ABN·AMRO

Veilig zaken doen

De 9 cybersecurity essentials voor MKB in 2020

1 Beveilig uw online domein

- Vergrendel het domein
- Schakel domein privacy in
- Beveilig domein configuratie (o.a. SSL, DNSSEC)

2 Bescherm gebruikers tegen Phishing

- Schakel webfilters in en zorg voor veilige browsers
- Voer email beveiliging in (b.v. DMARC)

3 Creëer awareness rondom cyber security

- Zorg ervoor dat het management op de hoogte is van kritieke assets en cyber dreigingen zoals phishing
- Zorg ervoor dat er een cybersecurity awareness programma is dat werknemers kunnen volgen

4 Faciliteer een veilige digitale werkplek

- Beveilig toegangsgegevens met sterke wachtwoorden en tokens (MFA)
- Schakel antivirus in op eindpunten
- Hanteer beveiligingsconfiguratie (bijvoorbeeld Safe USB-beleid) op eindpunten
- Beveilig externe toegang (VPN) tot uw organisatie

5 Voorkom exploitatie van uw IT

- Sta alleen het gebruik van geautoriseerde software toe
- Identificeer kwetsbaarheden in IT-systemen en zorg ervoor dat beveiligingspatches worden toegepast
- Houd uw software up-to-date

6 Beveilig uw netwerkomgeving

- Beveilig en beheer uw netwerkperimeter
- Beveilig WIFI toegangspunten

7 Zorg dat uw IT activiteiten weerbaar zijn

- Identificeer en maak back-ups van kritieke gegevens
- Zorg ervoor dat kritieke IT-systemen kunnen worden hersteld na een ramp
- Maak een plan om te reageren op cyberbeveiligingsincidenten

8 Doe zaken met veilige leveranciers

- Zorg ervoor dat uw leveranciers beveiligingsbewust zijn en / of voldoen aan door de industrie erkende beveiligingscertificeringen

9 Neem een cyber verzekering

- Kies een cyberverzekering met voldoende dekking

Voor meer informatie over veilig zaken doen, ga naar:
abnamro.nl/zakelijk/veiligzakendoen
of e-mail: **cybersecurity@nl.abnamro.com**