Je hebt het waarschijnlijk zelf gemerkt. We hebben de afgelopen maanden heel wat phishingmails - berichten en sms'en van cybercriminelen die ons geld proberen te stelen - over ons heen gekregen. Die viseren vaak particulieren, maar specialisten vrezen dat volgend jaar vooral bedrijven een potentieel doelwit zullen zijn van cybercriminelen.

2020 was een bewogen jaar

2020 was niet alleen het jaar van het coronavirus, we zijn ook allemaal van thuis beginnen werken. "Op vlak van cybersecurity was 2020 een heel bewogen jaar", zegt expert internetveiligheid Stijn Rommens. Rommens heeft doorheen de jaren veel ervaring opgedaan op het vlak van ransomeware-aanvallen (dat zijn aanvallen waarbij cybercriminelen computersystemen platleggen in ruil voor geld, red.). Hij werkt voor een bedrijf dat technologieën ontwikkelt om verborgen computervirussen te detecteren. "Computers en het internet hebben ons de mogelijkheid gegeven om te communiceren met collega's en families, en dat zorgde ook voor een sterke toename van het aantal cyberaanvallen."
Volgens Rommens moet je begrijpen hoe hackers werken. "Cybercriminelen zijn op zoek naar gegevens om daarmee geld te verdienen. En omdat we nu massaal van thuis werken, circuleren heel veel gegevens van ons online, daarom richten ze hun pijlen op thuiswerkers."
Thuiswerkers zijn dus een gegeerd doelwit voor hackers, ook omdat ze via de computer thuis in het netwerk van het bedrijf kunnen infiltreren. Zo komen ze terecht in de databank van de onderneming.

Office 365 wordt nagemaakt

Nico Sienaert ziet ook dat thuiswerkers een gegeerd doelwit zijn. Sienaert is cybersecurity expert bij Microsoft. Zijn bedrijf brengt elk jaar een lijvig rapport uit over de belangrijkste cyberdreigingen van het moment. "Tijdens de eerste lockdown moesten veel mensen plots van thuis werken. Wat gebeurde er? Er werden laptops vanonder het stof gehaald en aan de mensen gegeven om van thuis te werken. Hackers kunnen e-mails sturen onder jouw naam en kunnen zo collega's misleiden. Soms zijn dat toestellen die niet goed beveiligd zijn. Daarnaast hebben thuiswerkers niet dezelfde 'firewalls' (systemen om virussen buiten te houden) als op kantoor." Sienaert raadt de IT-diensten van de bedrijven aan om de veiligheid van de laptops van thuiswerkers regelmatig te testen op hun veiligheid.
"Cloud-oplossingen (systemen die via het internet draaien) kunnen snel een oplossing bieden om gebruikers veilig van thuis te laten werken, ook op pc's die vanonder het stof werden gehaald. We hebben wel gezien dat veel klanten nog niet klaar waren om mensen op grote schaal te laten thuiswerken. Hierdoor zijn er wat zaken 'quick & dirty' gebeurd. We raden dan ook klanten aan een stap terug te zetten en eens te kijken of ze de voorgeschreven 'security best practices' wel correct hebben toegepast", legt Sienaert uit.
"Maar hackers zijn heel slim", zegt Sienaert. "Omdat veel bedrijven met Office 365 (het softwarepakket van Microsoft met Word, Excel en PowerPoint) werken, kopiëren hackers een inlogpagina ervan. Zo proberen ze de login en wachtwoord te ontfutselen, en kunnen ze

onder jouw naam e-mails beginnen sturen naar collega's. Die gaan niet weten dat hier een hacker achter zit. Maar hackers gaan een stapje verder." Sienaert: "Wat ze vaak doen is o.a. 'domain spoofing', om zo gebruikers te misleiden via een fout e-mailadres (die sterk lijkt op een echte)." Maar volgens Sienaert zijn er binnen Office 365 mechanismen om dit tegen te gaan.

Ransomware 2.0

In 2020 hebben we ook een heel sterke toename gezien van cyberaanvallen die gerelateerd zijn aan de pandemie. Cybercriminelen sturen veel valse e-mails en berichten rond met "covid-19" of "corona" in de titel om de mensen te misleiden. Ook websites van pakjesbedrijven werden nagemaakt.

Eddy Willems, cybersecurity specialist bij G Data, voorspelt dat we de komende jaren nieuwe vormen van ransomware, waarbij cybercriminelen systemen lamleggen in ruil voor geld, zullen zien. "Ik noem dat ransomware 2.0. Nu versleutelen cybercriminelen systemen en vragen ze losgeld om die vrij te geven. In de toekomst zullen ze de gegevens die ze versleutelen ook gebruiken om de slachtoffers te viseren. Stel dat een ziekenhuis slachtoffer is, dan gaan de cybercriminelen de gegevens van de patiënten ook stelen en viseren."

