Twijfels over cyberdiefstal Russische bende

Klaas Broekhuizen
Monday 11 August 2014, 07:16
update: Monday 11 August 2014, 08:01

De berichten over de Russische diefstal van ruim een miljard inloggegevens, moeten met een korrel zout worden genomen.

Dit zegt Axel Arnbak, onderzoeker cybersecurity en informatierecht aan de Universiteit van Amsterdam en research fellow aan het Berkman Center van de Harvard University.Vorige week kwam het nieuws naar buiten dat Russische privéhackers 1,2 miljard westerse inlognamen en wachtwoorden zouden hebben gestolen. ‘Het is gemeld door Hold Security, een Amerikaanse firma waar ik nog nooit van had gehoord’, zegt Arnbak. ‘De details over die inbraak zijn niet vrijgegeven en ook niet gedeeld met het internationale netwerk van Crisis Emergency and Response Teams. Dat is vreemd. Hold Security bood wel meteen een abonnement aan om voor $120 per jaar te onderzoeken of je naam op de lijst van gehackte accounts staat.’

Bovendien zouden de Russische inbrekers volgens Arnbak de gegevens willen gebruiken om de gebruikers twitterspam te kunnen toesturen. ‘Die informatie is weinig waard. Alles bij elkaar heb ik me daarom nogal gestoord aan hoeveel aandacht en dynamiek dit al snel kreeg in alle media. Het had toch echt meer weg van een goede marketingcampagne van Hold Security.’

Onafhankelijke media

In het algemeen moeten volgens Arnbak vraagtekens worden gezet bij berichten over aanvallen op onafhankelijke media en 'kritische infrastructuur' zoals elektriciteitsnetwerken of energiecentrales. Vaak wordt gesuggereerd dat hier overheden achter zitten, maar dat de aanvallen zijn volgens Arnbak amper aan te herleiden tot landen. 'Bij een raketaanval is het vrij snel duidelijk wie deze heeft uitgevoerd, maar bij een goede cyberaanval is dat heel moeilijk te achterhalen. Er zijn allerlei anonimiseringstechnieken, waardoor aanvallen gedaan kunnen worden zonder dat er een duidelijke dader is te vinden.'

Omdat moeilijk is vast te stellen wie er achter een cyberdiefstal zit, is er veel ruimte voor spin, bevestigt Arnbak. 'Je moet je altijd afvragen wie wat zegt. Ongeveer een jaar geleden stelde een Amerikaanse firma dat Chinezen vanuit een gebouw in Sjanghai cyberaanvallen uitvoerden op The New York Times. Maar Chinezen zijn echt wel zo geavanceerd dat hun aanval niet te achterhalen is. Dan zet je toch een vraagteken achter de Amerikaanse firma die met dat nieuws komt', zegt Arnbak. Zijn advies is dan ook dat iedereen zich vooral op de eigen verdediging moet richten, en niet zozeer op de moeilijk te achterhalen aanvaller.

Cyberaanvallen? Ja!

Dat Rusland cyberaanvallen uitvoert als onderdeel van oorlogvoering, staat volgens Arnbak vast. Estland en Georgië, buurlanden van Rusland, zijn al eens het doelwit geweest. 'Het is ook begrijpelijk dat je, voor de troepen het land binnenrijden, de onafhankelijke media en elektriciteitscentrales uitschakelt.' Deze redenering omdraaien (zodra er een cyberaanval is, moet je beducht zijn op binnenrijdende troepen) noemt Arnbak te voortvarend. 'Maar cyberaanvallen passen wel bij oplopende spanningen.'