Jaarverslag 2021

Dit is het tweede Bestuursverslag en Financiële jaarverslag van stichting Dutch Institute for Vulnerability Disclosure, opgericht op 27 september 2019. Dit verslag is opgesteld door Chris van t Hof, directeur DIVD en op 9 februari goedgekeurd door het MT en het bestuur en op 28 februari door de Raad van Toezicht. De ambities voor 2022 staan beschreven in het Jaarplan 2022.

28 februari 2022
Auteur: Chris van ’t Hof

Inhoud

1. Introductie

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 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 gebruikers 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. Elk 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.

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 een duidelijke boodschap: zet KaseyaVSA nu uit. Binnen Nederland waren er rond de honderd gebruikers van KaseyaVSA. 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 threat analysis van de actor. En inderdaad, die zaterdag werd Wietses mailserver gebruteforced vanuit de Oekraïne. Deze aanval bleef zonder al teveel 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 uur lokale tijd, stond Nederland op nul potentiële slachtoffers.

KaseyaVSA is een van de 22 onderzoeken die DIVD in 2021 heeft verricht. Bij kwetsbaarheden in Microsoft Exchange, Solarwinds Orion en in 2020 met Citrix ging het om kwetsbaarheden van vergelijkbare omvang, maar liep het minder dramatisch af en bleef ons werk buiten de media. Maar door de ransomware-aanval via KaseyaVSA kwam ons werk wel onder de aandacht van de internationale media. Voorzitter Victor Gevers en CSIRT-manager Frank Breedijk waren in de week volgend op de aanval bijna dagelijks in het nieuws, o.a. in de Verenigde Staten bij nieuwszender CBS, dagblad de Wall Street Journal en persbureau

Bloomsberg. In Nederland kreeg de zaak bekendheid door berichtgeving door 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 kleine groep Nederlandse vrijwilligers. Journalisten vroegen zich af: Waarom doet de overheid of het bedrijfsleven dat niet?

Dat doen ze ook wel, maar elk van deze partijen heeft zijn 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 totdat de aantallen potentiële slachtoffers zodanig is gedaald dat we voldoende weerbaar zijn tegen toekomstige aanvallen.

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

Kortom: DIVD heeft in 2021 laten zien dat we ertoe doen. Na een eerste jaar waarin we bouwden aan onze bekendheid en hebben ingezet op professionalisering van onze werkprocessen, hebben we dit jaar de eerste stappen gezet richting de volgende fase: Institutionalisering, waarin DIVD wordt erkent als onderzoeksinstituut.

2. Missie, visie en strategie 2021

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 2021 vervuld door 39 onderzoeken te starten, waarvan er aan het eind van dat jaar 22 zijn afgerond en 17 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. Deze ambitie hebben we vervuld door het geven van een aantal publieke lezingen, aan het woord te komen in diverse media, nieuwe, jonge onderzoekers te begeleiden, een Code of Conduct voor onderzoek te actualiseren en de samenwerking in het veld van cybersecurity te versterken.

In onze visie biedt DIVD vrijwilligers die bij willen dragen aan deze missie een omgeving waarbinnen zij hun werk kunnen verrichten, van elkaar kunnen leren en ondersteund worden door andere vrijwilligers, betaalde krachten en passende technologie. DIVD is een onafhankelijk instituut met een eigen Code of Conduct, verricht geen diensten in opdracht van derden, helpt ongevraagd en sluit daarbij niemand uit. DIVD is het Rode Kruis van het internet.

Na onze oprichting 26 september 2019, zagen we 2020 als het jaar waarin we als onderzoeksinstituut naar buiten gingen treden met diverse grote onderzoeken zoals Citrix. 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 toen ook een eerste subsidie gekregen, van het SIDN Fonds en vergoedingen ontvangen voor lezingen.

De strategische doelstelling voor 2021 was verder gaan met de professionalisering van onze onderzoeksmethoden en werkprocessen. Om het aannemen en integreren van nieuwe vrijwilligers te verbeteren wilden we ons onboardingsproces stroomlijnen. Maar om alles bij elkaar te houden, wilden we ook niet te hard groeien. Dat is gelukt.

