Sogeti hackers vertellen over de valkuilen van de praktijk

ETHISCH HACKEN? **ETHISCHE** SECURITY!

Ethisch hacken is in de mode, maar sommige beoefenaars hebben een hekel aan de toevoeging ‘ethisch’. Niet omdat ze blackhat zijn, maar omdat ethiek eigenlijk normaal moet zijn. Ook voor kwetsbare organisaties die soms te weinig doen aan security. “Je noemt een dokter toch ook geen ethische dokter”, zeggen de hackers bijna in koor.

Michel van Veen:
‘Er zijn verschillende ethische stromingen’

Marinus Kuivenhoven:
‘We helpen steeds meer bedrijven met het maken van een security roadmap’

"Ethiek kun je niet in één ding vangen", zegt securitytester Arend Wolters tijdens een rondetafelgesprek over ethisch hacken. Hij en zijn collega-hackers bij IT-dienstverlener Sogeti bespreken het belang van ethiek plus de haken en ogen daaraan voor security. "Het gaat om hele grote dilemma's", knikt securityspecialist Rory Breuk.

GROTE DILEMMA'S

Cybersecurity specialist Michel van Veen vult aan: "Er zijn verschillende ethische stromingen." Want wat is nou precies ethisch: het melden en stilhouden van een kwetsbaarheid of het openlijk onthullen van een lek? De felle discussie over respectievelijk non-disclosure en full disclosure loopt al jaren, met nog tussenvormen zoals responsible disclosure en coordinated disclosure.

"Full disclosure is niet ethisch", reageert Jacco van Tuijl. Het volledig vrijgeven van een kwetsbaarheid compleet met details om er misbruik van te maken, kan niet door de beugel. De andere hackers vallen hem bij. Een aanpak met een timer voor de disclosure, zoals Google hanteert, kan beter zijn. "Responsible disclosure is wel een stok achter de deur", erkent Breuk. Hij zet dit dilemma verder uiteen met de hamvraag: hoe lang wacht je voordat je tot onthulling overgaat?

TIJD VERSUS IMPACT

De timing van onthulling na een paar dagen kan namelijk conflicteren met de complexiteit van een fix en de benodigde tijd voor het uitrollen daarvan. "Hoe lang is er nodig?", vraagt Breuk. Securitytester Guus Siebers draagt aan om het aan de organisatie zelf te vragen, wat hun inschatting is. "Maar soms kun je niet updaten", weet Van Tuijl. Het dichten van een lek kan bijvoorbeeld technisch niet mogelijk zijn of heeft teveel 'bijwerkingen'. "Soms wordt een oplossing overruled, bijvoorbeeld omdat het teveel business impact heeft", weet Siebers uit ervaring. Belangrijk is ook een afweging over de kwetsbaarheid zelf, voegt Breuk weer toe. "Wat is het: een klantenbestand of een DoS?" Kunnen gevoelige gegevens op straat komen te liggen of loopt een organisatie 'slechts' het risico van een DoS-aanval (denial of service)? Het beste zou zijn om samen met de getroffen leverancier of gebruikende organisatie een kwetsbaarheid in stilte te fixen, opperen de securityspecialisten van Sogeti. "En het moet ook via een betrouwbaar kanaal gaan", concludeert Wolters.

OBSTAKELS IN DE PRAKTIJK

Helaas is de realiteit anders. Enerzijds omdat de factor tijd niet alleen wordt bepaald door de ontdekkers en de fixers van kwetsbaarheden. Als wij iets kunnen vinden, kan een ander dat ook, legt de groep ethische hackers uit. Die ander kan dan criminele bedoelingen hebben. Anderzijds is er nog de complicerende factor van de getroffen leverancier of gebruikende partij. Soms kan of wil die een kwetsbaarheid niet oplossen. Bijvoorbeeld vanwege te hoog geachte kosten voor het fixen.

"Ik heb dat wel vaker gehoord", vertelt Van Tuijl. Hij heeft lang geleden een kwetsbaarheid bij gemeenten gevonden waardoor hij toegang kon hebben tot informatie over alle uitkeringen. Na netjes melding te hebben gedaan, kreeg hij een verrassende reactie: 'Het fixen hiervan kost tien euro per inwoner, dat gaan we niet doen'. De ethische hacker verbaasde zich over het gebrek aan verantwoordelijkheidsgevoel van de kwetsbare instantie. Want wat kost de eventuele schade die burgers lijden wel niet? En is dit wel ethisch?

