Voor je het weet bescherm je je bedrijf tegen cybercriminelen

Start met deze 7 maatregelen

Veilig ondernemen.
Daar maken we ons sterk voor.

PVO

Start met de cyberveiligheid van jouw bedrijf met de volgende 7 maatregelen

1 Maak een back-up

Een kopie van je bestanden kan een laatste redmiddel zijn als je systeem is gehackt. Zorg daarom voor één of meerdere kopieën van je bedrijfsgegevens, zoals je klantdata en dossiers en/of van je gehele systeem. Werk je in de cloud? Let dan op, kijk goed waar je gegevens staan opgeslagen en of je hier ook een back-up van hebt.

2 Log veilig in

Met multifactorauthenticatie (MFA) voeg je aan het inloggen met een wachtwoord nog een extra beveiligingslaag toe. Een voorbeeld van een extra stap is dat er een sms met een toegangscode naar je smartphone wordt gestuurd. Of je ontgrendelt je account met een code van een authenticatieapp of via je vingerafdruk. Stel MFA op zoveel mogelijk plekken in, in ieder geval bij je zakelijke e-mailaccount en de belangrijke applicaties en systemen voor je bedrijf. Zo maak je het moeilijker voor een onbevoegde om toegang te krijgen tot je gegevens.

3 Zet automatisch updaten aan

Software-updates bevatten vaak ook beveiligingsupdates. Voer je een update niet of later uit, dan kan je beveiliging kwetsbaar worden. Zet daarom bij voorkeur ‘automatisch updaten’ aan voor apparaten die met het internet zijn verbonden. Denk hierbij niet alleen aan je computer of smartphone, maar ook aan je printer, slimme deurbel, website, server en router.

4 Installeer antivirussoftware

Installeer een antivirusprogramma en zorg dat deze software up-to-date blijft. Doe dit op alle computers, telefoons en servers binnen je bedrijf. Zo loop je minder risico op schade door virussen en andere malware.

5 Check beveiliging

Via internet.nl controleer je of jouw e-mailsysteem en website voldoen aan moderne beveiligingsstandaarden. En als dat niet zo is, hoe je dat kunt verbeteren. Met een goede beveiliging voorkom je dat cybercriminelen je identiteit misbruiken om spam zoals phishing te versturen. Ook kan het verkeer op je website niet afgeluisterd of gemanipuleerd worden.

6 Herken phishing

Phishing is een groot gevaar voor iedere onderneming. Bij deze vorm van digitale oplichting misleiden fraudeurs je met nep e-mails, QR-codes, telefoontjes, sms of WhatsAppberichten. Trap je erin? Dan kun je onbedoeld gevoelige informatie prijsgeven, zoals wachtwoorden of betaalgegevens. Maak jezelf en je medewerkers alert en zorg ervoor dat jullie phishing kunnen herkennen. De phishingquiz of phishingbingo van het Digital Trust Center kunnen je daarbij helpen.

7 Print een bellijst

Bij een cyberincident is het belangrijk om te weten wie je kunt bellen om jou te ondersteunen. Bij zo'n incident telt elke seconde. Zorg er daarom voor dat je een geprinte bellijst met de contactgegevens van je IT-dienstverlener, softwareleverancier of securitybedrijf hebt klaarliggen.

digitaltrustcenter.nl/starten

Digital Trust Center (DTC)

Op de website van het Digital Trust Center (DTC) vind je meer uitleg over deze 7 maatregelen.

Kom je er zelf niet uit? Vraag dan je IT-dienstverlener dit voor je te doen.

PVO Nederland
Churchilllaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht
www.pvo-nl.nl

Veilig ondernemen.
Daar maken we ons sterk voor.