

Versterk je digitale weerbaarheid:

5 basisprincipes voor jou als ondernemer

Als Limburgse ondernemer sta je dagelijks voor diverse uitdagingen, en digitale dreigingen vormen daar geen uitzondering op. Je wilt de bedrijfscontinuïteit waarborgen en jezelf beschermen tegen cyberrisico's die je bedrijf in gevaar kunnen brengen. Maar hoe versterk je jouw digitale weerbaarheid op een effectieve manier?

Ontdek de 5 basisprincipes van veilig digitaal ondernemen, speciaal opgesteld voor jou als ondernemer door Digital Trust Center. Van het inventariseren van kwetsbaarheden tot het voorkomen van virussen en malware, deze principes zullen je helpen om je digitale basisbeveiliging op orde te brengen. Bereid je voor om de uitdagingen aan te gaan en je bedrijf te beschermen in de digitale wereld.

1. Inventariseer kwetsbaarheden

Begin met het inventariseren van de ICT-onderdelen en kwetsbaarheden binnen je organisatie. Voer een risicoanalyse uit en breng in kaart welke hardware, software en klantgegevens aanwezig zijn. Let daarbij op:

- ▼ Beschikbaarheid (kun je nog bij je gegevens of apparatuur?)
Integriteit (kloppen de gegevens nog en kun je dat checken?)
- ▼ Vertrouwelijkheid van gegevens (wat gebeurt er als data in vreemde handen komen?)

Dit helpt je de kwetsbaarheden van je organisatie en de mogelijke impact van cyberincidenten te begrijpen. Je kunt gebruikmaken van de Cyberscan van PVO-Limburg als hulpmiddel bij dit proces.

2. Kies veilige instellingen

Standaardinstellingen van apparatuur en software zijn vaak bekend bij kwaadwillenden. Controleer de instellingen van je apparatuur, software en netwerk- en internetverbindingen en pas de standaardinstellingen aan. Indien nodig kun je ook een expert inschakelen om hierbij te helpen.

3. Voer updates uit

Apparaten en software worden voortdurend doorontwikkeld door de fabrikanten. Controleer regelmatig of er updates beschikbaar zijn en installeer de laatste beveiligingsupdates direct. Schakel waar mogelijk automatische updates in, zodat je altijd gebruikmaakt van de meest recente versies van apparatuur en software.

4. Beperk toegang

Wees zorgvuldig bij het verlenen van toegang tot systemen en gegevens. Bepaal per medewerker welke toegang nodig is om hun werkzaamheden uit te voeren. Beperk uitgebreide toegangsrechten tot alleen degenen die het nodig hebben.

Zorg ervoor dat de toegang tot systemen adequaat is afgeschermd. Gebruik sterke wachtwoorden met minimaal 14 tekens, maak gebruik van multi-factor authenticatie en implementeer een wachtwoordmanagementbeleid. Deze maatregelen maken het aanzienlijk moeilijker voor onbevoegden om toegang te krijgen.

5. Voorkom virussen en andere malware

- ▼ Zorg voor bewustwording bij medewerkers over risico's en bedreigingen en stimuleer veilig gedrag. Online- en offline-trainingen kunnen hierbij helpen.
- ▼ Gebruik beschermingssoftware op al je apparaten, zoals laptops, tablets en smartphones. Installeer alleen apps van vertrouwde bronnen en verwijder ongebruikte apps.
- ▼ Beperk de mogelijkheden voor het installeren van software.

Als je hulp nodig hebt bij het implementeren van de vijf basisprincipes van veilig digitaal ondernemen of als je meer wilt weten over de Cyberscan, aarzel dan niet en neem contact op met PVO Limburg. Samen kunnen we werken aan het vergroten van jouw digitale weerbaarheid en het beschermen van je bedrijf tegen cyberrisico's.

Scan de QR code voor meer info over PVO-Limburg of neem contact op via onderstaande gegevens:

telefoon: 0475-792008 **email:** info@pvo-limburg.nl

