Beleidsplan DIVD - DUTCH INSTITUTE FOR VULNERABILITY DISCLOSURE

Wij streven ernaar om de digitale wereld veiliger te maken door kwetsbaarheden in digitale systemen te melden aan de mensen die deze kunnen oplossen. We hebben een wereldwijd bereik, maar doen het in Nederlandse stijl:
open, eerlijk, samen en gratis

We aim to make the digital world safer by reporting vulnerabilities we find in digital systems to the people who can fix them. We have a global reach, but do it Dutch style:
open, honest, collaborative and for free

Auteurs: Chris van ’t Hof en Astrid Oosenbrug

27 december 2021

1. INLEIDING

DIVD, Dutch Institute for Vulnerability Disclosure, is 1 oktober 2019 opgericht als platform voor security onderzoekers die op vrijwillige basis het internet scannen op veelvoorkomende kwetsbaarheden en de melden bij degenen die deze kwetsbaarheden kunnen verhelpen. We dragen hiermee bij aan een sterker internet. Omdat we een maatschappelijke doelstelling hebben, met vrijwilligers werken en geen winstoogmerk hebben, hebben we gekozen voor een stichtingsvorm. Dit geeft ons ook een neutrale positie, om van daaruit breed samen te werken met partijen in overheid en bedrijfsleven die ook werken aan vulnerability disclosures. De onkosten van onze stichting betreffen vooral overhead: softwarelicenties, verzekeringen, werkruimte en dergelijke. Vanaf 1 januari krijgt DIVD een klein managementteam dat deeltijd betaald wordt.

2. AANLEIDING EN DOELGROEP

Wereldwijd zijn er veel security onderzoekers die ook in hun eigen tijd zoeken naar kwetsbaarheden en die melden bij degenen die deze kwetsbaarheden kunnen verhelpen. Nederland loopt voorop in deze praktijk, die eerst werd aangeduid met Responsible Disclosure en nu vaker als Coördinated Vulnerability Disclosure. Het blijft echter voor individuele onderzoekers lastig om meldingen te doen vanuit hun eigen naam: ze moeten de ontvangers uitleggen wie ze zijn en dat ze het goed bedoelen, ze krijgen lastige vragen van journalisten, worden ongevraagd benaderd door recruiters of ontvangen in sommige gevallen dreigementen van advocaten. Deze individuele onderzoekers vinden vaak dezelfde kwetsbaarheden, wat leidt tot dubbel werk en verwarring bij ontvangers van meldingen.

DIVD verzorgt voor security onderzoekers een samenwerkingsplatform om hun bevindingen te vergelijken, eventuele onkosten te vergoeden en gezamenlijk naar buiten op te treden. DIVD is aanspreekpunt voor getroffen organisaties en partijen die meehelpen kwetsbaarheden te fixen, zodat dubbel werk wordt voorkomen en hiaten worden opgevuld.

In Nederland zijn al enige organisaties actief in vulnerability disclosure: NCSC voor Rijk en Vitaal, NBIP voor providers, ZCERT voor de zorgsector, IBD en Faalkaart voor gemeenten en Connect2Trust voor CISO's onderling. Ze bedienen echter specifieke doelgroepen, zijn beperkt in het delen van dreigingsinformatie en staan niet altijd open voor bevindingen van onafhankelijke onderzoekers. In het kader van het Landelijk Dekkende Stelsel van cybersecurity samenwerkingsverbanden, begint langzaamaan een netwerk te ontstaan waar meldingen van kwetsbaarheden kunnen worden neergelegd, maar dat is nog gefragmenteerd. DIVD keert het om: wij scannen heel Nederland, en staan open voor eenieder die actief zoekt naar veelvoorkomende, zware kwetsbaarheden, ongeacht bij wie die zich bevinden. We kanaliseren de activiteiten van een groeiend vrijwilligersleger en dienen verder geen politiek of commercieel doel.

