Hacken om te help

tekst Pieter Ariese
beeld RD, André Dorst

De overheid wil goedwillende hackers meer ruimte geven om lekken in websites en systemen te melden. Maar de richtlijnen die minister Opstelten hiervoor presenteerde, oogsten kritiek van professionele beveiligers én hackers.

De beveiliging van it-systemen is complex. De overheid realiseert zich dat en werkt daarom binnen het Nationaal Cyber Security Centrum (NCSC), verantwoordelijk voor 's lands digitale veiligheid, samen met tal van private partners en bedrijven.

Dat ook goedwillende, "ethische" hackers een bijdrage kunnen leveren aan meer digitale veiligheid, werd lange tijd genegeerd. Hackers die zwakke plekken meldden bij bedrijven, kregen niet zelden nul op het rekest. Soms resulteerde een melding in dreiging met juridische stappen of daadwerkelijke vervolging.

De realiteit is dat er hackers zijn die op beveiligingsrisico's stuiten, terwijl ze zónder criminele motieven online actief zijn. Met hun vaak grote technische kennis leggen ze problemen bloot die duurbetaalde it-afdelingen over het hoofd zagen.

Anders dan cybercriminelen misbruiken ze deze defecten niet. Maar omdat melden geen soelaas biedt, doen ze er het zwijgen toe en gebeurt er niets. Met het risico dat een kwaadwillende hacker alsnog zijn slag kan slaan.

Aangespoord door een Kamermotie van Hachchi (D66) en El Fassed (GroenLinks) stelde het NCSC een richtlijn op voor "responsible disclosure", het verantwoord melden van kwetsbaarheden. De leidraad (zie kader) moet duidelijk maken wat ethisch hacken inhoudt, onder welke voorwaarden het mag en welke grenzen hackers in acht moeten nemen.

Heldere kaders, waar iedereen mee uit de voeten kan. Zou je denken. Maar de regels leiden tot de nodige kritiek. Tijdens een paneldiscussie over het onderwerp, vorige maand in Den Haag, stonden professionele beveiligingsbedrijven en ethische hackers soms lijnrecht tegenover elkaar.

Een van de experts die doorgaans een goede boterham verdienen met beveiligingstests, zei te vrezen dat criminelen de regels zullen aangrijpen om zichzelf een dekmantel te geven. Een ander stelde dat, zonder melding vooraf, het hacken van systemen gelijkstaat aan inbreken.

Ethische hackers daarentegen gaat de richtlijn niet ver genoeg. Praktijkvoorbeelden van meldingen ontbreken, en er zijn onvoldoende garanties dat ze gevrijwaard blijven van juridische stappen.

Jacco van Tuijl is zo'n ethische hacker. Een beveiligingsenthousiast, noemt hij zichzelf. Hij legde de afgelopen jaren talloze –naar eigen zeggen honderden– zwakke plekken in websites en it-systemen bloot. De getroffen organisaties waren niet de minste: (semi)overheid, grote financiële instellingen én beveiligingsbedrijven.

Voorbeelden noemt hij zelf liever niet, „omwille van de betrokken partijen", maar een korte zoektocht op internet levert namen op als Europol, TNO, Cisco, communicatienetwerk C2000 en diverse ministeries. Zijn ervaringen bij het melden van de kwetsbaarheden zijn veelal negatief. „Een van de grootste financiële instellingen van Europa bedreigde me: „Als je hier ooit mee naar de media stapt, zit je voor de rest van je leven in de rechtbank.""

Een ministerie waar hij zich meldde, bedankte netjes. „Maar ze waarschuwden me ook om „een stapje terug te doen": een ander ministerie was er namelijk opuit me te vervolgen."

Nadat Van Tuijl aanklopte bij een gemeente met de mededeling dat alle gegevens van mensen met een uitkering –inclusief inkomen en burgerservicenummer– inzichtelijk waren via de website, antwoordde de webbeheerder: „Bedankt voor de tip. We nemen het mee in de volgende versie." Die vervolgens nog maanden op zich liet wachten.

„Als je naar de media stapt, zit je voor de rest van je leven in de rechtbank"

