Auteur: Chris van 't Hof is directeur bij DIVD en is bereikbaar via chris@divd.nl.

DIVD: het Rode Kruis van het internet

Vrijdagavond 2 juli 2021 startte REvil een wereldwijde ransomware-aanval via kwetsbaarheden in KaseyaVSA. Dit is software waarmee Managed Service Providers de IT van hun klanten op afstand kunnen beheren. Door deze kwetsbaarheid, een Authentication Bypass, konden de criminelen dus in een keer alle klanten van deze MSPs besmetten met ransomware. Het moment was niet toevallig gekozen: in de VS waren veel werknemers al naar huis om met bier en barbecue het weekend van de 4th of July in te luiden.

Niet bij het bedrijf Kaseya zelf, want daar gingen alle alarmbellen af. Onmiddellijk namen ze contact op met DIVD-onderzoeker Wietse Boonstra. Hij had namelijk diezelfde kwetsbaarheid al ontdekt op 2 april en nog zeven andere waar inmiddels ook een CVE-nummer voor was aangevraagd. DIVD-CSIRT Manager Frank Breedijk hielp hem een goede Proof of Concept te schrijven en DIVD-voorzitter Victor Gevers wendde zijn contacten aan om met Kaseya een Coordinated Vulnerability Disclosure traject in gang te zetten. Onderzoeker Lennaert Oudshoorn haakte aan om het internet te scannen op wie gebruik maakt van KaseyaVSA. Anders dan bij veel andere ontvangers van een CVD-verzoek, reageerde Kaseya destijds direct zeer coöperatief. De eerste zeven CVE waren al gefixed en patches werden verstuurd naar de MSPs. De laatste, de Authentication Bypass, was na twee maanden nog niet gefixed en Kaseya was dus net te laat.

Groot voordeel was dat DIVD al sinds april de hele IPv4 range van het internet scande op de aanwezigheid van KaseyaVSA. We kwamen op een totaal van 2.200 MSPs, elke met vele tientallen of honderden klanten in beheer, dus rond de miljoen potentiële slachtoffers. Er was ook al een early warning uitgegaan via CSIRT DSP richting MSPs dat er iets ernstigs aan de hand was met de software van Kaseya en er een disclosure aan zat te komen.

Nul potentiele slachtoffers

Met de contactenlijst van alle MSPs ging DIVD die vrijdagavond direct aan de slag om steeds weer alle IP-adressen te scannen op aanwezigheid van KaseyaVSA en meldingen uit te sturen naar de MSPs met de duidelijke boodschap: zet KaseyaVSA nu uit. Binnen Nederland waren er rond de honderd. Die werden niet alleen door DIVD gewaarschuwd, maar ook via onze Trusted Information Sharing Partners.

Intussen werden we ons ervan bewust dat we, door REvil te dwarsbomen ook zelf een target zouden kunnen zijn. Onze CISO Fleur van Leusden stelde direct de logfiles veilig, verhoogde de dijkbewaking en deed een treat analysis van de actor. En inderdaad, die zaterdag werd Wietses mailserver gebruteforced vanuit de Oekraiene, zonder al te veel schade. Op de DIVD-omgeving zagen we geen verdacht verkeer.

Zondag 4 juli zagen we eerst nog drie kwetsbare servers in Nederland online staan. De eigenaren daarvan werden gebeld en om 13.00 stond Nederland op nul potentiële slachtoffers van de ransomware aanval.

Rode Kruis van het internet

KaseyaVSA is een van de negentien onderzoeken die DIVD in 2021 heeft verricht. Daar publiceren we pas over als het onderzoek is afgerond. Echter, door de ransomware aanval en omdat het hier zero-days betrof die we zelf hadden ontdekt, kwam ons werk wel breed in de internationale media. Voorzitter Victor Gevers, CSIRT-manager Frank Breedijk en onderzoeker Wietse Boonstra waren in de week volgend op de aanval bijna dagelijks in het nieuws, in de VS o.a. bij CBS, Wall Street Journal en Bloomsberg en in Nederland bij RTL-nieuws, NOS Journaal en Nieuwsuur.

