volkskrant.nl

Opinie: Leg wettelijk vast dat experts onderzoek mogen doen naar gaten in cyberbeveiliging

5-6 minutes

*Dilan Yesilgoz-Zegerius, minister van Justitie en Veiligheid.*Beeld ANP

Op 10 oktober kwam de nieuwe Nederlandse cybersecuritystrategie uit. Volgens minister Yeşilgöz-Zegerius van Veiligheid en Justitie neemt de digitale dreiging fors toe: buitenlandse mogendheden en criminelen bedreigen onze belangen, ook in het digitale domein. En minister Adriaansens van Economische Zaken en Klimaat onderstreept bij publicatie dat digitale weerbaarheid echt belangrijk is.

Over de auteur

Ot van Daalen is advocaat en oprichter van advocatenkantoor Root Legal dat zich specialiseert in privacy en securityrecht. Hij is onderzoeker op het gebied van cybersecurity bij de Universiteit van Amsterdam en heeft onlangs een proefschrift afgerond over de wettelijke bescherming van onderzoek naar informatiebeveiliging.

De strategie zit bomvol goede voornemens. Zo moet informatie over dreigingen beter worden gedeeld, slachtoffers beter worden

geïnformeerd, het bedrijfsleven beter worden beschermd en digitale producten beter worden beveiligd. Daar worden in de komende jaren miljoenen voor uitgetrokken – miljoenen die hard nodig zijn, want ik ben het met ze eens: onze digitale infrastructuur is slecht beveiligd. Kijk maar naar de stroom datalekken en aanvallen met ransomware waarover we wekelijks lezen.

Ethisch hacken

Maar het gekke is: voor een expert blijft het gevaarlijk om onderzoek te doen naar informatiebeveiliging en om hierover te publiceren. Soms is het strafbaar dit soort onderzoek te doen en hierover te publiceren. Nu heeft heeft het Openbaar Ministerie in Nederland gelukkig aangegeven dat ze ethische hackers niet zal vervolgen, mits die hun hacks op een nette manier uitvoeren. Maar niet alle hackers vertrouwen die toezegging, en nog belangrijker: je moet altijd rekening blijven houden met een bedrijf dat een rechtszaak tegen je aanspant, zelfs als het OM heeft besloten geen strafzaak te beginnen.

Vraag maar aan Bart Jacobs, security-hoogleraar aan de Radboud Universiteit. Toen hij met zijn team zijn onderzoek wilde publiceren naar de slechte beveiliging van toegangschips, werd hij in 2008 voor de civiele rechter in Nederland gedaagd. En toen hij en zijn team een onderzoek naar de beveiliging van auto’s hadden gedaan,

verbood de Engelse rechter hem in 2013 over kwetsbaarheden te publiceren.

Ondertussen bleven die auto's dus onveilig. Met als gevolg dat onderzoekers wel twee keer nadenken voordat ze onderzoek naar serieuze kwetsbaarheden naar buiten brengen. Ook de Europese organisatie die verantwoordelijk is voor informatiebeveiliging, Enisa, concludeerde in 2022 dat experts in Europa nog steeds een juridisch risico lopen bij het doen van informatiebeveiligingsonderzoek.

Riskant

Dat is verschrikkelijk zonde. Want informatiebeveiliging is een continue cyclus van het nemen van maatregelen, en het vervolgens schenden van die maatregelen, waarop die maatregelen weer worden versterkt, et cetera. En het is nu eenmaal zo dat veel informatiebeveiligingsonderzoek wordt gedaan door buitenstaanders – experts die niets te maken hebben met de producten en diensten waarnaar ze onderzoek doen. Denk aan het Dutch Institute for Vulnerability Disclosure (DIVD), een Nederlands initiatief van vrijwilligers dat continu online-kwetsbaarheden opspoort en betrokken partijen informeert.

Om informatiebeveiliging te verbeteren, moet dit soort werk juridisch niet riskant zijn, maar juist worden gekoesterd: het moet

wettelijk worden vastgelegd dat experts dit soort onderzoek mogen doen, mits ze de resultaten daarvan op een verantwoordelijke manier delen met de betrokken partijen, zodat die hun beveiliging weer kunnen verbeteren.

En daarnaast moet de overheid het makkelijker maken voor onderzoekers om de bevindingen van dat onderzoek te melden. Want echte cybersecurity gaat niet alleen over het dichten van gaten – het gaat ook over het vínden van gaten. Mits je dat ethisch doet, zou dat moeten worden gestimuleerd.

Hier zou content moeten staan van bijv. Twitter, Facebook of Instagram

Om u deze content te kunnen laten zien, hebben wij uw toestemming nodig om cookies te plaatsen. Open uw cookie-instellingen om te kiezen welke cookies u wilt accepteren. Voor een optimale gebruikservaring van onze site selecteert u "Accepteer alles". U kunt ook alleen de sociale content aanzetten: vink hiervoor "Cookies accepteren van sociale media" aan.