Oekraïne hackte het Songfestival

Martin Heijnsbroek
zaterdag 21 mei 2016

We lezen over cybercrime als er weer iets spectaculairs gebeurt. Zoals met de centrale bank van Bangladesh, die in februari dit jaar $ 80 mln verloor omdat hackers toegang hadden tot het betalingssysteem Swift. Het meeste van wat er in die criminele cyberwereld gebeurt, gaat natuurlijk onopgemerkt aan ons voorbij. Maar als je het een beetje volgt, dan gaat er een complete industrie voor je open.

Wist je bijvoorbeeld dat hackers en veiligheidsdiensten continu informatie over nog onbekende softwarelekken opkopen van andere hackers, om met deze lekken toegang te krijgen tot je computer? Of dat je abonnementen voor € 1000 per maand kunt aanschaffen waarbij je met slimme software geholpen wordt om je 'malware' te installeren op duizenden andere computers, om daarmee iemands gegevens voor online bankieren te stelen?

En heb je eens gekeken op die websites, met registratie op de Cocoseilanden, waar je gestolen creditcardgegevens kunt kopen? Ter info: kaartgegevens met cvc-code kan je hier kopen vanaf $ 2 per kaart. Een kaart met gelezen magneetstrip kost je zo'n € 50. Het bijzondere is dat deze sites gewoon op het web te vinden zijn, omdat ze elke minuut van internetadres veranderen. Ze worden namelijk gehost op meer dan 2000 computers in Oost-Europa, die zelf ook weer gehackt zijn — een soort cloud-hosting voor de cybermaffia.

Het zijn niet alleen de burgers die in de professionalisering van cybercrime risico lopen, maar natuurlijk ook de bedrijven en overheden. Waar een phishing-aanval met een generieke e-mail aan honderdduizenden mensen hun wachtwoord en bankgegevens opvraagt, zijn er ook persoonlijke aanvallen op medewerkers. Die proberen op basis van alle informatie die over jou op het internet te vinden is, je een persoonlijke mail te sturen — bijvoorbeeld uit naam van je baas — waardoor je meer geneigd bent om belangrijke informatie te verschaffen.

En omdat de beveiligingstechnologie ook steeds slimmer wordt, realiseren de meeste organisaties zich dat de zwakste schakel in de keten vaak de medewerker zelf is. En om het risico van het roekeloos delen en openen van data en software over het internet te beheersen, moet je juist deze schakel versterken. Dus worden risico's uitgelegd aan medewerkers en wordt het 'compliance en security'-beleid vastgelegd. Bij MIcompany hebben we bijvoorbeeld voor alle medewerkers een jaarlijks examen en diverse security audits. Het is veel gedoe allemaal, om de ketting sterk te krijgen.

En daarom dacht ik verleden week even dat de uitzending van Nieuwsuur gehackt was. Ik hoorde dat de mail van minister Kamp gekraakt was met zo'n phishingaanval. En dat hij deze mail soms ook voor zijn werk gebruikt, als hem dat 'praktisch' uitkomt. Hij zag trouwens geen reden om dit te veranderen.

En toen Oekraïne het weekend daarop op onbegrijpelijke wijze Australië versloeg bij het Eurovisie Songfestival, wist ik het zeker: met die ‘crimeware as a service’ uit Oost-Europa worden we tegenwoordig zelfs op de televisie voor de gek gehouden.