In de media zagen we een terugkerend patroon. Na uitleg over de aanval, verwonderden de journalisten zich vooral over het feit dat het wereldwijd scannen en melden van dergelijke kwetsbaarheden afhangt van een klein groepje Nederlandse vrijwilligers. Waarom doet de overheid of het bedrijfsleven dat niet?

Dat gebeurt ook wel, echter heeft elk van deze partijen zo hun eigen doelgroep en mandaat. DIVD werkt precies andersom. We zijn ook geen CERT of SOC voor een specifieke doelgroep, maar gaan uit van een kwetsbaarheid en scannen daar de hele wereld op. Zitten daar IP-adressen bij die volgens ons door anderen bediend worden, bijvoorbeeld hun CERT of Internet Service Provider, melden we ook via die partijen.

We blijven scannen en melden om potentiële slachtoffers te helpen, ongeacht wie of waar ze zijn, ongevraagd en gratis. DIVD is daarmee een soort Rode Kruis van het internet.

Het belang van ons werk werd ook erkend door de Onderzoeksraad voor de veiligheid in hun rapport 'Kwetsbaar door software' van (16 december 2021). DIVD wordt daarin 47 keer genoemd, met een beschrijving van onze onderzoeken en als een van de hoofdconclusies: 'Alle door de Onderzoeksraad onderzochte voorvallen laten zien dat (vrijwillige) beveiligings- onderzoekers een cruciale rol spelen in de incidentbestrijding.'

Wel een Engelse naam

Dat terwijl DIVD nog geen drie jaar bestaat. Het begon met het werk van Victor Gevers, alias @0xDUDE. Ik schreef al eerder over hem in mijn vorige boek Helpende Hackers (2015), waarvan ook diverse stukken zijn verschenen in dit tijdschrift. Hij was toen al 16 jaar bezig met het hele internet te scannen op kwetsbaarheden en die ongevraagd te melden bij degenen die het kunnen oplossen. Na 9.000 uur vrijwilligerswerk had hij toen 4.000 responsible disclosures op zijn naam staan. 2016 was het jaar waarin hij met zijn missie naar buiten trad, door het hele jaar rond, alle 366 dagen, 15 uur per dag lekken te vinden en te melden. Daarna is hij

Gaandeweg haakten steeds meer organisaties aan als zogeheten Trusted Information Sharing Partners.

geloof ik gestopt met het tellen van zijn disclosures.
Victor verscheen daarop vaker in de media en op evenementen en ik zag steeds meer hackers die zich wilden aansluiten bij zijn missie. In het voorjaar van 2019 besloten Astrid Oosenbrug, Victor en ik een stichting op te richten om zijn werk in onder te brengen. We vroegen vier cyberzwaargewichten om onze Raad van Toezicht te worden: Lodewijk van Zwieten, Petra Oldengarm, Herbert Bos en Ronald Prins - namen die in dit tijdschrift geen toelichting nodig hebben.
Hoe moeten we dan gaan heten? Er mag geen 'cyber' in onze naam voorkomen, want dat zou menig lezer van dit tijdschrift alleen maar oproepen ons te trollen. Liefst iets met 'vulnerability' en 'disclosure'. Moeten we dan het woordje 'responsible' of 'coordinated' ervoor zetten? Nee, dat wordt weer zo'n eindeloze discussie. Ik herinnerde me ineens dat ik de domeinnaam divd.nl nog had, om ooit nog eens de Democratische Inlichtingen- en Veiligheidsdienst op te zetten, een soort wiki voor dreigingsinformatie. Dat was bedoeld als grap en als naam van een serieus onderzoeksinstituut kon dit natuurlijk niet.
Het moet ook wel een Engelse naam zijn, want het internet houdt zich niet aan landsgrenzen. Maar met een vier letterige .nl URL lijkt het wel alsof je al lang bestaat, want de meesten daarvan zijn allang vergeven. Puzzelend met de vier letters kwam ik tot Dutch Institute for Vulnerability Disclosure. We doen onderzoek, onthullen kwetsbaarheden en doen het op z'n Nederlands: open, eerlijk en gratis. Daar kon iedereen zich wel in vinden.
Op 26 september gingen Astrid, Victor en ik naar de notaris om stichting Dutch Institute for Vulnerability Disclosure te registreren en op 1 oktober hebben we tijdens de OneConference DIVD gelanceerd. Daar sloot ook Frank Breedijk zich bij ons aan. Hij had namelijk net een Security Meldpunt opgericht om ook kwetsbaarheden bij organisaties te melden. We vonden het logisch dit initiatief meteen te incorporeren in onze nieuwe stichting. Dat was maar goed ook, want rond de jaarwisseling barstte de Citrix crisis los en was dit voor Frank het startsein voor zijn meldpunt.

