Jaarverslag 2020

26 maart 2021

Auteur: Chris van ’t Hof

Inhoud

1. Inleiding

Dit is het eerste Bestuursverslag en Financiële jaarverslag van stichting Dutch Institute for Vulnerability Disclosure, opgericht op 27 september 2019. Het is opgesteld door de secretaris van de stichting en op 18 maart goedgekeurd door de Raad van Toezicht.

2. Missie DIVD

Het Dutch Institute for Vulnerability Disclosure is een stichting met een tweeledige ambitie. Ten eerste het veiliger maken van de digitale wereld door het doen van onderzoek naar kwetsbaarheden in informatiesystemen, gevonden kwetsbaarheden melden bij betrokkenen en hulp bieden bij het oplossen ervan. Deze ambities hebben we in 2020 vervuld door veertien onderzoeken te starten, waarvan er aan het eind van dat jaar zeven zijn afgerond en zeven nog lopen.

Ten tweede: het verrichten van alle verdere handelingen, zoals het geven van begeleiding en trainingen van onderzoekers, ontwikkelen van onderzoeksmethodieken, publiceren over kwetsbaarheden en het organiseren van evenementen hierover. Deze ambitie hebben we vervuld door een aantal publieke lezingen, aan het woord te komen in diverse media, nieuwe, jonge onderzoekers te begeleiden, een Code of Conduct voor onderzoek op te stellen en contacten aan te gaan in het veld van cybersecurity.

3. Doelstellingen 2020

Na onze oprichting 27 september 2019, zagen we 2020 als het jaar waarin we als onderzoeksinstituut naar buiten gingen treden. In januari 2020 zijn we gestart met ons eerste grote onderzoek, naar kwetsbare Citrix servers. Dat was ook de lancering van ons Security Meldpunt, later bekend als DIVD-CSIRT (Computer Security Incident Response Team) dat eigenaren van kwetsbare servers ging melden. Dit onderzoek heeft ons instituut landelijke bekendheid gegeven. Nieuwe onderzoekers zijn vervolgens aangehaakt die of zelf een onderzoek zijn gestart of mee gingen helpen met lopende onderzoeken. We zijn ongeveer in deelnemersaantal verdubbeld.

Verder stond 2020 in het teken van het professionaliseren van onze organisatie. Met name het CSIRT heeft onder leiding van Frank Breedijk veel werk verzet in het systematiseren van onze onderzoeken, structureren van meldingen en contacten aangaan met andere partijen. Om onze bedrijfsvoering te professionaliseren hebben we ons secretariaat ondergebracht en intern nieuwe rollen gecreëerd: een FG, CISO, portfoliomanager en reporter (die een verslag schrijft van een afgesloten onderzoek). We hebben een eerste subsidie gekregen, van het SIDN Fonds en vergoedingen ontvangen voor lezingen.

4. Onderzoek 2020

In 2020 zijn veertien onderzoeken gestart, waarvan er aan het eind van het jaar zeven zijn afgerond en zeven nog lopen. In de regel scannen we de Nederlandse IP range op een bepaalde CVE (bekende kwetsbaarheid volgens de genummerde lijst van Common Vulnerabilities and Exposures) en melden we de getroffenen op generieke e-mailadressen. Bij enkele andere onderzoeken worden we gewezen op een online lijst met gelekte credentials (gebruikersnaam - wachtwoord combinaties) en melden we de getroffenen. DIVD-onderzoeken doorlopen in de regel de volgende stappen:

1. Signaal (gepubliceerde kwetsbaarheid)
2. Triage onderzoekers (capaciteit, waardering)
3. Aanmaak Slack kanaal relevante onderzoekers
4. Vooronderzoek (mogelijkheid van scannen, proportionaliteit en subsidiariteit van ingezette middelen)
5. CSIRT-casenummer aanmaak (DIVD-Year-0000X)
6. Verrijking data (contactgegevens via IP info, hostnames, certificaten)
7. Casepagina en blogpost in review en daarna geplaatst
8. Slachtoffer notificatie verzending (via info@, security@ en abuse@ en indirect via providers)
9. CSIRT inbox controle op reacties en vragen
10. Herhaling scans
11. Laatste poging aansporen tot patchen kwetsbare systemen, eventueel belactie
12. Controle (alles gepatched, contact niet mogelijk of wil niet patchen)
13. Afsluitend case report
14. Afsluiting onderzoek