DIVD is een veilige plek waar zowel beginnende als ervaren onderzoekers zich kunnen aansluiten om van elkaar te leren. Momenteel hebben we rond de zestig ervaren specialisten. Deze pool aan expertise kunnen we inzetten om beginnende onderzoekers te begeleiden in het vinden en melden van kwetsbaarheden. DIVD staat open voor hackers, gamers, schoolverlaters en jongeren. Bij DIVD wordt aandacht besteed aan 21e-eeuwse vaardigheden op het gebied van IT/internet/onderzoek. Omdat iedereen anders is, wordt gekeken naar een passend ontwikkeltraject. Uitgangspunt hierbij is dat talent zich niet altijd laat vangen in diploma's of opleidingen, maar dat de deelnemers wel aantoonbare vaardigheden op doen. Door het vergroten van kennis, vaardigheden, ethisch besef alsmede het verbinden van jong talent dat nu buiten de boot dreigt te vallen vervult DIVD een specifieke 21e-eeuwse niche op het gebied van IT-onderwijs, onderzoek en veiligheid.

3. DE STICHTING

Handelsnaam:	DIVD
Inschrijvingsnummer KvK:	75957345
Rechtsvorm:	Stichting
Datum inschrijving KvK:	26-09-2019
RSIN:	RSIN 860456961

De initiatiefnemers van DIVD en tevens bestuurders van de stichting zijn Victor Gevers, Astrid Oosenbrug en Chris van 't Hof. Zij maken onderdeel uit van zowel de hackers community als de meer formele cybersecurity sector. De initiatiefnemers hebben allen een aanzienlijke trackrecord in community building en kennisoverdracht in cybersecurity. De drie initiatiefnemers dragen elk vanuit hun eigen expertise, achtergrond, netwerk en interessegebied in gezamenlijkheid bij aan de opbouw en verdere uitrol van DIVD.

Victor Gevers (voorzitter) is onze onvolprezen kampioen in Coordinated Vulnerability Disclosure: 5.600 online kwetsbaarheden gevonden, gerapporteerd en opgelost. Daar heeft hij bijna twintig jaar over gedaan, met als piekjaar 2016. Toen heeft hij een sabbatical genomen om 366 dagen lang, vijftien uur per dag lekken te vinden en melden. Zonder in te breken ziet hij al op afstand standaardfouten in instellingen van databases, verouderde softwareversies, computers waarvan de standaard wachtwoorden niet zijn aangepast en apparaten die helemaal niet online horen staan. Nu doet hij geen individuele meldingen meer, maar handelt ze vanuit DIVD af in bulk - ongevraagd, gratis en open source. Onvermoeibaar scant hij miljoenen sites en vindt daarmee tienduizenden kwetsbaarheden, die allemaal netjes gerapporteerd moeten worden bij de eigenaren van die systemen.

Chris van 't Hof (secretaris) is onderzoeker, schrijver en presentator in cyber security. Met zijn bureau Tek Tok maakt hij ingewikkelde zaken in informatietechnologie leuk. Als spreker en dagvoorzitter heeft hij 500 optredens op zijn naam. Zijn achtste boek "Helpful Hackers. How the Dutch do Responsible Disclosure" (2016) sluit direct aan bij de doelstelling van de stichting. Sinds 2017 heeft hij een eigen live praatprogramma, Hack Talk, waar hij de hackers community en het brede publiek bij elkaar brengt.

Astrid Oosenbrug (penningmeester) is oud-PvdA-Tweede Kamerlid en werkte bij een aantal organisaties en bedrijven als senior systeembeheerder. Ook in haar Kamerwerk had ICT haar belangstelling, zij was van 2012 tot en met 2017 woordvoerder op dat terrein en daarnaast over overheidsdienstverlening, privacy, telecommunicatie en auteursrecht. Zij was kritisch over aantasting van privacy door nieuwe opsporingswetgeving. Oosenbrug heeft zich sterk gemaakt voor de invoering van het Responsible Disclosure beleid binnen de Nederlandse overheid en begeleidt al jaren minderjarige hackers in het doen van ethisch onderzoek. Ze was een ongecompliceerde, authentieke afgevaardigde, die zich in het parlement echter niet helemaal op haar plek voelde. Sinds 2018 is ze voorzitter van COC Nederland. In 2017 werd Oosenbrug uitgeroepen tot Dutch Digital leader of the year door CIONET en ITWNET.

