Cybercriminaliteit bij ondernemingen

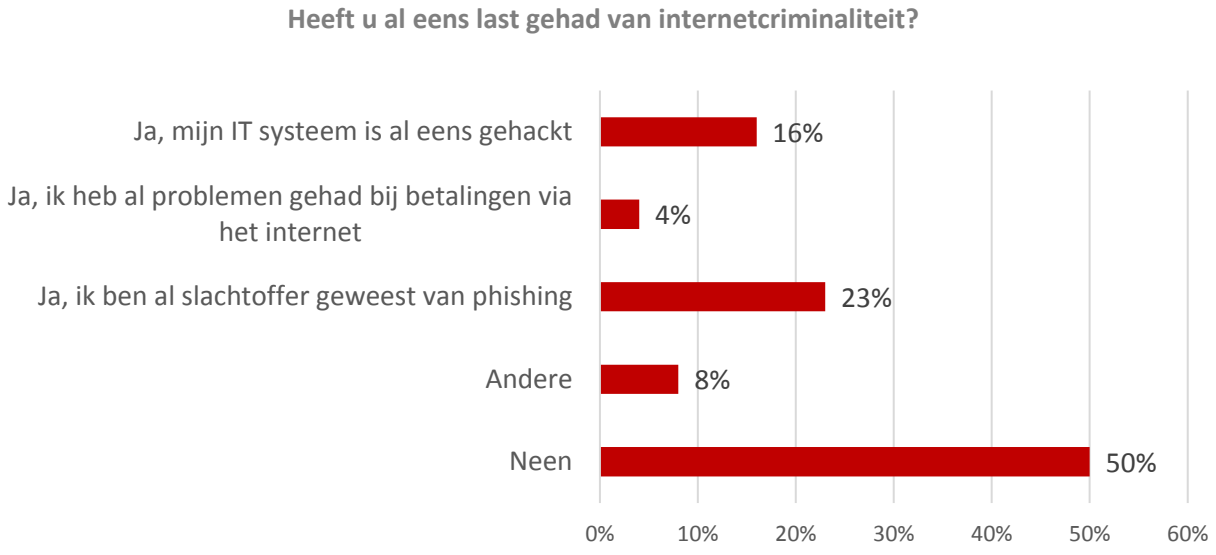
November 2016

- √ *50% van ondernemers werd reeds slachtoffer van een vorm van internetcriminaliteit*
- √ *70% neemt zelf IT-beveiligingsmaatregelingen, 30% besteedt IT-beveiliging uit aan een professioneel bedrijf.*
- √ *Als reden voor een beperkt IT-veiligheidsbeleid zegt vier op de tien ondernemingen dat het risico op een cyberaanval te klein is.*

Wekelijks krijgt de UNIZO Ondernemerslijn (meerdere) meldingen over gevallen van cybercriminaliteit. Daarom ondervroeg UNIZO 783 leden omtrent het thema cybersecurity. De bevraging werd uitgevoerd in september en sluit aan op eerdere bevragingen in 2014 en 2015.

Vandaag stellen we vast dat maar liefst de helft van onze respondenten (49.8%) te maken kreeg met een vorm van internetcriminaliteit. Een duidelijke stijging tegenover 2014 en 2015 toen respectievelijk 40% en 30% van de respondenten aangaf slachtoffer te zijn geweest van criminele feiten op het internet.

Als we polsen naar welk soort van cybercriminaliteit voorvalt blijkt dat het in 15% van de gevallen gaat om IT-systemen die worden gehackt. 4% van de ondernemers ondervond problemen bij betalingen via het internet (e-commerce, fraude bij internetbankieren), en 23% was reeds slachtoffer van phishing[1].



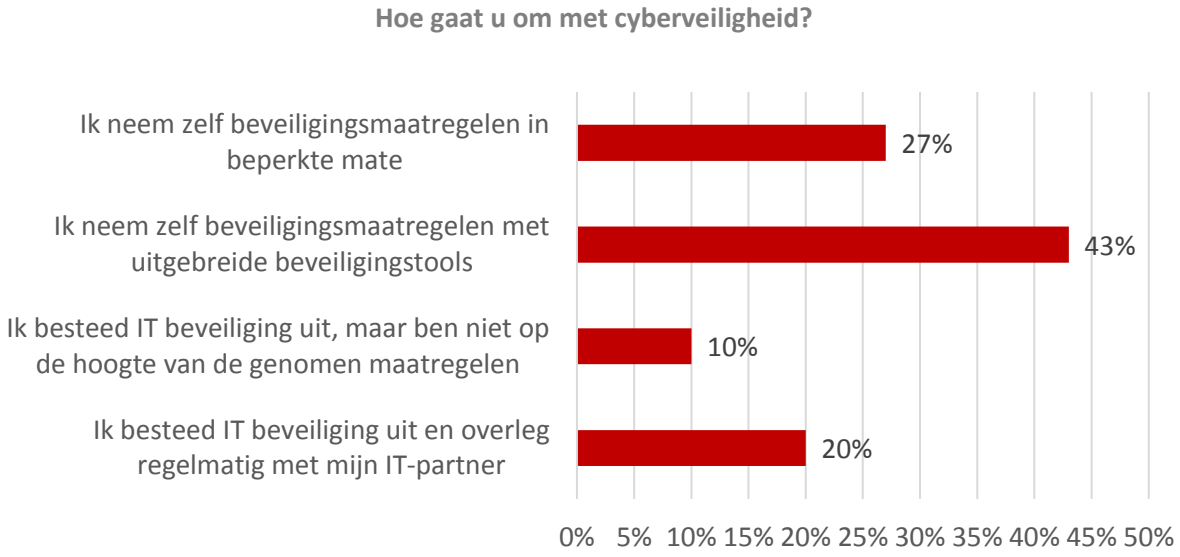
[1] Phishing is een veelvoorkomende vorm van internetfraude waarbij cybercriminelen vertrouwelijke of gevoelige informatie (zoals uw bankgegevens) proberen te ontfutselen door zich voor te doen als iemand anders (bv. uw bankdirecteur) in elektronische communicatie.