Meedoen

CVE-2019-19781 werd op 17 december 2019 bekend gemaakt door Citrix zelf, echter zonder patch. Victor scande het hele internet en vond 128.777 kwetsbare servers online. Dat was toen nog te veel voor onze kleine organisatie om te melden. Matthijs Koot scande op de Nederlandse IP range en vond er 600. Dat was wel te doen. Toen 11 januari 2020 ook een exploit beschikbaar werd, activeerde Frank het Security Meldpunt, zocht de url's bij de IP-adressen en stuurde waarschuwingsmails naar info@, security@ en abuse@. Bij herhaalde scans zagen we de aantallen dalen en stuurde Frank herinneringsmails naar degene die nog kwetsbaar waren. De laatste tien hebben we gebeld.
Citrix was de kickstart voor DIVD en er volgden vele onderzoeken, die allemaal zijn terug te vinden op divd.nl. Het DIVD-meldpunt werd omgedoopt tot CSIRT, omdat alles op de site in het Engels is en we ook steeds meer buiten Nederland gingen melden. DIVD heeft inmiddels ook een eigen scan infrastructuur, dat ook ons eigen Autonomous System runt: AS 50559, IPv4 range 194.5.73.0 - 194.5.73.255. Daarmee weten degenen die gescand worden dat wij het zijn en houden we zelf als stichting controle over de scanresultaten.

Gaandeweg haakten steeds meer organisaties aan als zogeheten Trusted Information Sharing Partners. DIVD CSIRT stuurt in eerste instantie meldingen van gevonden kwetsbaarheden direct aan de gevonden potentiële slachtoffers maar vervolgens nogmaals via deze TISPs. Enkele zijn: NBIP voor providers, ZCERT voor de zorgsector, Surfcert voor het hoger onderwijs, IBD voor gemeenten, DTC voor het ondernemend Nederland, FERM voor de Rotterdamse haven, Connect2Trust voor CISO's onderling, Cyberveilig Nederland voor security bedrijven en NCSC voor Rijk en Vitaal. Hier komt in 2022 een aparte stichting voor, onder dezelfde naam die Frank Breedijk ooit gebruikte voor zijn meldactiviteiten: het Nederlandse Security Meldpunt.
Zoals in de vorige iB-magazine te lezen was, zijn we in 2022 gestart met een subsidie van DTC voor betaalde deeltijdfuncties. Dat zijn vooral managementtaken om de vrijwilligers te ondersteunen: administratieve ondersteuning vanuit LunaVia, Lennaert Oudshoorn als Head of CSIRT, Victor Gevers als Head of Research en ik als directeur DIVD. Hier komen nog hoofden bij voor de afdelingen HRM, Operations en Communication. Dit jaar gaat ook de DIVD Academy van start om jongeren het hackersvak bij te brengen en komt er een internationale tak CSIRT.global om DIVD chapters op te richten in verschillende landen.
Kortom, het wordt een mooi jaar voor DIVD. En als je mee wilt doen, weet je ons te vinden.