4.1. Onderzoeken die in 2020 zijn gestart en afgerond

DIVD-2020-00001 - CITRIX ADC. Wereldwijd 90.000 kwetsbare servers gevonden, in Nederland 546. De Nederlandse getroffenen zijn gemeld, zowel direct als via hun providers. We hebben zes rondes gedaan van scannen en melden, waarbij het aantal snel afnam. De laatste vijf kwetsbare organisaties zijn telefonisch benaderd, waarna er nog een overbleef.

DIVD-2020-00002 - WILDCARD CERTIFICATEN CITRIX ADC. Bijvangst van het Citrix onderzoek. 461 IP-adressen gevonden en gemeld.

DIVD-2020-00003 - MICROSOFT RDP GATEWAY VULNERABLE FOR BLUEGATE RCE. 1.137 kwetsbare systemen gevonden en gemeld in vier rondes.

DIVD-2020-00004 - LIST OF MIRAI BOTNET VICTIMS PUBLISHED WITH CREDENTIALS. Eigenaren van 2.807 gebruikersnaam-wachtwoord combinaties zijn direct benaderd, in samenwerking met SURF.

DIVD-2020-00006 - SMBV3 SERVER COMPRESSION TRANSFORM HEADER MEMORY CORRUPTION. 226 kwetsbare servers gevonden, eigenaren eenmalig gemeld.

DIVD-2020-00009 - PULSE SECURE VPN ENTERPRISE LEAK. Database gevonden met 1.399 credentials van servers wereldwijd. Enkele keren gescanned en gemeld op individuele basis en onderzoek verricht naar gezondheid gekraakte wachtwoorden en gemeld op Twitter.

DIVD-2020-00010 - WPDISCUZ PLUGIN REMOTE CODE EXECUTION. Vervolgonderzoek na DIVD-2020-00008. 36 kwetsbare Nederlandse adressen gevonden en gemeld.

4.2. Onderzoeken die in 2020 zijn gestart en anno januari 2021 nog lopen

DIVD-2020-00005 - APACHE TOMCAT AJP FILE READ/INCLUSION VULNERABILITY. 773 kwetsbare servers gevonden, eigenaren in drie rondes gemeld, maar aantallen namen niet echt af. Herscan bleek lastig, waardoor we dit onderzoek gestopt zijn.

DIVD-2020-00007 - CITRIX SHAREFILE. 15 kwetsbare IP gevonden, gemeld en na herscan resterende kwetsbare organisaties telefonisch gemeld.

DIVD-2020-00008 - 313.000 WORDPRESS SITES SCANNED. Een lijst met alle Nederlandse websites die op Wordpress draaien gescand op diverse kwetsbaarheden: verouderde versie of plug-ins. Dit is doorlopend onderzoek, waarbij een specifieke kwetsbaarheid een nieuw onderzoek wordt aangemaakt.

DIVD-2020-00011 - VEMBU Vier zerodays gevonden in november, disclosure proces loopt nog.
DIVD-2020-00012 - FORTINET VPN DEVICES. 49.577 online kwetsbare devices op 34.829 IP-adressen, van 4.094 organisaties wereldwijd. 1.501 organisaties gemeld, waarvan 26 met .nl domein.

DIVD-2020-00013 - PHISHED CREDENTIALS. Lijst met 387 e-mailadressen met wachtwoorden, waarvan 187 in Nederland. 208 gemeld.

DIVD-2020-00014 - SOLARWINDS ORION. Wereldwijd 500 kwetsbare systemen gevonden en gemeld, geen in Nederland gevonden.