Wanneer we de cijfers vergelijken over verschillende regio's, merken we op dat cybercriminaliteit eerder een geografisch onafhankelijk fenomeen is. Ook tussen de sectoren verschillen de cijfers amper, met uitzondering van de industriesector die net iets meer (+12%) last had van internetcriminaliteit.

In de Politionele Criminaliteitsstatistieken van 2015 werd vastgesteld dat, ondanks een daling van het aantal gevallen van phishing, de schade per feit ook sterk is toegenomen. Hierbij wordt er steeds meer gebruik gemaakt van nieuwe vormen van ransomware[2] waarbij ondernemingen meer en meer het doelwit zijn geworden in plaats van particulieren.

Hoe beveiligen ondernemingen zich?

Zeven op de tien van de bevraagde ondernemers neemt zelf de beveiligingsmaatregen. Daarvan geeft 27% aan slechts hier en daar wat antivirus of antispam te hebben geïnstalleerd. Toch zegt 43% te beschikken over uitgebreide beveiligingstools, zoals een degelijk back-up systeem, een firewall, antivirus software, …. Drie op de tien van de bevraagde ondernemers besteedt haar IT-beveiliging uit aan een IT partner of een beveiligingsbedrijf. Daarvan is 10% niet op de hoogte van de genomen maatregelen door haar IT-leverancier. De overige 20% wordt wel betrokken bij de genomen maatregelen van haar IT-leverancier en overlegt op regelmatige basis.



[2] Gijzelsoftware die uw pc bestanden vergrendelt. Nadien wordt u opnieuw gecontacteerd om 'losgeld' te betalen.

Motivering voor een eerder beperkt veiligheidsbeleid

Vervolgens polsten we naar de motivatie voor een eerder beperkt veiligheidsbeleid. Daarbij gaf bijna 30% aan niet op de hoogte te zijn van de mogelijkheden om zich beter te beschermen tegen cybercriminaliteit. Ongeveer een kwart van de ondernemers vindt dat de kosten niet opwegen tegen de baten. En 40% vindt het risico dat er zich een cyber issue voordoet te beperkt.

Blijf waakzaam en bescherm u tegen cybercrime

We concluderen dat er enerzijds ondernemingen zijn die zich in beperkte mate beveiligen, en anderzijds ondernemingen die uitgebreide voorzorgen nemen. De ondernemingen met uitgebreide IT beveiligingstools en ondernemingen die nauw samenwerken met hun IT partner hebben minder last van internetcriminaliteit dan ondernemingen die dat minder doen. Hoe dan ook zien we dat fraudeurs creatief zijn en steeds op zoek blijven gaan naar de zwakste schakel in beveiligingssystemen. Daarom moet elke KMO zich vandaag de vraag stellen *wat* en *hoe* ze zich beter kunnen beschermen en hoe ze zullen communiceren als ze alsnog slachtoffer worden. De kans op een cyberaanval is immers reëel en het is cruciaal om op dat ogenblik correct te reageren naar klanten en leveranciers toe.

UNIZO roept op om waakzaam te blijven voor allerlei vormen van internetcriminaliteit. UNIZO adviseert haar leden ook om frauduleuze praktijken steeds te melden bij de FOD Economie via https://meldpunt.belgie.be/meldpunt/. Bovendien spoort UNIZO haar leden aan om steeds klacht in te dienen wanneer ze slachtoffer werden van cybercriminaliteit. Ook al bent u opgelicht voor slechts enkele euro's, veel kleine zaakjes samen kunnen grote lijnen zichtbaar maken en bijgevolg de politie helpen om fraudeurs op te pakken.

In de UNIZO advies pocket 'Veilig omgaan met ICT en het internet' vindt u meer uitgebreide informatie om uw onderneming te beschermen tegen cybercrime (www.unizo.be/publicaties/pockets-en-gidsen/veilig-omgaan-met-ict-en-het-internet-digitaal). UNIZO biedt ook professioneel advies aan via Expert@Board. U kan hierbij beroep doen op de KMO-Portefeuille (subsidies) waarbij de Vlaamse Overheid 30% tot 40% van uw factuur betaalt. Meer weten? www.unizo.be/expertatboard/.

****