Cyberaanval treft **2 op 5 bedrijven**

2 op de 5 mkb-bedrijven in Nederland is aangevallen door cybercriminelen; 1 op de 5 werd daadwerkelijk slachtoffer. Dit blijkt uit onderzoek van het Lectoraat Cybersecurity in het mkb, dat de Haagse Hogeschool in samenwerking met MKB-Nederland uitvoert in twintig branches.

De vijf meest voorkomende vormen van cybercrimes bij bedrijven:

- **30% malware**. Software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Malware kan onder andere op de computer komen door gratis software te installeren of door louche websites zoals porno sites of sites met gratis mp3-bestanden te bezoeken.
- **17% ransomware**. Criminelen blokkeren de computer en/of gegevenstoegang door middel van malware en vragen geld om deze blokkade op te heffen.
- **10% phising**. Internetfraude waarbij je naar een valse maar nét echt lijkende (bank)website worden gelokt. Zodra je inlogt, beschikt de fraudeur over jouw inloggegevens en creditcardnummer.
- **7% fraude/oplichting via internet**.
- **7% hacking**. Wanneer iemand de beveiliging heeft omzeild en binnen dringt in je computernetwerk. Voor veel hackers is dit enkel een sport; anderen willen zich illegaal informatie toe-eigenen.

Andere voorkomende vormen van cybercrime in het mkb zijn diefstal van datadragers (6%), Denial of Service (DoS-)aanval (5%), vernieling van gegevens (4%), smaad/laster (4%), identiteitsmisbruik (3%), afpersing via internet (3%), defacing (3%), chantage via internet (2%), ongeautoriseerd gebruik van het bedrijfsnetwerk (2%), skimming van pinpas- of creditcardgegevens van het bedrijf (2%), diefstal van gegevens zoals wachtwoorden (1%).
1 op de 5 voor het onderzoek ondervraagde mkb'ers was slachtoffer van één van bovengenoemde vormen van cybercrime. Daarnaast wist 21% van de mkb-bedrijven een cyberaanval succesvol af te weren.

Meer mensen = meer kans

Bedrijven met meer dan vijftig medewerkers zijn aanmerkelijk vaker slachtoffer van cybercrime dan kleinere bedrijven. 39,1% van de bedrijven met meer dan vijftig medewerkers werd slachtoffer. Bij kleinere bedrijven ligt het percentage lager: 21,8% van de bedrijven met tien tot vijftig medewerkers en slechts 1,51% van de bedrijven met minder dan tien medewerkers hebben te kampen gehad met cybercrime.

Hoe veilig is jouw netwerk?

De website veiligzakelijkinternetten.nl geeft bedrijven inzicht in de status rond cybercrime. Via een gratis scan van het bedrijfsnetwerk en de website worden de kwetsbaarheden inzichtelijk. Het project Veilig Zakelijk Internetten is een initiatief van MKB-Nederland en de Haagsche Hogeschool en wordt ondersteund door de ministeries van Justitie en Veiligheid en Economische Zaken.

Stelling: Een cyberaanval? **Dat overkomt mij niet!**

Jostein Kiezebrink
Buro26

"Elke website of webshop krijgt continue, 24 uur per dag, te maken met hackpogingen. Op het internet zijn geautomatiseerde scripts actief die proberen misbruik te maken van bekende softwarelekken. Dit zijn vaak foutjes in veelgebruikte CMS'en zoals WordPress of Joomla die benaderbaar zijn door een url aan te roepen. Veelgebruikte combinaties tussen gebruikersnaam en wachtwoord worden gebruikt om te proberen toegang te krijgen tot het beheergedeelte. Ook e-mailformulieren zijn vaak doelwit om spam mee te gaan versturen. Veel pogingen worden al tegengehouden door de hostingprovider of geïnstalleerde firewall in je website. Gebruik altijd een complex wachtwoord. Laat je website van de nieuwste updates voorzien. Daarmee kun je veel ellende voorkomen."