4.3. Methodeontwikkeling

Op divd.nl is te zien wat de specifieke kwetsbaarheid inhoudt en wat onze onderzoeken hebben opgeleverd. Daarnaast hebben we veel geleerd over vulnerability scanning en het valideren van scanresultaten. Zo hebben we bijvoorbeeld vergelijkbare scans gedaan vanaf verschillende IP-adressen om het vertekenend effect van black/whitelisting tegen te gaan. Ook zijn we ons er gaandeweg meer bewust van geworden hoe belangrijk het is scans op een systematische manier periodiek te herhalen, om zo te kijken of het aantal kwetsbare IP-adressen afneemt. We zijn ons er uiteraard van bewust dat zo'n afname niet alleen te danken is aan onze meldingen. Bottleneck blijkt vooralsnog het onderzoek af te ronden met een case report. Dat is anno januari 2021 gelukt bij slechts de eerste twee onderzoeken.

5. Samenwerking

2020 is het jaar dat DIVD bekend is geworden in de media en onder publieke en private partijen die zich bezighouden met cybersecurity. Het algemene beeld dat hieruit naar voren komt is dat ons werk wordt gewaardeerd, onze meldingen worden opgevolgd, maar men vindt het lastig ons te plaatsen omdat wij geen duidelijke doelgroep of achterban vertegenwoordigen. We scannen en melden immers heel Nederland.

Bij de oprichting van DIVD in 2019 hadden we al actief contact gezocht met het Nationaal Cyber Security Centrum omdat zij binnen Nederland een belangrijke partij zijn als het gaat om Coordinated Vulnerability Disclosure en het delen van online kwetsbaarheden. Verschillende medewerkers hebben aangegeven dat ons werk noodzakelijk is en wordt gewaardeerd, maar

zij hier niet aan kunnen bijdragen omdat dat buiten het mandaat van het centrum valt. Het NCSC richt zich namelijk alleen op Rijk en Vitaal en deelt alleen dreigingsinformatie met daartoe aangewezen partijen (CERTs en OKTTs). In de praktijk komt het erop neer dat wanneer een van onze onderzoekers een lijst met kwetsbare IP-adressen naar het NCSC stuurde, die hartelijk in ontvangst werd genomen, maar de medewerkers vervolgens niet mochten terug rapporteren met welke adressen ze aan de slag gaan en of een melding is opgevolgd. Over deze gang van zaken zijn verschillende berichten in de media verschenen en is overleg geweest op het hoogste niveau. Vooralsnog zonder resultaat.

Een samenwerkingsverband waar meldingen wel goed werden opgevolgd was met NBIP, de Stichting Nationale Beheersorganisatie Internet Providers. Bij vier van de bovengenoemde onderzoeken hebben zij lijsten met kwetsbare IP-adressen via de providers aan de eindgebruikers doorgemeld. De getroffenen kregen dan dus zowel van ons CSIRT als hun provider een melding dat zij een kwetsbaarheid op hun IP-adres moeten verhelpen.

NBIP is ook een van de partijen die op 14 februari deelnam aan de oprichting van AAN, het Anti Abuse Netwerk. Het is een spontane samenkomst van uiteenlopende partijen die informatie willen delen over online kwetsbaarheden, dreigingen en misbruik. Deelnemende organisaties zijn: NBIP, RIPE NCC, Politie, THTC, OM, EOKM, DTC, AbuseIX, Secura, AbusIO, DHPA, ISP Connect, EZK, LMIO, Connect2Trust, VVR, A2B, ECP, SIDN Fonds, SIDN, Cyberveilig Nederland, DINL en NL Digital. Het netwerk wordt geleid door Inge Bryan, die elke zes weken iedereen bijeenbrengt voor overleg, waar altijd meerdere DIVD-ers aan deelnemen. Voor ons CSIRT is dit een goed netwerk om meldingen door te zetten naar netwerkbeheerders.

Andere belangrijke samenwerkingspartner uit deze lijst zijn Connect2Trust, ECP en het SIDN Fonds. Connect2Trust is een samenwerkingsverband van in Nederland actieve bedrijven en is opgericht om onderling vertrouwde dreigingsinformatie te delen. Ook hier kunnen wij onze scanresultaten aan doorgeven en het helpt Connect2Trust om bekendheid te krijgen binnen het bedrijfsleven. ECP is bij veel ICT-initiatieven een verbindende partij, in connecties aangaan en bekendheid creëren via congressen en publicaties. Via ECP zijn we ook terechtgekomen bij ProSec, die voor ons administratieve taken oppakt.