Om deze bestuurders te adviseren en controleren, hebben we een Raad van Toezicht opgesteld. We hebben gekozen voor security zwaargewichten en hen de bevoegdheid gegeven niet-functionerende bestuursleden te ontslaan. Zij zijn: Lodewijk van Zwieten (voorzitter) van het OM, Petra Oldengarm van Cyber Veilig Nederland, Herbert Bos van de VU, Chantal Stekelenburg van Zerocopter en Ronald Prins van Hunt & Hackett.

Vanaf 1 januari 2022 krijgt DIVD een klein managementteam dat deeltijd betaald wordt: directeur (twee dagen / week), hoofd onderzoek (twee dagen / week), onderzoekscoördinator (een dag / week) en kantoorondersteuning vanuit LunaVia (een dag/week). Dit MT wordt van 2022 tot en met 2024 gefinancierd uit de 'Regeling Cyberweerbaarheid' van DTC.

4. Beloningsbeleid

DIVD is een vrijwilligersorganisatie. Onze kernactiviteit, onderzoek doen naar kwetsbaarheden en die melden, wordt verricht door vrijwilligers. Die krijgen geen vergoeding daarvoor, maar worden wel ondersteund met trainingen, technologische middelen en begeleiding.

Per 1 januari krijgt DIVD ook enkele betaalde krachten, zoals hierboven genoemd. Zij werken allen op freelance basis. Ongeacht de functie, krijgt elk eenzelfde tarief: 80,- euro per uur (ex BTW).

5. Activiteiten van DIVD

DIVD is 1 oktober 2019 in Den Haag officieel van start gegaan tijdens de One Conference, waar een open bijeenkomst werd gehouden voor iedereen die mee wil doen aan dit initiatief. Sommige onderzoekers kwamen direct opdagen met een lijst gevonden kwetsbaarheden, terwijl anderen aanboden om te helpen met sponsoring, het bouwen van het platform of wilde netwerken. Tijdens de conferentie mocht onze voorzitter Victor onze boodschap op het hoofdpodium brengen. Onze secretaris Chris bereikte ook het hoofdpodium. Niet als spreker, maar als dummy in een demo van een medische hack.

Tijdens deze lancering speelde de PulseVPN-zaak: onderzoeker Matthijs Koot had ontdekt dat honderden Nederlandse organisaties kwetsbaar waren en meldde dit als individu. Later trad hij toe als een van onze onderzoekers. Frank Breedijk, CISO bij Schuberg Phillis bleek bij de lancering al bezig te zijn met een soortgelijk initiatief, een Nederlands Security Meldpunt. Besloten is zijn meldpunt bij de stichting DIVD onder te brengen als het platform waar de Nederlandse meldingen worden afgehandeld, terwijl voorzitter Victor Gevers zich meer richt op de internationale scans en meldingen.

In januari 2020 speelde onze eerste publieke zaak. Toen bekend werd dat voor de recent bekendgemaakte Citrix kwetsbaarheid een exploit gepubliceerd was, hebben onze onderzoekers IP-adressen gescand op deze kwetsbaarheid. Onze internationale scan wees op 120.000 kwetsbare servers. Die konden we onmogelijk allemaal melden, al hebben we dat wel bij enkelen gedaan. De onderzoekers achter Security Meldpunt, onder andere Frank Breedijk en Matthijs Koot, vonden binnen de Nederlandse IP-range 700 kwetsbare servers en hebben die via providers, tussenpartijen of direct bij de eigenaren gemeld. Zij kwamen hiermee ook regelmatig in de media als Security Meldpunt.

De Citrix zaak gaf in 2020 een kick-start aan een groeiende groep onderzoekers die gingen helpen met scannen en melden, gevolgd door nog 13 onderzoeken. In 2021 heeft DIVD in totaal 18 onderzoeken verricht, waarvan KaseyaVSA in juli 2021 internationaal veel impact en publiciteit heeft gehad en Log4j in december een goed voorbeeld was van samenwerking met verschillende partners om deze crisis te lijf te gaan. Deze en andere van onze onderzoeken onderzoeken zijn ook genoemd in het rapport "Kwetsbaar door software" (16 december 2021) van de Onderzoeksraad voor de veiligheid, met als een van de hoofdconclusies:

"Alle door de Onderzoeksraad onderzochte voorvallen laten zien dat (vrijwillige) beveiligings-onderzoekers een cruciale rol spelen in de incidentbestrijding."