Daarnaast wilden we ons gaan oriënteren op het eventueel in dienst nemen van medewerkers. Te beginnen met een financiële kracht die fondsen kan werven. Andere functies zouden kunnen zijn: operationeel manager, administratieve ondersteuning, communicatie of algemeen directeur. Ook voor de nog op te richten DIVD Academy dachten we aan betaalde krachten, zoals een onderwijscoördinator die de lesroosters en programma's opstelt. Dat is niet gelukt en schuift als doelstelling door naar 2022.

We wilden in 2021 ook uitzoeken voor welke subsidies DIVD in aanmerking zou komen. Eind 2021 werd ons de subsidie "Versterking cyberweerbaarheid" toegekend door het Digital Trust Centre (DTC), waarmee we 2022 kunnen starten met enkele betaalde krachten. Daarnaast wilden we ook sponsoring en giften werven. Ook dat is gelukt, zie hiervoor het financieel jaarverslag. In december hebben we ook een ANBI-status aangevraagd bij de Belastingdienst, zodat deze giften niet worden belast.

Om onze scan-activiteiten te professionaliseren wilden we een eigen server en liefst een eigen Autonomous System (AS), dus een eigen reeks van 254 IP-adressen. Dat is gelukt.

Anno januari 2022 kunnen we vaststellen dat onze doelstellingen van dit jaar deels zijn behaald. De DIVD heeft wel veel meer bereikt dan voorzien. Deze successen bespreken we hieronder per afdeling.

3. DIVD Academy

DIVD Academy is een leerschool voor het vergroten van kennis, vaardigheden en ethisch besef als ook het verbinden van jong talent dat nu buiten de boot dreigt te vallen. Daarnaast is DIVD Academy een veilige plek waar zowel beginnende als ervaren onderzoekers zich kunnen aansluiten om van elkaar te leren. De Academy is een 21ste-eeuwse niche op het gebied van IT-onderwijs, onderzoek en veiligheid.

Er zijn ook aardig wat jongeren in Nederland die erop los hacken en niet altijd weten wanneer ze de fout in gaan, ze missen vaak (logischerwijs) een ethisch kompas. In het reguliere onderwijs vinden deze jongeren vaak geen aansluiting, vallen buiten de boot en zoeken hun heil elders. Naast de maatschappelijke schade die dit teweeg brengt, is dit funest voor de toekomst van de jongeren. Een steeds groter wordende groep komt op jonge leeftijd al in aanraking met justitie. Zo eindigt een talentvolle groep jongeren in het 'verkeerde circuit', dit terwijl er juist een groot tekort is aan cybersecurity experts en ethische hackers.

De DIVD Academy is kort samengevat een vernieuwend hackers-initiatief dat zich inzet voor twee doelen: (1) Het opleiden van een nieuwe generatie hackers en (2) het verhogen van bewustzijn rondom cyberveiligheid. De DIVD Academy is een leerschool voor het vergroten van deze kennis, vaardigheden en ethisch inzicht onder jong talent. Online vinden jonge hackers die aansluiting wel, maar onder het mom van 'leuk uitproberen' of zichzelf bewijzen richten ze daar onbewust soms voor miljoenen schade aan.

DIVD leidt met haar Academy deze nieuwe generatie hackers op tot junior security researchers (vanaf level 0) en laat hun de geleerde vaardigheden in de praktijk brengen bij DIVD. De afdeling Research neemt junior security researchers aan op level 1 en laat ze daarna doorstromen naar level 2 waar ervaren onderzoekers het hele internet scannen op bekende en nieuwe, zelf-ontdekte kwetsbaarheden. De onderzoeksresultaten worden door DIVD CSIRT verwerkt tot meldingen met passende adviezen die verstuurd worden aan de eigenaren van de systemen waar de kwetsbaarheden zijn aangetroffen en het herscannen van de afdeling Research overnemen. Zo dragen zij allen bij aan een veiliger internet en een cyberweerbaar Nederland.