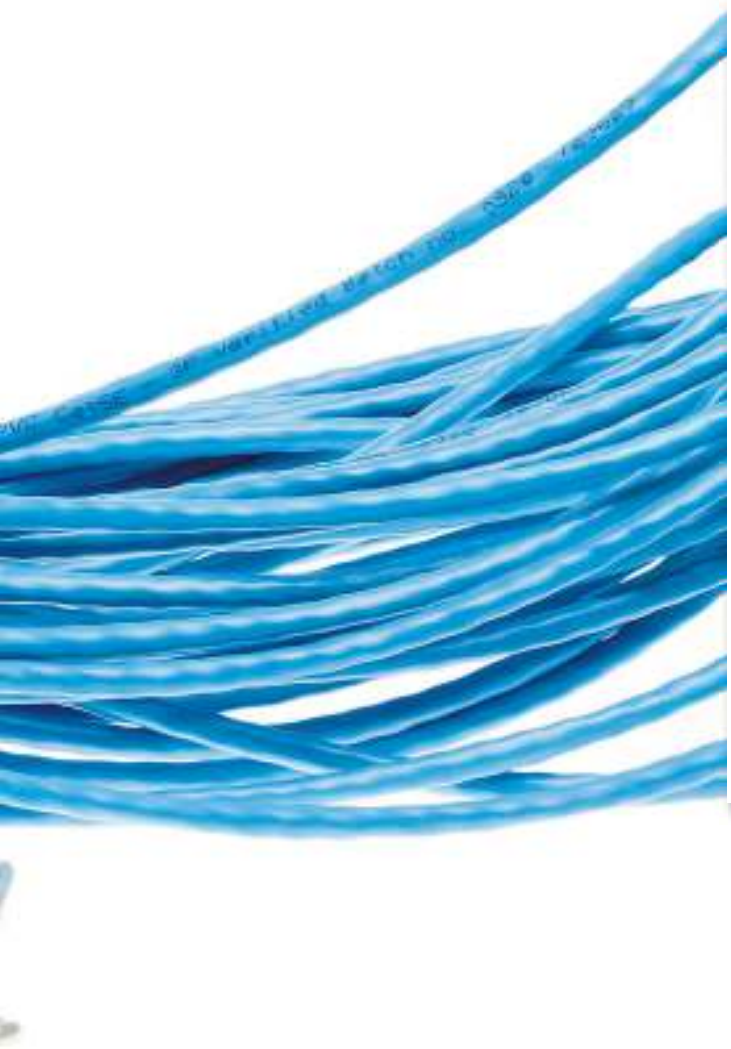
Is de richtlijn een stap in de goede richting?

„Ik vind het vreemd dat de overheid regels opstelt voor hackers met goede intenties. Het zijn juist de softwareontwikkelaars en systeembeheerders voor wie richtlijnen geschreven zouden moeten worden. De verantwoordelijkheid van de organisatie die gegevens lekt, blijft erg onderbelicht.

Wat mij betreft werken de regels eerder beperkend. Strafrechtelijke vervolging wordt niet uitgesloten en de anonimiteit van de melder wordt niet gegarandeerd. Daardoor zullen ethische hackers lekken soms niet meer melden, wat de situatie alleen maar verslechtert."

Maar het is nu toch duidelijk wat wel en niet mag?

„De leidraad verbiedt bijvoorbeeld het downloaden van gegevens. Maar zolang dat niet mag, heeft een hacker alleen een vermoeden van een zwakke plek en kan hij niet vaststellen of het daadwerkelijk mogelijk is gevoelige gegevens



Responsible disclosure

Het Nationaal Cyber Security Centrum omschrijft "responsible disclosure" als het „op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ict-kwetsbaarheden."
De leidraad onderstreept de belangrijke rol van ethische hackers. Hij benadrukt dat getroffen organisaties en melders moeten samenwerken om de digitale veiligheid te vergroten.
Daarvoor stelt het NCSC een aantal richtlijnen voor. Zo moeten bedrijven het laagdrempelig maken om melding te doen. Hackers op hun beurt mogen de zwakke plek niet misbruiken, gegevens wijzigen of verwijderen.
Bedrijven die beleid willen opstellen voor het geval ethische hackers zich melden kunnen een voorbeeld vinden op de website responsibledisclosure.nl.

en

in te zien, aan te passen of de controle over vitale systemen over te nemen. Mijn ervaring is dat organisaties nadat een lek is gemeld niet altijd de waarheid spreken over de gegevens die op straat liggen. In de media beperken ze hun verhaal tot de data waarvan ze weten dat de hacker die heeft gezien. Of erger: ze stellen dat hij overdrijft, dat er eigenlijk niets aan de hand is.

Zo trekken ze de geloofwaardigheid van de goedwillende hacker publiekelijk in twijfel. Als hij geen bewijs kan downloaden, kan hij zich hiertegen niet verweren.

Daarnaast is het moeilijk om organisaties te overtuigen van de ernst van een gevonden kwetsbaarheid. Er zijn softwareontwikkelaars die nog nooit van een sql-injectie hebben gehoord, een veelgebruikte techniek om websites te kraken. Om hen te overtuigen, zal je moeten bewijzen dat je bij gevoelige gegevens kunt."

Downloaden zonder toestemming, is dat niet gewoon stelen?
„Stelen is wegnemen. Dat is niet aan de orde; een ethische hacker zal niet moedwillig gegevens verwijderen. Hij bepaalt enkel wat de omvang van een informatielek is en hij stelt bewijs veilig waarmee hij zich kan verweren als hij in de media wordt gebagatelliseerd of zelfs belachelijk wordt gemaakt.

De gedownloade gegevens kunnen ook nuttig zijn voor toezichthoudende instanties. Die kunnen eruit afleiden of bedrijven zich wel aan de wettelijke normen houden. Denk aan de Wet bescherming persoonsgegevens of regels waar banken of organisaties die medische gegevens verwerken aan moeten voldoen.