Niet alleen particulieren worden geviseerd. Een aantal weken geleden probeerden hackers in te breken in het computernetwerk van het Europees geneesmiddelen-agentschap (EMA). Zij slaagden erin om gegevens van vaccinproducent Pfizer/BioNTech te bekijken. Volgens Sienaert gaan we in de toekomst meer en meer van dit soort aanvallen zien. "Bedrijven en organisaties die nu bezig zijn met de ontwikkeling van het vaccin zijn een gegeerd doelwit. Criminelen gaan dus alle moeite doen om aan recepten van de vaccins te geraken", zegt Sienaert.

Maar daar blijft het niet bij. Hackers gaan op een heel vernuftige manier te werk om in computernetwerken in te breken. Dat hebben we gezien bij de recente cyberaanval op SolarWinds, een bedrijf dat software ontwikkelt voor andere bedrijven. "Dit is zowat de grootste cyberaanval van het jaar", zegt Willems. "De manier waarop ze zijn binnen geraakt, noemen we een supply chain aanval. Hackers breken in een softwarepakket dat door duizenden bedrijven worden gebruikt, en geraken zo ongemerkt binnen." En dat maakt het volgens Rommens extra moeilijk om het virus te detecteren. "Allicht waren de hackers sinds maart actief, maar niemand heeft dat gemerkt." Via SolarWinds geraakten de hackers in het computernetwerk van duizenden bedrijven binnen, waaronder technologiereuzen VMware, Cisco, Nvidia en Belkin. Ook Microsoft, het Amerikaanse leger en het Amerikaanse ministerie van financiën zijn geviseerd.

Meer 'state sponsored' aanvallen

Over één ding zijn alle specialisten het eens. We gaan in de toekomst ook meer 'state sponsored' cyberaanvallen krijgen. Dat zijn cyberaanvallen die georganiseerd worden door groeperingen die door een bepaald land betaald of ondersteund worden. "Daar is SolarWinds

een mooi voorbeeld van. De hackersgroepering Cozy Bear zou hierachter zitten. Die zou gelinkt zijn aan de Russische geheime dienst", zegt Rommens.
Volgens Rommens is de dreiging van zulke groeperingen niet te onderschatten. Zij hebben verschillende doeleinden. Niet alleen doen ze aan spionage en willen ze zoveel mogelijk gegevens ontfutselen, zij gaan bevoordeeld – en dat hebben we gezien bij groeperingen uit Noord-Korea – bewust computernetwerken lamleggen en eisen dan losgeld (ransomware). Volgens het rapport van Microsoft zijn vier landen heel actief met het financieren en ondersteunen van hackersgroeperingen: Rusland, China, Iran en Noord-Korea. “Maar zolang een land een cyberaanval niet opeist, ga je nooit weten wie erachter zit”, benadrukt Willems. En dat maakt het moeilijk om bij een grote cyberaanval de daders te traceren en te berechten. Dan eindig je in een welles-nietes-spelletje tussen grootmachten die elkaar viseren. Volgens Microsoft viseren de hackers vooral NGO's en bedrijven die opdrachten uitvoeren voor de overheid. Daarnaast worden ook gezondheidsorganisaties, zoals het WHO en onderwijsinstellingen aangevallen. Volgens Willems heeft dit te maken met het feit dat die instellingen over het algemeen minder budgetten hebben om hun computernetwerken voldoende te beveiligen.

Tweestapsverificatie is een must

Maar hoe maak je je systemen veiliger? Dat doe je het best met tweestapsverificatie (MFA). Dan log je in met een wachtwoord en een sms die je krijgt op je smartphone. "Uit onze analyse blijkt dat 99 procent van de cyberaanvallen op identiteit kan opgevangen worden door MFA", zegt Nico Sienaert van Microsoft. "Kunstmatige intelligentie, 'machine learning' en 'big data' zullen in de toekomst een belangrijke rol spelen om mogelijke cyberaanvallen te voorspellen en tegen te houden." Rommens treedt hem bij, maar hij vindt ook dat bedrijven de gevaren van cyberaanvallen beter onder de aandacht moeten brengen. "Eén van de problemen bij cyberaanvallen is dat bedrijven daar niet graag over communiceren. Dit is ook met SolarWinds gebeurd. De aanval dateert van maart dit jaar, maar men wilde daar niet over communiceren. Bedrijven zijn terughoudend omdat men schrik heeft voor slechte publiciteit. En aandeelhouders horen dat niet graag." Wat kunnen de bedrijven zelf doen? Rommens is duidelijk: "Bedrijven moeten blijven investeren in goede veiligheidssystemen en moeten hun medewerkers continu waarschuwen voor de gevaren van mogelijke cyberaanvalen."