**OPINIESTUK N.A.V. CYBERAANVAL VTM GISTERENAVOND**

10 juni 2016

*Organisaties vrijwel weerloos tegen ddos-aanvallen*****

**‘Een bulldozer door uw veranda is lastig te stoppen’**

**Om maar gelijk met de deur in huis te vallen: Er is vrij weinig dat organisaties kunnen uitrichten tegen ddos-aanvallen. “Maar dat wil niet zeggen dat er lijdzaam moet worden toegekeken hoe de servers van je website worden platgegooid, zegt Peter Magez, country manager Belux bij beveiligingsbedrijf Sophos.**

Een ‘distributed denial of service’-aanval, zoals een ddos-aanval voluit heet, is een aanval die wordt uitgevoerd door zogenaamde botnets. “Een botnet is eigenlijk een groot netwerk van geïnfecteerde computers die door kwaadwillenden op afstand kunnen worden bestuurd. Zo kan de computer thuis ook zonder jouw medeweten onderdeel zijn van een botnet”, legt Magez uit. “De mensen die een ddos-aanval willen uitvoeren op de servers van een bepaald bedrijf, sturen alle pc’s in zo’n botnet. Dat kan bestaan uit miljoenen computers wereldwijd, naar de website van dat bedrijf. De servers waarop die website draait, kunnen die enorme vraag niet aan en gaat plat. Dat is in het kort een ddos-aanval.”

**Risicoanalyse**

“Eigenlijk kun je je als organisatie nauwelijks wapenen tegen zulke aanvallen”, stelt Magez. “Natuurlijk zijn er technologische maatregelen zoals intrusion prevention, web application firewalls en intrusion protection anti flooding, maar net als met gewone inbrekers geldt: als ze naar binnen willen, komen ze er echt wel in. De technologische maatregelen zijn solide sloten, maar daar heb je bar weinig aan als er iemand met een bulldozer door je veranda rijdt.”

Magez adviseert bedrijven om een goede risicoanalyse te maken en aan de hand daarvan te bepalen welke investeringen in solide sloten noodzakelijk zijn. “Als een website slechts een digitale folder van het bedrijf is, kun je je afvragen hoe ernstig het is als die even onbereikbaar is. Maar is de site bedrijfskritisch, omdat je er bijvoorbeeld via een webshop je omzet mee haalt, dan zijn investeringen in maatregelen al meer gerechtvaardigd. Voor echt grote bedrijven met dito budgetten, die miljoenen omzet maken via hun website, is het logisch dat zij alles uit de kast halen om de uptime van de website te garanderen.”

**Imagoschade**

Als de website bedrijfskritisch is, dan is de meest eenvoudige manier om te zorgen voor uptime, het outsourcen naar een hosting partij. Daarbij kan er ook gekozen worden om de site over meerdere datacenters te verspreiden, zodat er in geval van een aanval uitgeweken kan worden. “Maar dat zijn vooral maatregelen om ervoor te zorgen dat je zo weinig mogelijk schade ondervindt van een aanval. Het zijn geen oplossingen om een aanval tegen te gaan, omdat die er feitelijk niet echt zijn.” Zorg ervoor dat je een duidelijk stappenplan hebt, zodat je weet wat er moet gebeuren op het moment dat de bedrijfswebsite ten prooi valt aan een ddos-aanval,” adviseert Magez.

VTM was gisteren nog het slachtoffer van een ddos-aanval. “Eigenlijk zijn zij het klassieke voorbeeld van onmacht”, zegt Magez. “Je mag er vanuit gaan dat de grootste commerciele omroep van ons land wel op orde is op het vlak van IT security en zo niet kunnen ze altijd eens bellen. Wellicht valt er hier en daar nog wel wat aan te passen, maar ik vind het al knap dat ze niet hebben geroepen ‘We doen er alles aan om het te voorkomen en zorgen dat het niet meer gebeurt’. Want bij een ddos-aanval kun je die garantie gewoon niet geven. En als je vervolgens nogmaals plat gaat, is de imagoschade alleen maar groter. Je moet als bedrijf geen beloftes doen die je niet kunt houden.”

**Modern protest**

Het aantal ddos-aanvallen stijgt gestaag. Dat is te wijten aan het stijgende belang van internet. “Pas de afgelopen jaren is internet voor veel bedrijven bedrijfskritisch geworden. De risico’s zijn groter, maar het gewin dus ook.” Magez ziet dat ddos-aanvallen niet alleen uit financiëel gewin worden uitgevoerd, maar dat er ook steeds meer sociaal-maatschappelijke aanvallen zijn. “Dat vind ik een interessante ontwikkeling. Een groep als Anonymous laat op zo’n manier heel duidelijk merken aan organisaties wat zij vinden dat correct is en wat niet. Het is een moderne manier van actievoeren maar met het grote verschil dat niet het ganse land er last van heeft.”

In principe hoeft een organisatie een ddos-aanval niet te melden onder de komende EU wetgeving op gebied van databeveiliging. Feitelijk zijn het twee zaken die los staan van elkaar. Toch sluimert daar een gevaar volgens Magez. “Hoe weet een organisatie nu zeker dat het alleen een ddos-aanval was en dat er niet ook iemand binnen is geweest? Bij een ddos-aanval gaat alle aandacht daar naar uit. Als hackers kwaad willen, zouden ze dat met zo’n aanval kunnen verbergen. Het is een theoretische mogelijkheid, maar dat betekent dat in de toekomst ook ddos-aanvallen gemeld moeten worden.”