To-do lijst: Cyberevent Wijk bij Duurstede

Tijdens het Cyberevent Wijk bij Duurstede hebben we stilgestaan bij de 5 basisprincipes van digitaal veilig ondernemen van het Digital Trust Center (www.digitaltrustcenter.nl). Om deze basisprincipes iets praktischer te maken hebben we een to-do lijst opgesteld van de 7 belangrijkste maatregelen rondom deze basisprincipes. Zodat jij jouw onderneming een stukje weerbaarder kan maken!

1. Maak een back-up van je belangrijkste bestanden

Een reservekopie kan een laatste redmiddel zijn als je bedrijf is aangevallen. Zorg daarom voor één of meerdere kopieën van je bedrijfsgegevens, zoals je klantdata en dossiers. Zo'n kopie heet ook wel een back-up. Kopieer de belangrijkste bestanden naar een externe harde schijf, koppel deze vervolgens los en berg deze op een veilige plaats op. En bewaar minimaal één back-up op een andere locatie.

Werk je in de cloud? Let dan op, dit betekent niet dat er automatisch een back-up van je gegevens wordt gemaakt.

2. Stel Multi Factor Authentication in (MFA)

- Bedenk goed voor welke informatie het belangrijk is dat het door MFA wordt beschermd. Denk hierbij aan systemen die toegang geven tot klant-, financiële- of bedrijfsgegevens. Je kunt hiervoor een risicoanalyse doen;
- Maak een plan hoe je toegang tot die gegevens wilt beschermen;
- Kies een MFA-methode die bij je plan past;
- Zorg ervoor dat (indien van toepassing) medewerkers en accountgebruikers weten hoe het werkt;
- Zet MFA aan en zorg ervoor dat iedereen het gebruikt;

3. Zet automatische updates aan

Software-updates bevatten vaak verbeteringen voor de gebruiker. Ook bevatten ze vaak beveiligingsupdates. Voer je een update niet of later uit, dan kan je beveiliging kwetsbaar worden. Zo kan er bijvoorbeeld een beveiligingslek ontstaan. Kwaadwillenden zoeken actief naar manieren om binnen te dringen via zo'n lek.

Wacht daarom niet met het updaten van apparaten die met het internet verbonden zijn. Zet bij voorkeur 'automatisch updaten' aan. Denk hierbij niet alleen aan je computer of smartphone, maar ook aan je printer, slimme deurbel, website, server en router.

4. Gebruik antivirussoftware

Een antivirusprogramma of antivirussoftware die je beschermt tegen internetvirussen en 'malware' is op veel apparaten inmiddels standaard aanwezig. Soms kun je ook zelf een antivirusproduct kiezen.

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. Controleer de beveiligingsstandaarden van je e-mail

Via internet.nl controleer je de beveiliging van je e-mailadres en domeinen. De website vertelt of je e-mailadres en/of domeinnaam voldoet aan moderne beveiligingsstandaarden. Zo krijg je een beeld van hoe jouw website en e-maildomeinen ervoor staan qua veiligheid.

6. Leer phishing herkennen (zie phishingbingo)

- Controleer altijd het e-mailadres, de afzender en de inhoud van een bericht. Let daarbij op onder andere deze punten:
- Controleer of de domeinnaam en het e-mailadres van de afzender hetzelfde zijn.
- Controleer of de domeinnaam overeenkomt met het website-adres.
- Let op de details: zie jij het verschil tussen info@31008mailers.nl en info@3I008mailers.nl?
- Klik niet op een link als je het niet vertrouwt, maar beweeg (hoover) met de aanwijzer van je muis over de link. Zo ontdek je waar de link écht naar toe gaat.

7. Print een bellijst voor noodsituaties

Heb je door een cyberaanval geen toegang meer tot je informatiesystemen? Dan is er sprake van een noodgeval. Zorg er daarom voor dat de contactgegevens van je IT-dienstverlener, softwareleverancier of securitybedrijf uitgeprint klaarliggen.
Bekijk een voorbeeld van zo'n bellijst.

Heb je belangrijke klanten en (keten)partners? Zorg er dan ook voor dat jouw IT-dienstverlener bij hen geregistreerd staat als contactpersoon.

Wil je meer specifieke informatie over jouw cyberveiligheid? Doen dan via de site van het Digital Trust Center de CyberVeilig Check.

Websites om eens te bezoeken:

• www.digitaltrustcenter.nl	Meer tips over digitaal veilig ondernemen
• www.digitaalveilig.com	Informatie over cybercriminaliteit
• www.nomoreransom.org	Wat is ransomware en wat kan je ertegen doen?
• www.haveibeenpwned.com	Zijn jouw gegevens betrokken geweest bij een hack?
• www.politie.nl/checkjehack	Zijn jouw gegevens laatst gelekt?
• www.hackhelpdesk.nl	Wat doe je als je bent gehackt?
• www.samendigitaalveilig.nl	Houd de kennis van jezelf en je medewerkers op orde.

Bedankt voor je aanwezigheid.

PVO / Midden-Nederland

info@pvo-middennederland.nl
www.pvo-middennederland.nl