Ik snap dat die liever niet hebben dat een hacker het bewijs van hun nalatigheid en onkunde in handen heeft. Maar als ze tekortschieten of hun verantwoordelijkheid niet nemen, moeten ze daarop aangesproken kunnen worden."

Sommigen stellen dat onaangekondigd hacken strafbaar moet blijven...
„Als een aannemer door een gebouw loopt en ziet dat het op instorten staat, dan vind ik het zijn plicht dat te melden.

Zelf zal ik geen servers binnendringen als mij daar niet om is gevraagd. Maar ik steek ook m'n kop niet in het zand als me tijdens het bezoeken van een website duidelijk wordt dat deze aan alle kanten gevoelige gegevens lekt of kwaadaardige software verspreidt. Dan zal ik niet zwijgen.

Ik wil het omdraaien: je moet geen huis bouwen als je daar geen verstand van hebt. Zo moet je ook geen gevoelige informatiesystemen bouwen als je niet weet hoe dat moet. Doet een bedrijf dat wel, dan moet het daar zelf de consequenties van dragen. Niet de mensen die het bedrijf erop wijzen."

Iemand die twittert dat hij de kersttoespraak van de koningin heeft gevonden, is dat ethisch?
„Daar kan ik niet over oordelen. Het draait bij ethisch hacken om de intentie: die moet goed zijn. Wat mij betreft passeer je wel een grens als je organisaties niet de tijd geeft om problemen op te lossen voordat ze in de media worden gebracht."

Wat moet er gebeuren om de leidraad tot een succes te maken?
„Er moet een instantie zijn die bemiddelt tussen de melder en de lekkende organisatie. Het NCSC of het College bescherming persoonsgegevens zou deze rol op zich kunnen nemen. Ze kunnen onafhankelijk de goede bedoelingen van de melder vaststellen en er vervolgens op toezien dat de lekkende organisatie haar verantwoordelijkheid neemt."

column

Protocollen

tekst Joop Hardeman

Straks komt de insectentijd er weer aan, dus we moeten als gezin maar eens bedenken hoe we dit probleem gaan aanpakken. Verdelgen we het ongedierte met een vliegenmepper, met een krant, of is de stofzuiger ook toegestaan? Wie heeft dit corvee in de even weken en wie in de oneven? Wie is eindverantwoordelijk voor dit deel van het huishouden? We moeten zorgen dat voor Koninginnedag alles vastligt, zodat we in de zomer en de herfst gegarandeerd geen last van kleine beestjes hebben. Daarna kunnen we begin november alles evalueren en waar nodig de regels aanpassen.

Zo, dit is ons insectenprotocol. We gaan er ook nog een maken voor het inleveren van de was, voor het opruimen van de slaapkamers, voor het bijhouden van de fietsen, voor – tja, waarvoor niet? Misschien landt er een zieke arend in onze tuin. Dan moeten we ons achteraf wel kunnen verantwoorden tegenover de Dierenbescherming, de gemeente, de Partij voor de Dieren, de buren, de PVV en de dierenarts.

Nederland protocolland. Hoe zou dat toch komen? Ik ga een poging doen: idee van maakbaarheid, gebrek aan verantwoordelijkheidsgevoel, teloorgang van het gezag, ontbreken van nuchterheid, compensatie van gevoelens van onzekerheid en instabiliteit. Het draait dus om mentaliteit en vertrouwen of –liever– om het verdwijnen daarvan. Tussen haakjes: daarom ook dat soms overdreven gehamer op openheid en transparantie. Wie daar een zekere grens aan wil stellen, is bij voorbaat verdacht.

Ik vrees dat er nog een ander aspect is. Er is een link met de ontkerkelijking in ons land. Het loslaten van de Tien Geboden doet roepen om nieuwe regels. Maar dan nu genormeerd naar de waan van de dag. Daarnaast geeft de secularisatie gelegenheid om zaken die niet deugen geaccepteerd te krijgen. Giet ze in een protocol, waarna alleen nog gekeken hoeft te worden of de richtlijnen wel precies zijn gevolgd. Zo ja, dan is het goed.

Helemaal mis natuurlijk, want wat niet deugde, is nog steeds fout. Abortus blijft verschrikkelijk, ook al wordt er precies volgens de regels gewerkt.

Gezonde regelgeving is oké. Een uniforme handleiding kan handig zijn. Maar doorgeslagen geloof in protocollen zal telkens op teleurstelling uitdraaien. Alles krampachtig in de hand houden, lukt niet. Omdat (onverwachte) situaties niet hetzelfde zijn en menselijk gedrag ongrijpbaar blijft.

Ik herinner me een interview met een ouderling die al zo'n veertig jaar in het ambt stond. De desbetreffende kerkelijke gemeente ging splitsen vanwege doorgaande groei. Uiteraard werd er over de nieuwe kerkgrens nagedacht. Maar dat die grens in de praktijk een stippellijn zou zijn, wist die ervaren ambtsdrager wel: „Mensen zijn geen turven."