Cyberkidnappers kosten Belgische bedrijven almaar meer

Cybercriminaliteit kost Belgische bedrijven al drie keer meer dan drie jaar terug. Vooral cryptolockers, die IT-systemen platleggen om losgeld te krijgen, zijn aan een opmars bezig.

PIETER SUY

Hoe groot de impact van een cybergijzeling kan zijn, ondervond recent nog Nyrstar. De zwalpende Belgische zinkverwerker werd ruim een week geleden het slachtoffer van een cyberaanval. Daardoor konden medewerkers niet langer mailen en waren een aantal servers bedoeld voor administratief werk een tijdlang niet bereikbaar.

De IT-gijzeling bij Nyrstar is allesbehalve uitzonderlijk, leren cijfers van de Belgische verzekeringsmakelaar Vanbreda Risk & Benefits. Sinds 2016 zag de makelaar het aantal schadegevallen bij ondernemingen door cybercriminaliteit met 194 procent exploderen. Een verdrievoudiging in drie jaar.

20.000

Bij het merendeel van de door ransomware getroffen bedrijven is de schade niet hoger dan 20.000 euro.

Die stijging blijkt vooral op naam te schrijven van 'cryptolockers' of 'ransomware'. Dat is software waarmee criminelen pc's en hele IT-systemen kunnen lamleggen. Pas als het bedrijf losgeld heeft betaald, liefst in bitcoin, geven de cyberkidnappers de computersystemen vrij.

De voorbije maanden steeg het aantal gevallen van cryptolocking explosief, meldt Vanbreda. In 2017 dienden nog maar een achttal bedrijven een claim in bij hun verzekeraar nadat ze het slachtoffer waren van ransomware. Eind 2018 is het aantal slachtoffers opgelopen tot bijna 35.

Het werkelijke cijfer ligt allicht een pak hoger. Nog steeds hebben heel wat ondernemingen geen verzekering afgesloten om zich in te dekken tegen cybercriminaliteit. Andere bedrijven verkiezen dan weer het gevraagde bedrag op tafel te leggen. Zo vermijden ze dat hun reputatie wordt besmeurd.

'In het merendeel van de gevallen loopt de schade zelden hoger op dan 20.000 euro,' geeft Vanbreda-cybersecurity-expert Tom Van Britsom mee. 'Maar we hebben ook een melding gekregen van een onderneming die meer dan 1 miljoen euro heeft betaald om zich vrij te kopen.'

'Ransomware is al jaren aan een opmars bezig,' beaamt Stéphan Goddé, veiligheidsexpert van de consultant BDO. 'En daar komt niet meteen verandering in.' Dit soort software geeft criminelen helaas behoorlijk wat zekerheid dat slachtoffers gaan betalen, weet Goddé. 'Ook al stapt het slachtoffer naar de politie, als misdadiger heb je nog altijd de sleutel in handen om de IT-systemen vrij te geven.'

Om dat aan te pakken schoot ook de overheid in actie. Het Centrum voor Cybersecurity België sloot zich samen met de Federal Computer Crime Unit van de federale politie aan bij een internationaal project tegen ransomware. Via een website - nomoreransom.org - worden softwaresleutels aangeboden waarmee slachtoffers hun bestanden kunnen vrijmaken zonder daar losgeld voor te moeten betalen. Al is dat volgens Goddé maar een deel van de oplossing. 'Voor criminelen is het geen grote opgave om hun schadelijke software te updaten. Dan helpen de sleutels van de overheid niet meer.'

Goddé wijst erop dat bedrijven nog veel meer werk moeten maken van hoe hun personeel omspringt met IT. 'Ransomware sluipt bedrijfssystemen binnen via de zwakste schakel. Zoals iemand die de pc of de tablet van het werk niet alleen op kantoor gebruikt, maar ook voor persoonlijke doeleinden. Werknemers daar bewust mee leren omspringen, kan een deel van de oplossing zijn.'

De Tijd 01/02/2019, bladzijden 4 & 5