Uiterwijk Winkel VERZEKERINGEN sinds 1929

Preventie adviezen

Ook als u geen ICT expert bent, kunt u veel doen om het risico op een cyberincident te verminderen.

Bewustwording van medewerkers

- Weten uw medewerkers hoe ze een phising mail kunnen herkennen?
- Zijn ze bekend met uw veiligheids- en privacy beleid en weten ze waarom dit beleid er is?
- Weten uw medewerkers wat ze moeten doen als ze een datalek hebben veroorzaakt of op een (mogelijk) foute link geklikt hebben?
- Weten uw medewerkers dat zij nooit op openbare netwerken mogen inloggen om te werken?

Zorg voor een goed log-in beleid

- Heeft u een wachtwoordbeleid en wordt dit door alle medewerkers gevolgd?
- Geldt dit beleid voor alle wachtwoorden? Bijvoorbeeld ook voor social media accounts of voor uw wifi netwerk voor gasten?
- Maakt u gebruik van tweestapsverificatie?

Beperk autorisaties

- Heeft u de autorisaties in uw software beperkt zodat medewerkers niet onnodig toegang hebben tot alle systemen?
- Worden toegangsrechten aangepast als iemand een nieuwe functie krijgt of uit dienst treedt?

Inventariseer risico's

- Weet u welke programma's of machines kritiek zijn voor uw bedrijfsvoering?
- Welke data is cruciaal voor uw bedrijfsvoering?
- Hoe erg is het als uw computersysteem uitvalt? Kunt u dan nog doorwerken?
- Weet u welke apparaten gebruik maken van het internet en aangesloten zijn op uw netwerk (internet of things)
- Zijn persoonsgegevens goed afgeschermd?voor uw bedrijfsvoering?
- Als u ICT-diensten heeft uitbesteed, heeft u dan goede afspraken gemaakt over wat u kunt verwachten van uw dienstverlener bij een incident?

Zorg voor goede back-ups

- Heeft u van al uw belangrijke gegevens en documenten een recente (offline) back-up?
- Bewaart u deze back-up apart van uw netwerk?

Voer updates uit

- Installeert u altijd direct de meest recente software updates en security patches, op uw software?
- Doet u dit ook voor apparaten waarop software aanwezig is?

Gebruik antivirus

- Heeft u op al uw (mobiele) apparaten antivirussoftware geïnstalleerd? Worden de apparaten regelmatig gescand?

Datalekbeleid

- Is er iemand in uw bedrijf die goed op de hoogte is van wat wel of geen datalek is?
- Zijn er processen om een datalek tijdig te melden?

Wifi voor gasten

- Is het wifi netwerk voor gasten gescheiden van uw eigen netwerk?
- Is dit netwerk beveiligd met een wachtwoord dat regelmatig gewijzigd wordt?

Continuïteitsplan

- Heeft u een continuïteitsplan dat gevolgd kan worden als er iets mis is?
- Is dit plan breder bekend binnen uw onderneming, bijvoorbeeld bij ICT als zij ongebruikelijke activiteiten op het netwerk signaleren?
- Wordt dit plan regelmatig getest?
- Wordt dit plan doorlopend geüpdatet?