Beerepoot Automatisering zorgt voor veiligheid

# Cybercriminaliteit is gevaarlijk voor elke onderneming

**Cybercriminaliteit vormt een reële bedreiging voor elke onderneming. Toch zijn lang niet alle ondernemers zich bewust van de vele risico's die het internet met zich meebrengt. Voor slachtoffers van cybercriminelen kunnen de financiële gevolgen dramatisch zijn. Westfriese Zaken in gesprek met Alex Middelburg van Beerepoot Automatisering over cybercriminaliteit.**





'Steeds vaker komt de term "Ransomware" naar voren in nieuwsberichten. Deze vorm van internetcriminaliteit is zowel voor ondernemers als voor particulieren een bedreiging. Ransomware betekent letterlijk: gijzelingssoftware. Criminelen blokkeren de computer van ondernemers en doen zich vaak voor als justitie of politie. De ondernemer zou zich zogenaamd schuldig hebben gemaakt aan strafbare feiten en er moet een boete betaald worden. Pas na betaling zijn de bestanden weer toegankelijk, houden de criminelen de ondernemer voor. Tot die tijd kan de ondernemer niet verder werken. Maar vaak blijft óók na betaling de computer nog geblokkeerd', vertelt Alex.

## Imagoschade

Alex gaat verder: 'De meest vervelende vorm van Ransomware is Cryptoware. Dit zorgt ervoor dat bestanden op besmette computers worden versleuteld, deze kunnen dus niet meer geopend worden. Het komt vaker voor dan men denkt; de eerste twaalf weken van dit jaar hebben al zes bedrijven een beroep gedaan op Beerepoot Automatisering omdat hun complete IT-omgeving was versleuteld door Crypto-Ransomware. Bestanden raakten ontoegankelijk. Hierdoor kwamen bedrijfsprocessen in gevaar. Voor veel organisaties heeft dit tot ernstige imagoschade en financiële schade geleid.'

## Voorkomen is beter dan genezen

De politie adviseert slachtoffers van cybercrime om niet te betalen en aangifte te doen. Het is duidelijk dat ook voor cybercriminaliteit geldt: voorkomen is beter dan genezen. Wie eenmaal slachtoffer is van cybercriminaliteit kan zijn bestanden vrijwel niet zonder enige vorm van schade terugkrijgen. 'Cybercriminelen verstoppen hun kwaadaardige programmatuur meestal op onzichtbare plekken in websites of afbeeldingen. De kans op "besmetting" kan op meerdere manieren worden verkleind. Zo is het belangrijk om het besturingssysteem en programma's up-to-date te houden. Ook is het belangrijk om niet te surfen op internet zonder een antivirusprogramma, geen onbekende bijlages in e-mails te openen, niet op links in e-mails te klikken en uiteraard alert te zijn bij het downloaden van software, muziek, films, PDF's en andere bestanden. Om de bestanden van de onderneming veilig te houden, is het belangrijk regelmatig een back-up te maken van de documenten. Deze back-up moet op een andere plek dan de computer opgeslagen worden. Het klinkt allemaal vrij logisch, maar toch zijn er regelmatig ondernemers die door de slimheid van cybercriminelen de mist ingaan.' Om de veiligheid van computersystemen veilig te stellen en te zorgen dat er voldoende back-up mogelijkheden zijn, kan een ondernemer het beste een automatiseringsbedrijf in de arm nemen.

## Virusscanners houden niet alles tegen

'Virusscanners zijn een belangrijk instrument om problemen te voorkomen, maar helaas houden deze niet alle virussen tegen. Een traditionele virusscanner haalt updates binnen. Dit zijn zogenaamde virusdefinities/signatures van bekende virussen. Op deze manier wordt ongeveer 70% van de virussen tegengehouden. Daarnaast heeft de huidige generatie virusscanners een mechanisme wat "verdacht gedrag" verifieert bij een online database. Hierdoor worden recent ontdekte virussen (29%) die nog onbekend zijn in de eerder genoemde virusdefinities tegen gehouden. 1% van de virussen wordt standaard niet ontdekt door virusscanners. Hier valt ook Crypto-Ransomware onder. En juist deze groep zorgt voor veel schade bij organisaties. Beerepoot Automatisering heeft wel oplossingen om deze aanvallen te voorkomen.'

Het onderwerp beveiliging staat al een aantal jaar hoog op de agenda van Beerepoot Automatisering. Speciaal voor ondernemers organiseert het bedrijf een gratis seminar 'Trends in cybercrime' op 9 juni. Tijdens dit seminar wordt ingegaan op hoe cybercriminelen werken en hoe ondernemers zich hier tegen kunnen wapenen. Alex: 'Ondernemers zijn doorgaans in de veronderstelling dat hun netwerk veilig is, maar vaak zijn er toch "lekken" te vinden. Wie twijfelt over de veiligheid van zijn netwerk, kan contact met ons opnemen. Onze consultants kunnen een objectieve analyse uitvoeren. Uit deze analyse volgt een rapport waarin punten ter verbetering van de veiligheid worden opgenomen.'

Wie meer wil weten over de risico's en de veiligheid van zijn digitale werkomgeving kan altijd vrijblijvend contact opnemen met Beerepoot Automatisering via 0229-76 87 68. Kijk ook eens op **www.bpaz.nl**.

*Tekst en beeld: Indrukmakers BV*