INTERVIEW **MIKKO HYPPÖNEN** EXPERT CYBERVEILIGHEID

‘Maak fabrikanten aansprakelijk’

Finse expert Mikko Hyppönen pleit voor een cyberveiligheidslabel voor elektronische apparatuur.

FOTO ISTOCK

Door onze redacteur
Wouter van Noort

ROTTERDAM. Van Justin Bieber tot Amnesty International: vlak voor de verkiezingen van afgelopen woensdag twitterden ze ineens allemaal een Turkse tweet waarin Nederland een nazi-land werd genoemd, inclusief hakenkruizen. Via de externe dienstverlener Twitter Counter kregen hackers toegang tot de accounts en zo verspreidden ze hun politieke boodschap, naar aanleiding van de rel waarbij een Turkse minister Nederland werd uitgezet. De daders zijn nog niet opgespoord, maar het was de zoveelste politiek gevoelige hack van de laatste tijd: van de e-mails van de Amerikaanse Democratische Partij tot het recente WikiLeaks-lek van CIA-methodes.

„*Hacktivisten* uiten al langer hun mening online, dus zo’n hack als van Twitter Counter is op zich niets nieuws. Maar het aantal politieke hacks groeit absoluut”, zegt Mikko Hyppönen, de onderzoeksdirecteur van de Finse internetbeveiliger F-Secure. Hyppönen, lange paardenstaart en rond brilletje, is een van de bekendste cyberveiligheidsdeskundigen van Europa en is in Nederland voor cyberveiligheidscongres Security Bootcamp.

„Er is zeker een wapenwedloop aan de gang tussen staten, en de grenzen tussen activisten, criminelen en overheden vervagen daarbij”, zegt hij. „Ironisch genoeg is die wedloop vooral geëscaleerd na het lek over de methodes van de Amerikaanse NSA door Edward Snowden. Toen zagen andere landen ineens wat Amerikanen deden en konden ze niet achterblijven.”

Passen de recente onthullingen van WikiLeaks daar ook bij?
„Dat recente lek is een heel ander soort lek dan dat bij de NSA in 2013. Dat ging over massasurveillance. Dit nieuwe lek lijkt niet te gaan over jou of mij. De CIA richt zich met name op leiders van vijandige landen of terroristische organisaties. Hun methodes vereisen vaak dat iemand fysiek systemen infecteert: met een usb-stick in een smart-tv bijvoorbeeld. De IT-afdeling van IS zal wel druk zijn geweest de laatste week, maar de rest van de wereld hoeft zich volgens mij minder zorgen te maken.”

Is WikiLeaks überhaupt een betrouwbare bron?
„Ik vond WikiLeaks altijd leuk, maar nu niet meer. Acht jaar geleden lekten ze documenten die een echt schandaal blootlegden over het bedrijf Trafigura. Iedereen was het erover eens dat het goed was dat dat schandaal aan de kaak werd gesteld. Godzijdank dat WikiLeaks er was, transparantie! Maar wat er bij de Amerikaanse verkiezingen gebeurde, veranderde de zaak. Daarbij lekte WikiLeaks gehackte e-mails van de Democratische Partij. Dat was overduidelijk materiaal dat was gehackt door Russische inlichtingendiensten. Op een presenteerblaadje aan WikiLeaks gegeven, die het vervolgens publiceerde. Dat zorgt ervoor dat ze eruitzien als een middel van de Russen. We weten niet of het recente lek ook van de Russen afkomstig is, maar dat zijn wel vragen die je je moet stellen. Wel is het zo dat er geen aanwijzingen zijn dat WikiLeaks ooit documenten heeft gelekt die vals zijn. En het recente lek toont reële zwaktes in het ‘internet of things’.”

Welke zorgen heeft u daar over?
„Bij mensen thuis en in fabrieken komen allerlei apparaten online die slecht beveiligd zijn. Je zet een beveiligingscamera in je huis, en hackers kunnen je huis bekijken. Je bouwt een fabriek met slimme machines, en ineens kunnen buitenstaanders je fabriek bedienen. Er is maar één foutje nodig in de instellingen en het kan misgaan. Mensen zijn zich daarvan niet genoeg bewust. In thuisnetwerken is het niet meer je computer die je kwetsbaar maakt, het is je verdomde *smart* koffiezetapparaat.”

Daar wordt al jaren voor gewaarschuwd, en toch gebeurt er te weinig aan goede beveiliging. Wat zijn daarvoor oplossingen?
„Mensen moeten de gebruiksaanwijzing lezen, en hun wachtwoorden en instellingen op orde krijgen, maar dat is niet realistisch helaas. Fabrikanten moeten daarom zelf meer uitgeven aan de veiligheid, aan betere software en bijvoorbeeld verplichte installatie-*wizards* waar klanten helemaal doorheen moeten lopen om hun apparaten veilig in te stellen. Maar de markt lost dit niet op. Als mensen een wasmachine kopen, letten ze op de prijs, niet op de kwaliteit van de firewall.”

Als de markt het niet oplost, moeten overheden dan ingrijpen?
„Een oplossing is misschien iets als een energielabel, alleen dan voor de cyberveiligheid. Een bedrijf als Philips zal niet snel uit zichzelf zijn producten duurder maken voor betere veiligheid, daar moet regulering bij komen kijken. Fabrikanten van apparaten moeten daarnaast aansprakelijk gesteld worden voor slechte cyberveiligheid. Als een wasmachine kortsluiting krijgt en je huis in de fik zet, kan de fabrikant daarvoor aansprakelijk zijn. Als je wasmachine jouw wifi-wachtwoord lekt naar criminelen, moeten bedrijven daarvoor ook aansprakelijk worden gehouden.”

Fabrikanten zullen dat een onaanvaardbaar risico vinden; in de duizenden regels programmeertaal in hun producten hoeft maar één foutje te zitten en het is al mis.
„Als ze regulering willen voorkomen, moeten ze zélf beter hun best doen. Dat gebeurt soms al. De stichting achter besturingssysteem Linux werkt bijvoorbeeld aan zelfcertificering voor de beveiliging van het internet of things. Linux zit in de meeste internet of things-apparaten, dus dat kan een belangrijke eerste stap zijn. Maar er moet duidelijk wat gebeuren, want er komen snel miljarden apparaten online.”

> Een bedrijf als Philips zal niet snel uit zichzelf zijn producten duurder maken voor veiligheid

Wat niet bijdraagt aan het gevoel van urgentie: cyberdreiging lijkt steeds zo abstract, zo ver weg.
„Mensen voelen totaal niet wat het risico voor henzelf is, maar dat kan snel veranderen. Je ziet nu al steeds meer *ransomware*: software die belangrijke bestanden van slachtoffers kaapt, en pas in ruil voor losgeld weer vrijgeeft. Binnenkort krijg je vast ook ransomware voor het internet of things. Dat cybercriminelen je smart broodrooster hacken en hem pas in ruil voor een losgeld in bitcoin weer vrijgeven. Dat zien we nu nog niet, maar dat lijkt mij een kwestie van tijd als je ziet hoe snel de wedloop gaat.”

TED-spreker

Wie is Mikko Hyppönen?

Hyppönen (1969) is onderzoeksdirecteur van het Finse veiligheidsbedrijf F-Secure, waar hij sinds 1991 werkt. Hij is één van de meest zichtbare cyberveiligheidsexperts van Europa, onder meer dankzij enkele TED-talks die hij de afgelopen jaren hield.