een gestolen wachtwoord alleen niet genoeg om binnen te komen.	☐	☐
8. We hebben een back-up, en ik weet dat we die ook echt kunnen terugzetten. Een back-up die nooit getest is, is vooral hoop. Haal af en toe een bestand terug om te zien of het werkt.	☐	☐

Vraag	Ja	Nee
9. We delen bestanden via een link, niet als bijlage. Een link naar bijvoorbeeld OneDrive kun je intrekken, een verstuurde bijlage niet. Zo blijft je data op één plek en houd jij de controle.	☐	☐
10. Iedereen die met onze gegevens werkt, heeft een geheimhoudingsverklaring getekend. Medewerkers, maar ook freelancers en stagiairs. Zo is voor iedereen duidelijk wat er van ze verwacht wordt.	☐	☐
ALS HET MISGAAT		
11. Ik weet wat ik moet doen bij een cyberincident of een datalek. Wie bel je als eerste? Wat moet je melden, en binnen welke termijn? Op het moment zelf is er geen tijd om dat uit te zoeken.	☐	☐
12. Mijn medewerkers weten dat ze zich niet hoeven te schamen als ze per ongeluk op een phishinglink hebben geklikt. Iedereen kan erin trappen. Wie zich schaamt, meldt het niet of te laat. Wie zich veilig voelt, meldt het meteen, en dan kun je de schade beperken.	☐	☐

MEER JA KUNNEN ANTWOORDEN?

Wil je op meer punten van deze checklist ja kunnen antwoorden? Maar heb je geen zin om de kennis hiervoor zelf op te bouwen? Neem dan geheel vrijblijvend contact met ons op.

Wij scheiden zin van onzin, zodat jij grip krijgt en zelf de regie houdt.

janot@noordpunt.nl · lotta@noordpunt.nl · noordpunt.nl