Tot slot zijn we bijzonder trots dat we door SIDN erkend zijn als pioniersproject. We kregen daarmee een startsubsidie van 10.000 euro, begeleiding in onze opstart en bekendheid via diverse publicaties.

6. Media en optredens in 2020

Veel van onze deelnemers geven regelmatig presentaties, waarin ze ook DIVD noemen. Hier alleen de presentaties die ook uit naam van DIVD zijn gegeven:

- 28/1 “NLSecureID” van KPN Security: Matthijs Koot, Astrid Oosenbrug en Chris van ‘t Hof
- 7/2, Surfnet: Victor Gevers
- 15/2, “Hacker Hotel”. Frank Breedijk, Astrid Oosenbrug en Chris van ‘t Hof.
- 19/6 “Hack Talk: Anderhalvemetermeeting met DIVD”. Frank Breedwijk, Astrid Oosenbrug, Barry van Kampen, Brenno de Winter, Victor Gevers en Chris van ‘t Hof
- 9/10 “Hack Talk: Niet lullen maar patchen.” Frank Breedijk en Chris van ‘t Hof.
- 7/11 “Tweakers Meet-up”. Victor Gevers

DIVD en/of Security Meldpunt zijn in 2020 veel genoemd in de media. In deze artikelen komen met name Frank Breedijk en Matthijs Koot aan het woord over ons Citrix onderzoek en de rol van het NCSC in het Landelijk Dekkend Stelsel. Daarnaast enkele artikelen over Victor Gevers,

met name over zijn onderzoek in het algemeen. Berichten over zijn hack van het Twitteraccount van Donald Trump zijn niet in deze lijst opgenomen omdat hij dat niet uit naam van DIVD heeft gedaan en omdat het er erg veel zijn.

- 30/11 313.000 Nederlandse WordPress-sites gescand op kwetsbaarheden Security.nl
- 27/10 Ethisch hacken voor een veiliger internet | Cybersecurity SIDN.nl
- 05/10 Internet-Batman Victor Gevers: 'Wakker worden met een inbox vol dankjewels is verslavend' Vrij Nederland
- 30/09 Waarom beveiliging in de basis brak blijkt AG Connect
- 26/08 Nationale cyberwaakhond blaft lang niet voor iedereen FD
- 17/08 Overheid wist wie kwetsbaar was, maar liet bedrijven toch gehackt worden FD
- 15/07 Brede coalitie pakt info-gebrek misbruik internet aan Computable
- 02/07 MongoDB ransom threats step up from blackmail to full-on wiping Naked Security
- 24/02 Honderden Nederlandse servers kwetsbaar door Tomcat-lek Security.nl
- 20/02 Nederlands Security Meldpunt: 'Als zij het niet doen, doen wij het wel' AG Connect
- 04/02 'Nog altijd tientallen Citrix-servers met ernstig beveiligingslek' BNR
- 04/02 Nog zeventig Nederlandse Citrix-systemen kwetsbaar NRC
- 28/01 Expertisecentrum: Citrix-lek treft meer dan honderd zorginstellingen Nu.nl
- 26/01 Patching the Citrix ADC Bug Doesn't Mean You Weren't Hacked Bleeping Computer
- 24/01 Citrix patches vulnerability as ransomware attacks emerge By: Rob Wright TechTarget
- 22/01 'Hackers die Citrix-lek misbruiken kunnen website nabootsen' BNR
- 20/01 Citrix-paniek? Nederland werkt nuchter door, ondanks gapend vpn-gat RTLZ
- 17/01 Bedrijfsleven smeekt om hulp van overheid bij aanpak cybercriminaliteit FD
- 16/01 Duizenden bedrijven te hacken door bug in Citrix en Trump vs Apple - NOS op 3 Tech Podcast - Podcast NOS op 3 Tech Podcast
- 15/01 ICT-diensten 14 jan Honderden Nederlandse bedrijven met Citrix-servers vatbaar voor hack FD
- 15/01 Honderden servers in Nederland kwetsbaar voor hackers Trouw
- 14/01 Systeembeheerders in de zorg: Wakker worden. Citrix-servers kwetsbaar. Zorg ICT Zorgen

