SLIMME REGELGEVING

Wat eeuwen van spam ons leren over cybersecurity

Axel Arnbak

Meer dan 90% van alle wereldwijd verstuurde e-mail bestaat uit spam. Al jaren. Achter de welbekende Nigeriaanse prinsen en viagra-pillen die onze communicatienetwerken overspoelen, schuilt een van de vroegste vormen van cybercrime en een intrigerend businessmodel. Bovendien leert de vrij succesvolle bestrijding van spam ons slimme en geestige lessen over zinvol cybersecuritybeleid in 2015.

In zijn geniale boek *Spam: A Shadow History of the Internet* serveert onderzoeker Finn Brunton ons het complete spamverhaal. 'Spam' ontstond medio jaren zeventig, toen het Amerikaanse studenten lukte om Arpanet, de voorloper van het internet, te hacken om te laten zien hoe onveilig het communicatiesysteem was. Computergebruikers werden via berichten op 'bulletin boards' verleid om hun programmaatje te openen, waarop het scherm alleen nog maar 'Spam! Spam! Spam!' liet zien. Opnieuw opstarten was de enige optie.

De term is geleend van een mateloos populaire sketch van de legendarische Britse comedygroep Monty Python, waarin niet veel anders gebeurt dan het voorlezen van een menu in een Brits straatcafé door een gillende keukenmeid. Spam, een soort derderangs spek, komt steeds vaker in de gerechten voor totdat het menu alleen maar bestaat uit 'spam, spam, spam, spam'. De studentengrap legde de vinger op de zere plek: als studenten het internet kunnen misbruiken voor irritante geintjes, dan kunnen cybercriminelen en overheden dat ook.

Eigenlijk bestaat spam al sinds de 16e eeuw. Toen al draaide het meestal om geld en exploiteerden spammers avant la lettre de naïviteit en geldzucht van rijkelui in heel Europa. Zo smeekte de 'Spaanse Gevangene', zogenaamd onterecht gevangen in een Frans cachot, per brief om financiële steun voor zijn losgeld. Uiteraard beloofde de 16e-eeuwse spammer bij vrijlating gouden bergen, die nooit kwamen. Die $15.000.000 'investment opportunity' van de Nigeriaanse prins in uw mailbox is dus al 500 jaar oud. Volgens Brunton is de aard van de spammer en van de opportune sufferd die erin tuint nooit veranderd.

Zijn we na al die jaren nog steeds zo stom? In het briljante artikel *Why do Nigerian Scammers say they are from Nigeria?* ontrafelt speltheoreticus Cormac Herley het businessmodel van spam. Miljoenen spamberichten versturen kost niks. Pas als iemand zo stom is om te reageren, moet de spammer tijd en moeite investeren om diegene met vervolgmails, telefoontjes en nepcontracten te verleiden harde poen over te maken. Als cybercrimineel wil je dus zeker weten dat je meteen een enorme kneus te pakken hebt. Door altijd maar weer met die Nigeriaanse prins en geslachtsvergroting aan te komen zetten, minimaliseren spammers vals-positieven.

Zoals altijd in cybersecurity bestond de eerste spamregelgeving uit het verhogen van strafmaten en meer cyberpolitie. Zo werden in 2010 miljarden euro's verkwanseld aan belastinggeld,

'Investment opportunity' van $ 15.000.000 van Nigeriaanse prins in uw mailbox is al 500 jaar oud

terwijl de grootste spamgang van 2010, verantwoordelijk voor 33% van alle spam wereldwijd, slechts $ 2,7 mln opleverde. Onsuccesvol, peperduur. Effectieve spambestrijding bestaat uit een geavanceerde technische strijd, waarin internetaanbieders spam filteren op basis van veel voorkomende woordcombinaties. In plaats van meer politie, blijkt regelgeving die eist dat 'ongevraagde communicatie' — zoals e-mailmarketing door bedrijven — vergezeld gaat van naam, adres en telefoonnummer een schot in de roos. Dit helpt de filters het kaf van het koren te scheiden, en maakt spammers of identificeerbaar, of gefilterd.

Om die algoritmische, zelflerende filters van internetaanbieders te omzeilen, wordt spam steeds onbegrijpelijker. Mocht een spambericht dan toch in onze mailbox belanden, zien we vooral onsamenhangende nonsens. En inderdaad, door een combinatie van slimme techniek en pientere regelgeving zien we de Nigeriaanse en Russische spamboegbeelden steeds minder vandaag de dag.

Spambestrijding leert ons algemenere lessen over cybersecuritybeleid. Altijd zien we hetzelfde patroon: strafmaten verhogen, meer cyberpolitie en stoere woorden van ministers. Jaren en miljarden euro's verder, blijken echte oplossingen te liggen in het verantwoordelijk houden van internetbedrijven en maatwerk in beleid. Laat het waanzinnige motto van Monty Python het cybersecuritybeleid van 2015 inspireren: 'and now for something completely different'.

Axel Arnbak is onderzoeker cybersecurity en informatierecht aan het IViR (UvA) en het Berkman Center (Harvard). Reacties @axelarnbak