Ons netwerk aan samenwerkingspartners groeit. Bedrijven: Zerocopter, Secura, Google, KPN, Schuberg Philis, Cap Gemini, Connect2Trust, ESET, DTACT en NBIP. Maatschappelijke projecten: Hack in the Class, Hack_Right (politie, OM en Reclassering), Hack Talk (Tek Tok, dcypher, Stedin en gemeente Rotterdam). Overheid: we hebben een samenwerkingsovereenkomst gesloten met het NCSC en DTC zal ons vanaf 2022 steunen met subsidie. En andere non-profits, zoals ZCERT en SurfCERT. Tot slot zijn we actief lid van het Internet Abuse Overleg: AAN, waar zo'n 30 partijen abuse informatie delen.

Momenteel zijn we dit team van onderzoekers aan het uitbouwen en professionaliseren. Op termijn kunnen zij zich ook inzetten om jonge onderzoekers te begeleiden, voor zover ze dat niet nu al doen. Bij onze jonge rekruten kijken we niet naar vooropleiding of komaf, maar naar vaardigheden en potentieel. We hebben ook expliciet als doel jonge hackers aan de goede kant te houden door hen naast technische vaardigheden ook moreel bewustzijn bij te brengen en perspectief te bieden op de arbeidsmarkt. Hiervoor hebben we een Code of Conduct.

6. SWOT-ANALYSE

De interne sterke punten van de DIVD organisatie:
1. Ervaring en een groot netwerk op het gebied van (cyber)security
2. Innovatief op het gebied van (cyber) disclosures
3. Ervaring met sociaal maatschappelijk ondernemen
4. Ervaring met en het vertrouwen van deze specifieke doelgroep

De interne zwakke punten van de DIVD organisatie:
1. Klein team: wellicht snel (te) veel werk en moeite met opschalen
2. Leden doen dit veelal naast een al drukke baan
3. Mogelijke verschillen in visie, doel en de werkwijze van DIVD
4. Vasthouden van vrijwilligers
5. Omgang met gevoelige data

De externe kansen voor de DIVD organisatie zijn:
1. We voorzien in een duidelijke maatschappelijke behoefte
2. Kweekvijver voor cybersecurity-talent
3. Verbindende factor tussen bedrijven, gemeenten, overheid en onderwijsinstellingen
4. Mensen, bedrijven en overheid bieden spontaan hun hulp aan

De externe bedreigingen voor de DIVD organisatie zijn:
1. Vooroordelen ten aanzien van helpende hackers
2. Juridische claims van bedrijven die denken schade te hebben ondervonden door ons werk
3. Onvoldoende fondsgelden voor een stevige basis
4. Nog geen stevige thuisbasis
5. Nog geen goede basisvoorziening voor melden van lekken

7. FINANCIËN

DIVD is een non-profit organisatie. Het werk wordt verricht door vrijwilligers. Aanvullende fondsen zijn nodig om kostendekkend te kunnen zijn. Voor presentaties vragen we een vergoeding van €. 1.500,-, die al enkele malen is gehonoreerd en we zijn bezig een sponsorwerving strategie op te stellen en partners aan ons te binden. Daarnaast ontvangen we ook in-kind steun in de vorm van software licenties, hardware en serverruimte.

2019	**kosten**	**1.099,82**	**baten**	**3.500,-**
2020	**kosten**	**2.538,03**	**baten**	**9.700,-**
2021	**kosten**	**92.768,36**	**baten**	**103.599,55**

In 2021 hebben we extra investeringen gedaan in o.a. hardware, software, secretariële ondersteuning, professionalisering eigen omgeving (o.a. aanschaf eigen AS) en kantoorruimte.

In kas op 27-12-2021: €. 2.180,73