In 2021 heeft de DIVD Academy vooral ingezet op de opbouw en inrichting van de Academy, het inrichten van het lespakket en workshops en het aangaan van duurzame partnerschappen. Eind 2021 is besloten door het bestuur de DIVD Academy af te splitsen als een zelfstandige stichting, met een eigen bestuur en begroting, maar wel met deelname van deelnemers van het DIVD Instituut.

4. DIVD Research en CSIRT

In 2021 heeft DIVD Research 19 onderzoeken verricht. Dat is ten opzichte van 14 onderzoeken in 2020 een groei van 36%. Naast deze kwantitatieve groei zijn we vooral gegroeid in het soort onderzoek dat DIVD verricht. Naast het scannen op een bekende kwetsbaarheid, in de regel een CVE high/high, zijn er twee nieuwe onderzoekslijnen ontwikkeld: gelekte credentials en zero-days. Hiervoor is ook de Code of Conduct aangepast om ook binnen deze bredere scope verantwoordelijk te kunnen handelen.

De afdeling DIVD CSIRT heeft in 2021 in totaal 77.727 kwetsbaar bevonden IP adressen genotificeerd. Ten opzichte van 57.809 in 2020 is dat een groei van ruim 34%. Op het moment van schrijven zijn nog niet alle cases uit 2021 geheel afgerond, dus het werkelijke aantal notificaties ligt nog iets hoger. Ook hier zit de groei niet zozeer in de kwantiteit, maar in de kwaliteit. Onze meldingen werden namelijk, meer dan het jaar hiervoor, ook doorgezet via een groeiende groep Trusted Information Sharing Partners.

Van elke lopende case is een beschrijving en blog te volgen op csirt.divd.nl. De afgeronde cases hebben elk een report dat is terug te lezen op divd.nl/reports. Hieronder volgt een overzicht van 2021.

CVE scans

DIVD-2021-00001 - MICROSOFT ON-PREM EXCHANGE SERVERS
DIVD-2021-00005 - PULSE SECURE PREAUTH RCE
DIVD-2021-00010 - VCENTER SERVER PREAUTH RCE
DIVD-2021-00011 - KASEYA VSA LIMITED DISCLOSURE
DIVD-2021-00017 - SOLARWINDS N-ABLE N-CENTRAL AGENT VULNERABILITIES
DIVD-2021-00022 - EXCHANGE PROXYSHELL AND PROXYORACLE

DIVD-2021-00026 - OMIGOD: MICROSOFT OPEN MANAGEMENT INTERFACE RCE
DIVD-2021-00027 - APACHE HTTP 2.4.49 PATH TRAVERSAL AND FILE DISCLOSURE
DIVD-2021-00030 - GITLAB UNAUTHENTICATED RCE FLAW
DIVD-2021-00033 - SITES WITH POTENTIAL SQL-INJECTION
DIVD-2021-00036 - VMWARE VCENTER SERVER ARBITRARY FILE READ VULNERABILITY
DIVD-2021-00038 - APACHE LOG4J
DIVD-2021-00039 - HP ILO

Leaked Credentials
DIVD-2021-00003 - FACEBOOK LEAK
DIVD-2021-00004 - GELEKTE PHISHING GEGEVENS / LEAKED PHISHING CREDENTIALS
DIVD-2021-00012 - WAREHOUSE BOTNET

Zero-day research
DIVD-2021-00002 - KASEYA
DIVD-2021-00006 - SMARTERMAIL
DIVD-2021-00007 - XSS AND RCE IN EA ORIGIN GAME LAUNCHER
DIVD-2021-00014 - UNITRENDS
DIVD-2021-00017 - NABLE / SOLARWINDS
DIVD-2021-00021 - QLICK SENSE
DIVD-2021-00028 - ATERA
DIVD 2021-00031 - BELEL
DIVD 2021-00037 - ITARIAN

In 2021 zijn negen zero-day cases gedraaid vanuit Research. Hiervan zijn er vijf gepubliceerd op csirt.divd.nl. Door de onderzoekers zijn er afgelopen jaar 92 individuele RD meldingen gedaan die geen casenummer hebben. Het research team is nu uitgegroeid tot een volledige afdeling bestaande uit drie teams.

