Is jouw bedrijf voorbereid op cybercriminaliteit?

Het zal niemand ontgaan zijn: afgelopen weekend werden zeker 150 landen getroffen door een cyberaanval van enorme omvang. Ook in Nederland was het raak. Vooral bedrijven kregen te maken met het computervirus en nog steeds wordt er gevreesd voor een nieuwe aanval. Is jouw bedrijf voorbereid op cybercriminaliteit? Wat kun je als bedrijf doen om te voorkomen dat je slachtoffer wordt van deze vorm van criminaliteit?

Bronnen: CBS, MKB-Nederland, Deloitte, Aon, Stopcybercrime.nu

Wereldwijd werden vele bedrijven en organisaties dit weekend geconfronteerd met de heftige gevolgen van cybercriminaleit. Wat is er precies gebeurd? Computers werden geïnfecteerd met het programma WannaCry, dat de toegang tot de computers afsluit. Daardoor heb je niet langer toegang tot je eigen bestanden. Doordat het virus bestond uit een unieke combinatie van ransomware en een wormvirus, werden vrijwel alle computers getroffen die op hetzelfde netwerk zijn aangesloten als de geïnfecteerde computer. Hierdoor was de impact immens.

Gevolgen cyberaanval

Niet alleen bedrijven werden getroffen, ook allerlei instanties en organisaties werden het slachtoffer. Diverse Britse ziekenhuizen hadden bijvoorbeeld niet langer toegang tot hun computers waardoor patiënten niet geholpen konden worden. De oplossing volgens de hackers? Losgeld betalen. Uiteraard is dat geen oplossing waar ondernemers op zitten te wachten. Dat geldt ook voor parkeerbedrijf Q-Park. Wie de auto dit weekend geparkeerd had in een van de Q-Park garages in bijvoorbeeld Gouda, Rotterdam of Ede kon vrij uitrijden en slagbomen moesten handmatig geopend worden. Een enorme chaos was het gevolg. Inmiddels is de digitale beveiliging scherp aangepast en lijkt alles weer op de rit, maar het gevaar voor een nieuwe aanval is nog niet geweken.

Cybercriminaliteit in Nederland

Gezien de grootte van de cyberaanval viel de schade in Nederland nog mee. Toch zijn er ook in ons land nog veel bedrijven niet op de hoogte van de gevaren van een cyberaanval. Volgens cijfers van het CBS vindt 83% van de Nederlandse ondernemers niet dat ze volledig voorbereid zijn op cybercrime. 55% kent zelfs de gevaren niet en 39% heeft geen digitaal beveiligingsplan. Om het hackers niet te makkelijk te maken, zijn sterke wachtwoorden noodzakelijk. 33% van de ondernemers heeft hier echter niks over afgesproken met zijn personeel. Eenzelfde percentage van de ondernemers heeft niets vaststaan over omgang met klantgegevens.

Tips om een cyberaanvallen te voorkomen

Ook in ons land kan de digitale beveiliging dus sterk verbeterd worden. Wat kun jij als ondernemer doen om de kans op deze vorm van criminaliteit te minimaliseren? We geven 10 tips:

1. Zorg voor goede antivirus software.
2. Installeer regelmatig software-updates.
3. Gebruik sterke wachtwoorden.
4. Open geen berichten en bestanden van verdachte afzenders: controleer altijd de afzender.
5. Klik niet zomaar op vreemde links.
6. Controleer altijd de URL en het certificaat: een slotje voor de URL toont aan of het een SSL beveiligde website is.
7. Bespreek de risico's met jouw personeel.
8. Maak afspraken over de omgang met klantgegevens.
9. Denk na over een mogelijke verzekeringsdekking, wij helpen je graag daarbij.
10. Evalueer regelmatig of de aanpak het gewenste resultaat heeft.

Uit de aanval van afgelopen weekend blijkt maar weer hoe belangrijk het is om de digitale beveiliging in orde te hebben. Ben jij goed voorbereid?

Neem contact op met eric@renaudwolf.nl om samen dit item te bespreken.