Cybercriminelen spelen handig in op corona-uitbraak

Stijn van Gils
Amsterdam

Cybercriminelen storten zich massaal op de paniek rondom het coronavirus. 'De afgelopen dagen zagen we het aantal valse mailtjes over het zich snel verspreidende virus vervijfvoudigen', vertelt Bertil Holthuis, ceo van cyberbeveiliger Tesorion.

Het mailbericht oogt nog als een logische mededeling van het management. Nadat iedereen in Noord-Brabant waar mogelijk thuiswerkt en de Verenigde Staten geen Europeanen meer binnenhaalt, sluit ook bedrijf X tijdelijk een aantal van zijn kantoren. Medewerkers op deze locaties wordt gevraagd om vanaf nu vanuit huis te werken. De rest krijgt de bekende adviezen: vaker de handen wassen, voldoende afstand van collega's bewaren, in de elleboog niezen, dat soort dingen.

Zou kantoor Haarlem ook dichtgaan? Het staat op intranet, vertelt de e-mail. Even klikken op het linkje. De bekende inlogpagina van Office 365 verschijnt, keurig met een slotje. Alleen nog even het wachtwoord intikken dat je dagelijks invult.

Bovenstaand bericht is vals en werd opgespoord door het Amerikaanse securitybedrijf KnowBe4. De mail was bedoeld om inloggegevens van medewerkers te ontfutselen. 'En we hebben veel meer coronascam gekregen', mailt de Nederlandse oprichter en ceo Stu (in Nederland heette hij Sjoerd) Sjouwerman.

KnowBe4 is lang niet het enige bedrijf dat een toename ziet. Cyberbeveiliger Check Point noteerde dat de afgelopen maanden ten minste vierduizend domeinnamen over het virus werden geregistreerd, schrijft de Nederlandse vakwebsite Computable. Ongeveer 3% van die websites blijkt kwaadaardig.

Tesorion uit Leusden constateerde de afgelopen dagen een vervijfvoudiging van dergelijke valse berichten in zijn *security operations center*. Absolute aantallen wil het cyberveiligheidsbedrijf, met ruim 160 medewerkers, niet geven. De wereld van cyberveiligheid zit nu eenmaal vol geheimen.

Ook e-mailbeveiligingsbedrijf Barracuda ziet wereldwijd een duidelijke toename van coronascam. De grootste hoeveelheid nepberichten over het virus ging deze maand rond in Azië, gevolgd door Noord-Italië — de eerste twee plekken waar het coronavirus om zich heen greep — maar ook Noordwest-Europa doet inmiddels aardig mee.

In Nederland ging onder andere een bericht rond dat van het Rijksinstituut voor Volksgezondheid en Milieu (RIVM) afkomstig leek, constateerde mailbeveiligingsbedrijf Mimecast. De mail gaf wat algemene informatie over de Nederlandse situatie. Meer specifieke informatie was — u raadt het al — achter een link te vinden.

Sommige opstellers van nepberichten zijn uit op inloggegevens, anderen installeren virussen (voor de computer) of willen betaalgegevens roven. Zo ontdekte Mimecast een e-mail die sprak over een compensatiefonds voor schade door corona (vul hier je bankrekeningnummer in). En er blijken vaccins tegen corona op de markt (betaal direct met creditcard).

De nepsites kunnen behoorlijk vernuftig in elkaar zitten, weet Stefan van der Wal, *pre sales engineer* bij Barracuda. Ze bieden bijvoorbeeld ook een mogelijkheid om een tweede factor, bijvoorbeeld een code per sms, in te vullen. De nepsite vult die gegevens vervolgens direct in op de echte site.

Dat cybercriminelen inhaken op de actualiteit is niet nieuw. Wel worden nepmails steeds vaker in kleine hoeveelheden verstuurd en zijn ze vaker afgestemd op een specifieke groep. 'De kans dat de berichten worden opgespoord door een spamfilter wordt daardoor kleiner en de kans dat iemand erin trapt groter', zegt Van der Wal van Barracuda.

Met allerlei technieken weten beveiligingsbedrijven veel mails alsnog op te sporen. Maar het blijft een kat-en-muisspel. Van der Wal: 'Als cybercriminelen goed hun best doen, weten ze mij misschien ook te pakken.'

> **Thuiswerken? Je klikt, de bekende Office-pagina verschijnt. Alleen nog even het wachtwoord intikken**

> **Sommige opstellers van nepberichten zijn uit op inloggegevens, anderen installeren computervirussen**