Marc Jongsma
ICT-manager De Groot - grootsgedrukt.nl

"Ik herinner me nog goed dat we voor het eerst een virus in ons netwerk hadden; een MS-DOS virus dat de gebruiker eerst een simpel rekensommetje liet oplossen voordat zijn commando werd uitgevoerd. Tamelijk onschuldig en daarmee dus ook wel grappig. Latere virussen werden steeds kwaadaardiger en formatteerden je harde schijf of overschreven de BIOS van je PC. Anno 2018 moeten we constateren dat cybercriminaliteit in een alarmerend tempo groeit en dat cyberaanvallen vaak geen eenvoudige verstoringen zijn, maar gecoördineerde aanvallen die op specifieke doelen gericht zijn. We zitten in een tijd waarin cyberaanvallen geen risico of mogelijkheid meer zijn, maar een onvermijdelijk gegeven. Daarnaast is er een enorme groei van digitale technologieën waardoor maatregelen die in 2018 nog effectief zijn, in 2019 al achterhaald zijn.
Moeten we dan stellen dat het dan een hopeloos gevecht is? Nee, zeker niet! Er zijn genoeg middelen om digitaal verkeer, netwerken en computers te beveiligen en daarmee de kans op infectie of het platleggen van systemen te beteugelen of te voorkomen. Een basishouding die ik graag hanteer; wees nooit te zeker van je zaak, zekerheid is de vijand van verandering.
Iemand heeft eens gezegd; je kunt niet voorkomen dat er vogels boven je hoofd vliegen, maar wel dat ze een nest op je hoofd bouwen. Geweldige uitspraak en direct toe te passen op cyberaanvallen!"

Machiel van der Schoot
De Angelot Office (Angelot.nl)

"Als je denkt dat jouw bedrijf dat niet overkomt, ben je per definitie een slachtoffer.Het aantal cyberaanvallen per bedrijf is het eerste kwartaal van 2018 weer met 82 procent toegenomen. Per gemonitord bedrijf worden er gemiddeld 256 exploits per dag gedetecteerd. Inmiddels verkopen wij onze kantoorartikelen in heel de Benelux. Onze klanten zijn ons grootste kapitaal. Voor de vaak privacy gevoelige informatie van onze klanten zijn en voelen we ons extreem verantwoordelijk. Daarbij wil je beslist niet dat je webshop plat komt te liggen. Dat kost simpelweg te veel. Daarom reserveren wij jaarlijks een flink bedrag voor nieuwe investeringen in online-veiligheid."

Dennis Baaten
Baaten ICT Security

"Iedere organisatie valt vroeg of laat ten prooi aan cybercriminelen. Het is niet zozeer de vraag "of" dit gebeurt, maar eerder "wanneer" dit gebeurt. Dreigingen zijn continu en in vele vormen aanwezig; er is altijd wel iemand die baat heeft bij het hacken van een computersysteem. Bij ransomware bijvoorbeeld, worden bestanden van willekeurige slachtoffers ontoegankelijk gemaakt en vragen de cybercriminelen losgeld in ruil voor het herstellen van de toegang.
De meeste organisaties zijn in sterke mate afhankelijk van ICT en geraken al snel in de problemen op het moment dat de ICT-voorzieningen niet functioneren. Organisaties dienen zich in voldoende mate beschermen tegen cybercriminelen door het nemen van technische en organisatorische maatregelen. Deze maatregelen verkleinen de kans en/of impact van informatiebeveiligingsrisico's door het minimaliseren van kwetsbaarheden. Belangrijke maatregelen zijn in ieder geval: tijdig installeren van beschikbare updates, gebruik van sterke wachtwoorden, maken van offline back-ups, trainen van medewerkers, en het gebruiken van antivirussoftware.
De grote uitdaging hierbij is om dicht op de bal te blijven spelen. Informatiebeveiliging is geen eenmalige actie zoals het plaatsen van een slot op de deur. Het vereist voortdurend aandacht om te zorgen dat een organisatie opgewassen blijft tegen de continu veranderende dreigingen."