MOEIZAAM MELDEN

Zijn eigen ethiek heeft hem er nog wel toe aangezet om de gevonden kwetsbaarheid elders aan te kaarten. Maar waar dan? Waar kun je terecht? Het NCSC (Nationaal Cyber Security Center) en het centrale meldpunt daar bestonden toen nog niet, legt Van Tuijl uit. En bij GovCERT.nl kreeg hij nul op het rekest. De kleinschalige voorganger van het NCSC opereerde namelijk voor organisaties die lid waren en het lek bij gemeenten viel buiten die scope.

In die tijd was het lastig om van hacken een fulltime baan te maken, geeft de security-expert van Sogeti aan. Dat is na 2011 wel veranderd. Mede door de beruchte Lektober-actie waarbij elke dag in oktober een beveiligingsgat of privacylek is onthuld. Tegenwoordig valt er een goede boterham te verdienen met ethisch hacken, zegt Van Tuijl. "Ik kan nu volledig met security bezig zijn."

ALIAS UIT BITTERE NOODZAAK

Naast hacken binnen het werkgebied van Sogeti en haar klanten, zoekt hij ook elders naar kwetsbaarheden. Om die dan netjes te melden. Vanuit een drijfveer om de wereld veiliger te maken. "Dat doe ik niet uit eigen naam", geeft Van Tuijl aan. Het vinden van een kwetsbaarheid kan al strafbaar zijn, of in ieder geval vervolgbaar. Bovendien kun je een kwetsbaarheid al toevallig tegenkomen bij normaal gebruik, legt hij uit.

Van Tuijl heeft ooit melding gedaan van een groot beveiligingsgat en kreeg van de betrokken minister de boodschap dat hackers niet vervolgd worden als ze er geen gewin bij hebben. "Dus gebruik ik een alias." Dit om buiten schot te blijven wanneer een organisatie of aanklager toch meent dat er sprake is van gewin, of van schade die op iemand verhaald moet worden. Het is dus zaak om een betrouwbare tussenpartij te hebben.

ORGANISATIES DOEN HET STEEDS BETER

Op de vraag hoe bedrijven en overheden vandaag de dag met hun digitale veiligheid omgaan, zijn de hackers het snel eens over het antwoord. "Het gaat steeds beter, ook al verschilt het nog erg per organisatie. Bij het ene bedrijf moet de security-mindset nog veel groter worden", vertelt Tessa Smolenaars. Bij andere organisaties is het bewustzijn groot, maar wordt er nog teveel op eilandjes gewerkt. "Zo leiden wij ontwikkelaars op om security te borgen in het ontwikkelproces", vertelt Van Veen. "We helpen steeds meer bedrijven met het maken van een security roadmap", voegt Kuivenhoven toe. En toch is er ook nog altijd sprake van een bepaalde mate van naïviteit, vindt Van Tuijl. Zo zijn er nog genoeg ontwikkelaars die denken dat bijvoorbeeld een Internet-of-Things oplossing in een gesloten netwerk ontwikkeld kan worden. Dat is een illusie. Overal zit al draadloze technologie", aldus Van Tuijl.

HEKEL AAN 'ETHISCH' HACKEN

De ethische hackers aan tafel bij Sogeti zeggen tenslotte dat hacken nog te vaak verkeerd wordt gezien. Het is geen boosaardige of zelfs kwaadaardige activiteit. De toevoeging van het woord 'ethisch' aan wat hackers doen, is eigenlijk fout. Van Tuijl: "Dat komt door de media en films waarin de vreselijkste doemscenario's voorbij komen. Noem dat andere gewoon 'crimineel hacken'!" Zijn collega Breuk vat kort samen: "Ik heb een hekel aan 'ethisch' hacken."

Jasper Bakker, freelance journalist

Jacco van Tuijl:
'Full disclosure is niet ethisch'

Rory Breuk:
'Het gaat om hele grote dilemma's'

Tessa Smolenaars:
'Het gaat steeds beter, ook al verschilt het nog erg per organisatie'

Guus Siebers:
'Soms wordt een oplossing overruled, bijvoorbeeld omdat het teveel business impact heeft'

Arend Wolters:
'Ethiek kun je niet in één ding vangen'