OMGAAN MET CYBERCRIME: ZO BESCHERM JE JE ONDERNEMING

Als ondernemer loop je risico op aanvallen van cybercriminelen. Beveiligingssoftware houdt slechts een deel van de cybercrime tegen. Daarom is het belangrijk om jezelf, je bedrijf én de privacy van jouw klanten hiertegen te beschermen. Maar hoe doe je dat? En wat doe je als je toch slachtoffer wordt van cybercrime?

Volgens het CBS is 1 op de 10 Nederlandse bedrijven jaarlijks slachtoffer van cybercrime. Dat is een hoog aantal. Werk je in jouw onderneming veel met digitale systemen? Dan is het extra belangrijk om hier aandacht aan te besteden.

Unieke wachtwoorden en tweestapsverificatie

Een belangrijke manier om de toegang tot je systemen en social media-accounts te beveiligen is door unieke wachtwoorden te gebruiken. Gebruik dus niet voor elk account of systeem hetzelfde wachtwoord. Daarnaast kun je met tweestapsverificatie zorgen voor extra beveiliging. Dat wil zeggen dat je naast je wachtwoord of pincode ook nog op een andere manier laat zien dat je toegang mag kijken tot een account. Bijvoorbeeld door een extra code in te vullen, die je op je telefoon ontvangt.

Maak goede afspraken met je medewerkers

Zorg dat je goede afspraken maakt met je medewerkers en dat zij zich bewust zijn van de risico's van cybercrime. Laat medewerkers bijvoorbeeld regelmatig hun wachtwoorden veranderen en zorg dat zij hun wachtwoorden niet met anderen delen. Regel ook goed wie waartoe toegang heeft. Een beleidsmedewerker hoeft bijvoorbeeld geen toegang te hebben tot de financiële administratie.

Blijf up-to-date

Sotware updaten is vaak zo'n klusje dat blijft liggen, omdat het precies even niet uitkomt. Toch maar niet meer uitstellen, want softwareupdates repareren zwakke plekken in de oude software. Installeer dus altijd direct je updates voor je programma's en beveiligingssoftware. Nog beter: stel automatisch updaten in. Zo kun je je eigen uitstelgedrag voorkomen.

Veilig opslaan

Wellicht ten overvloede, maar als je je elke dag met hart en ziel inzet voor jouw onderneming wil je natuurlijk niet dat bestanden kwijtraken. Maak daarom regelmatig back-ups van je data en sla deze op verschillende plekken op.

Werk je met klantgegevens, zoals adressen en facturen? Dan werk je met privacygevoelige informatie. Een datalek kun je voorkomen door gevoelige gegevens versleuteld op te slaan. Dat wil zeggen dat je je bestanden onleesbaar opstaat en een toegangscode nodig hebt om ze te openen.

OMGAAN MET CYBERCRIME: ZO BESCHERM JE JE ONDERNEMING

WWW.YOURVIRTUALASSISTANT.ONLINE

Heb je hier vragen over? Neem contact op via info@yourvirtualassistant.online

www.yourvirtualassistant.online | Einsteinstraat 1 | 4702 WB | Roosendaal | Nederland |
Tel: 06 55 627 847 | E-mail: info@yourvirtualassistant.online | KvK Nummer: 69069859

OMGAAN MET CYBERCRIME:
ZO BESCHERM JE JE ONDERNEMING

Zorg dat je voldoet aan de AVG

Het verwerken van persoonsgegevens wordt steeds meer geautomatiseerd en dat heeft invloed op de informatiebeveiliging. Heb je bijvoorbeeld goed gedocumenteerd hoe je gegevens beveiligd? En alle mogelijke maatregelen getroffen om kwetsbaarheden en datalekken te voorkomen? Slechte beveiliging kan namelijk leiden tot een datalek. En dat kan weer misbruik van deze gegevens tot gevolg hebben. Bijvoorbeeld voor identiteitsfraude.

Volgens de AVG moet je hier als ondernemer passende maatregelen voor nemen. Weet je niet precies hoe hier aan moet voldoen? Of waar je moet beginnen?
Schrijf je dan in voor de AVG-training van Your Virtual Assistant, waarin je leert hoe je de privacy van jouw klanten kunt beschermen én zelf niet voor verrassingen komt te staan.

Doe altijd aangifte

Ben je slachtoffer geworden van cybercrime? Uit onderzoek van I&O Research blijkt dat 60% van de slachtoffers zich hiervoor schaamt. Ze hebben vaak het gevoel dat het hun eigen schuld is dat ze gehackt zijn. Toch is het enorm belangrijk dat je aangifte doet van cybercriminaliteit. Want het niet of laat melden van een cyberincident kan leiden tot méér schade. Denk aan een hack met ransomware die zich door je computer verspreid.
Of persoonsgegevens van je klanten die op straat komen te liggen. En dat laatste ben je zelfs verplicht om binnen 72 uur te melden bij de Autoriteit Persoonsgegevens.

Daarbij heeft de politie zoveel mogelijk informatie nodig om cybercriminelen op te sporen. Hoe meer informatie zij hebben, hoe meer patronen zij kunnen ontdekken.
En hoe groter dus ook de kans wordt dat cybercriminelen worden opgepakt. Doe dus altijd aangifte.

Heb je hier vragen over? Neem contact op via info@yourvirtualassistant.online
www.yourvirtualassistant.online | Einsteinstraat 1 | 4702 WB | Roosendaal | Nederland |
Tel: 06 55 627 847 | E-mail: info@yourvirtualassistant.online | KvK Nummer: 69069859