Wesley Hof, Combell

Wij willen al onze klanten steeds online houden

Cyberaanvallen zitten jaar na jaar in de lift en blijven onophoudelijk slachtoffers maken. Ransomware en DDoS-aanvallen tieren welig, en de bescherming is niet eenvoudig. Wij spraken met Wesley Hof, CTO bij Combell, om na te gaan hoe deze aanvallen werken en hoe we ons kunnen beschermen.

Met de stijging van het aantal ransomware-aanvallen en hun vernietigende impact vergeten we soms wel dat er nog andere manieren zijn om te hacken, en dat ook DDoS-aanvallen nog steeds bedrijven op de knieën krijgen. Volgens Hof moeten we wat meer oppassen, maar gaat het wel de goede richting uit. “Wat er vooral veranderd is, is de hoeveelheid DDoS- en ransomware-aanvallen. Daar zien we een felle stijging de laatste jaren. Bovendien was de awareness van ICT-security in België heel slecht. Heel veel bedrijven kijken er pas naar vanaf het moment dat ze een incident meemaken. Nu zien we de laatste twee jaren een verschuiving naar klanten die er iets proactiever mee bezig zijn dan normaal. Vroeger waren enkel IT-bedrijven met dit soort security bezig, en nu merk je dat ook bedrijven uit andere sectoren die IT gebruiken als ondersteunende diensten ermee bezig zijn. Dat is een stap in de goede richting.”

“Het is een internationaal probleem, en ook bij Belgische bedrijven moet de nodige voorzichtigheid aan de dag gelegd worden. Belgische bedrijven moeten er zeker voor zorgen dat ze met hun IT bij een partij zitten die klaar is voor dat soort aanvallen. Als bedrijf moet je bezig zijn met het kiezen van een hostingpartij die een goede strategie heeft om DDoS-aanvallen te blokkeren, en die er mee bezig is om klanten te ontzorgen. Je moet je zeker afvragen welke maatregelen er genomen worden tegen dit soort aanvallen.”

DDoS vs. ransomware

Naast de blijvende dreiging van DDoS-aanvallen wint ook ransomware aan terrein, en dat voornamelijk uit financiële overwegingen, zo meldt Hof. “Er is een fundamenteel verschil tussen een DDoS- en ransomware-aanval. Het doel van een DDoS-aanval is om tijdelijk een onderbreking te veroorzaken bij een bepaald bedrijf, zodat het even minder performant draait. Een ransomware-aanval wordt voornamelijk gebruikt om data van een bedrijf te versleutelen om losgeld te vragen. Data brengt geld op en is het meest waardevolle bezit van een bedrijf, en ze zijn dan ook iets flexibeler in het uitbetalen van het losgeld om hun data terug te krijgen. De aanvaller gaat er veel sneller iets mee verdienen. En ten tweede heb je als aanvaller veel minder capaciteit nodig om ransomware-aanvallen uit te voeren dan een DDoS-aanval. Een DDoS-aanval zelf uitvoeren is niet zo complex. Je moet wel een relatief groot botnet ter beschikking hebben en connecties hebben in dat wereldje om zo’n aanval te kunnen opstarten naar een bepaald doelwit. Bij een ransomware-aanval is het vaak een klein beveiligingsincident dat voldoende blijkt om binnen te kunnen. Je hebt slechts één klein foutje nodig om er misbruik van te kunnen maken en data te versleutelen.”

Wesley Hof, CTO bij Combell

Voorzorgsmaatregelen

In de strijd tegen cybercriminaliteit en DDoS-aanvallen ben je voor een deel afhankelijk van de security die jouw partners bieden. Volgens Hof is het daarom belangrijk om de juiste hosting-partner te kiezen die je kan helpen bij jouw online veiligheid. “Een van de belangrijkste stappen is ervoor zorgen dat alles dat op ons netwerk wordt gehost op orde is. Als je er in jouw eigen netwerk niet voor zorgt dat alles qua security op orde is met bijvoorbeeld reguliere security updates, dan zie je dat je zelf sneller het doelwit wordt van een DDoS-aanval. De tweede stap is dat wij ons eigen netwerk beheren. Daarin hebben wij op strategische plaatsen sensoren staan waarmee we constant al het verkeer dat op ons netwerk binnenkomt monitoren. Als we zien dat het afwijkt van een bepaald stramien, dan blokkeren we dat automatisch. Je moet ook voldoende capaciteit voorzien. Ze proberen jouw uplink naar het internet te verzadigen. Het is onze verantwoordelijkheid om voldoende capaciteit te hebben en voldoende buffers te voorzien tussen wat we gebruiken en naar waar we kunnen pieken bij een DDoS-aanval. Bij een DDoS-aanval hebben we ook een ‘scrubbing-service’ waar alle ‘vuile’ pakketjes eruit worden gefilterd. De rest loopt door waardoor onze klanten online blijven terwijl ze worden aangevallen. We zien dat andere hostingpartijen ervoor kiezen om klanten die aangevallen worden offline te halen om andere klanten te beschermen. Wij hebben een andere filosofie en proberen alle klanten steeds online te houden.”

Eigen inspanningen

Ook al lijkt het wat vechten tegen de bierkaai, toch is Hof van mening dat je als bedrijf voldoende zelf kan doen om jouw eigen bescherming te optimaliseren. “Zo heb je bijvoorbeeld reguliere ‘pentesting’. Ook bedrijven die iets van diensten doorsturen naar het internet kan ik ook adviseren om een ‘bug bounty’-programma te lanceren. Het is belangrijk omdat ze bij een ransomware-aanval eerst moeten binnen kunnen op jouw netwerk. Er is ook een inzicht of monitoring nodig om te zien wanneer iemand iets op jouw netwerk probeert uit te spoken. Als je ziet dat men bijvoorbeeld elke ochtend vanuit buitenlandse IP-adressen toegang probeert te krijgen, dan weet je dat er iets aan de hand is. De reactiesnelheid op zo’n incident bepaalt hoe hard je in de problemen komt. Als je ziet dat ze op jouw netwerk zitten, dan is het al te laat en heb je geen controle meer. Dat is dan ook het belangrijkste advies. Ook regelmatige updates rond phishing binnen het bedrijf kunnen het verschil maken.”

“Wat er vooral veranderd is, is de hoeveelheid DDoS- en ransomware-aanvallen. Daar zien we een felle stijging de laatste jaren. Bovendien was de awareness van ICT-security in België heel slecht. Heel veel bedrijven kijken er pas naar vanaf het moment dat ze een incident meemaken"