7. Personele en organisatorische ontwikkelingen

Het bestuur is in 2020 constant gebleven: Victor Gevers (voorzitter), Chris van 't Hof (secretaris) en Astrid Oosenbrug (penningmeester). Ook onze Raad van Toezicht: Lodewijk van Zwieten (voorzitter), Petra Oldengarm, Ronald Prins en Herbert Bos, is in 2020 ongewijzigd gebleven. Frank Breedijk fungeerde eerst als manager van zijn zelf opgerichte Security Meldpunt, dat eind van het jaar is omgedoopt tot DIVD-CSIRT, om zo de eenheid van de organisatie weer te geven. De scans werden voornamelijk uitgevoerd door Matthijs Koot en Victor Gevers. Deelnemers die vanaf de oprichting betrokken zijn vanuit een meer algemene rol zijn Raymond Bierens, Hans van de Looy en Zawadi Done.

Rondom deze stabiele kern van de organisatie zijn gaandeweg het jaar verschillende nieuwe deelnemers aangehaakt. Ons onderzoeksteam is uitgebreid met Lennaert Oudshoorn, Barry van Kampen, Sander Spierenburg, Célistine Oosting en Wietse Boonstra. Om hun werk te ondersteunen haakten aan: Willem Kutschruiter als portfolio manager, Richard Marsmeijer om meldingen telefonisch af te handelen, Brenno de Winter als Functionaris Gegevensverwerking, Fleur van Leusden als CISO, André Koot voor Identity & Access

Management, Jeroen van de Weerd als webeditor en onderzoeksrapporteur en Gerard Janssen als pr-adviseur en onderzoeksrapporteur. Om het team bijeen te houden, hielden we elke maand een gezamenlijke vergadering en afzonderlijke CSIRT-meetings.

Met deze groep hebben we ook enkele protocollen opgesteld om ons werk te professionaliseren. De belangrijkste is onze Code of Conduct om uit te dragen dat wij ons onderzoek verrichten op een verantwoorde wijze. Hieruit vloeien voort onze vrijwilligersovereenkomst, privacy statement, verwerkingsovereenkomst en security visie. Aan deze documenten wordt anno januari 2021 nog gewerkt. Verder hebben we onderzocht of we aangemerkt kunnen worden als CERT of OKTT, maar dat bleek een heilloze weg.

Daarnaast waren er tien mensen die zich wel hadden aangemeld als deelnemer van DIVD, maar om uiteenlopende redenen gaandeweg zijn afgehaakt.

Diensten die we extern hebben ingekocht zijn de kantoorondersteuning vanuit ProSec en Rechtsbijstands- en Aansprakelijkheidsverzekering via VLC & Partners.

8. Lessen geleerd

We kijken als stichting terug op een geslaagd jaar. We hebben met onze onderzoeken en de professionalisering van de ondersteuning daarvan, gezamenlijk geholpen het internet veiliger te maken. De behoefte bij bedrijven om te worden geïnformeerd over aanwezige en vastgestelde kwetsbaarheden is onverminderd hoog. Een behoefte waarin DIVD voorziet. Ons werk wordt door velen gewaardeerd en negatieve reacties op het ongevraagd scannen bleven uit. Niettemin blijft het lastig, met name voor overheidsorganisaties om ons te plaatsen, omdat we geen duidelijke doelgroep vertegenwoordigen.

Op methodologisch vlak hebben we veel geleerd: hoe te scannen, de uitkomsten te valideren en herscans te doen. Zo blijken de resultaten van scans beïnvloed te worden door vanaf welk IP-adres we scannen en of dat al of niet op een blacklist of whitelist staat. Vervolgens is het van belang dat de resultaten van een nieuwe scan vergelijkbaar zijn met de vorige, door die op eenzelfde manier uit te voeren. Echter kan de scanwijze intussen aangepast zijn op basis van voorgaande resultaten. Oftewel, de methode verandert tijdens het onderzoek. Dit willen we verder professionaliseren, zodat ons onderzoek beter te reproduceren en te verifiëren is.

Met onze groei, in aantallen onderzoeken en deelnemers, ontstond gaandeweg een gat in de communicatie tussen de onderzoekers, het CSIRT en bestuur. De onderzoekers gingen zich voornamelijk richten op hun eigen onderzoek en hielden overleggen als Meldpunt, waardoor het bestuur het zicht op de voortgang kwijtraakte. Omgekeerd deden enkele onderzoekers niet mee aan de algemene vergaderingen, waardoor nieuwe afspraken over onze werkwijzen niet bij hen over kwamen. We hebben uitgebreide discussies gehad over workflow-management systemen, maar dat liep op niets uit. Dit hebben we geprobeerd te ondervangen door op elke maandelijkse meeting een to-do lijst af te werken en het aanstellen van een portfolio manager die het overzicht bewaakt van de lopende onderzoeken, de voortgang hierin en wie als onderzoekers betrokken zijn.

Professionalisering door het opstellen van protocollen voor onze werkwijze verliep over het algemeen stroef. Onderzoekers willen toch vooral onderzoeken draaien en zitten niet te wachten op bureaucratie, ook al zien ze hier wel de noodzaak van in. We zijn een vrijwilligersorganisatie, dus we kunnen niemand ergens toe dwingen. Het enige wat we kunnen doen is elkaar helpen en het werk leuker maken, zodat het geen werk lijkt. Wat ons wel weer telkens bijeenhoudt is ons gezamenlijke doel: het internet veiliger maken.

9. Ambities 2021

Komend jaar zullen we verder gaan met de professionalisering van onze onderzoeksmethoden en werkprocessen. Om onze scanactiviteiten te professionaliseren hebben we een eigen server nodig en liefst een eigen AS (Autonomous System), dus een eigen reeks van 254 IP-adressen. Dan weten degenen die gescand worden dat wij het zijn, komen we van het blacklist/whitelist probleem af en houden we zelf als stichting controle over de scanresultaten.

Nieuwe onderzoekers kunnen zich aansluiten, maar, om alles bij elkaar te houden moeten we niet te hard groeien. Wel willen we ons gaan oriënteren op het eventueel in dienst nemen van medewerkers. Te beginnen met een financieel iemand die fondsen kan werven. Andere functies zouden kunnen zijn: operationeel manager, administratieve ondersteuning, communicatie of algemeen directeur. Ook voor de op te richten DIVD Academy denken we aan betaalde krachten, zoals een onderwijscoördinator die de lesroosters en programma's opstelt.

We zijn ons nu aan het oriënteren voor welke subsidies wij in aanmerking zouden komen en hoe wij die kunnen aanvragen. Daarnaast willen we sponsoring en giften werven. Daarvoor moeten we wel eerst de ANBI-status aanvragen.

10. Financieel verslag 2020

Kosten		Bruto	Netto	BTW
	Totaal €	**3.071**	**2.538**	**533**
01-jan	Transip	18	15	3
09-jan	Kamer van Koophandel	57	47	10
28-jan	BTW-afdracht 2019	504	504	0
05-feb	Kosten Bankpassen	60	60	0
01-apr	Bankkosten Q1	38	38	0
14-apr	BTW-afdracht Q1	285	285	0
01-jul	Bankkosten Q2	38	38	0
28-jul	VLC-verzekering	1.065	880	185
01-okt	Bankkosten Q3	38	38	0
22-okt	Pro-Sec Q4	968	800	168

Baten		Bruto	Netto	BTW
	Totaal €	**10.620**	**9.700**	**920**
11-mrt	Gift Hackerhotel	200	200	0
31-mrt	Eventive Events	1.815	1.500	315
07-nov	Tweakers Meet-up	605	500	105
30-apr	SIDN Fonds	8.000	8.000	0

Resultaat		Bruto	Netto	BTW
	Totaal €	**7.549**	**7.162**	**387**