5. DIVD Instituut

Naast de uitvoerende afdelingen Research en CSIRT ligt de ondersteuning van deze afdelingen bij DIVD Instituut. De financiën werden gedaan door de penningmeester en de administratieve taken door de secretaris en voorzitter. Daar is halverwege het jaar de functie project management ondersteuning bijgekomen, uitgevoerd door Nikola Diete. Met name de onboarding van nieuwe deelnemers en het bijhouden van de deelnemersadministratie heeft ze voortvarend opgepakt. In december is LunaVia aan de slag gegaan om project management ondersteuning en financieel management op te pakken voor DIVD.

Op 1 januari 2022 telt DIVD 76 deelnemers: zeven bij Academy, dertien bij CSIRT, achttien bij Instituut, acht bij Operations en dertig bij Research. Van deze deelnemers zijn er negentien pas in december 2021 aangenomen. Die moeten nog integreren om volledig aan de slag te kunnen. De verwachting is dat een aantal nog zal afvallen omdat het werk hen toch niet past. Deelnemers van wie we al maanden niets meer vernomen hebben zijn in december 2021 benaderd. Hierdoor zijn er een paar afgevallen en uiteindelijk nog zo'n 18 die nauwelijks actief zijn en later weer benaderd worden.

Communications was in 2021 nog geen afdeling, maar een reeks taken die vooral werden opgepakt door wie zich daar op dat moment toe geroepen voelde. Communicatie met de media werd per onderzoek opgepakt door de case lead. Corporate communicatie over het instituut werd opgepakt door het bestuur en onderzoekers. Cases werden meer dan vorig jaar goed samengevat in een afsluitend report door Gerard Janssen en Jeroen van de Weerd. Om communciatie goed te borgen in de organisatie begint begin 2022 een Head of Communications.

In 2021 heeft DIVD ook een Privacy Officer en FG aangesteld, maar die functies zijn niet echt van de grond gekomen. De functie van CISO wel. Fleur van Leusden heeft dit voortvarend opgepakt door Security plannen op te stellen en die af te stemmen met bestuur en deelnemers, maar vooral ook door betrokken te zijn bij lopende zaken en advies op maat te geven. Januari 2022 is een nieuwe Privacy Officer aan de slag gegaan.

Operations (bij andere organisaties meestal aangeduid als afdeling IT) is in 2021 een eigen afdeling geworden en wordt geleid door Casper Kuijper. Samen met de System Engineers van Schuberg Phillis heeft hij ervoor gezorgd dat DIVD een eigen Autonomous System (AS) heeft. Hiervoor is rackruimte vrij gemaakt, zijn routers, firewalls en servers geplaatst en ingericht en is de basis gelegd voor de doorontwikkeling van onze eigen scan en research infrastructuur. AS50559 wordt ontsloten vanuit het datacenter van Schuberg Phillis en scant vanaf de IPv4 range 194.5.73.0 - 194.5.73.255. Zo 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.

Daarnaast is hard gewerkt aan het ontwerp voor onze kantoorautomatisering. Op deze omgeving zal onder andere ons IAM platform, SIEM, Datalake en interne communicatie worden ontsloten. Dit werd bij DIVD in 2021 door verschillende deelnemers opgepakt. Met name de Slack omgeving voor dagelijkse communicatie en Trello als To do bord, die zijn opgezet door de voorzitter Victor Gevers, werkten goed om alle activiteiten op elkaar af te stemmen. Elke DIVD deelnemer kan zo binnen verschillende open themakanalen communiceren en taken bijhouden. Voor de onderzoekers en bestuur zijn er besloten kanalen. Binnen DIVD wordt vrijwel niet gemaild. Verder hebben CISO Fleur van Leusden en penningmeester Astrid Oosenbrug een intranet opgezet met onder andere documentatie voor nieuwkomers.

Het bestuur is in 2021 constant gebleven: Victor Gevers (voorzitter), Chris van ‘t Hof (secretaris) en Astrid Oosenbrug (penningmeester). Vanaf 1 januari 2022 wordt Victor Gevers Head of Research en Chris van ‘t Hof Managing Director. Zij treden uit het bestuur. Onze Raad van Toezicht is naast Lodewijk van Zwieten (voorzitter), Petra Oldengarm, Ronald Prins en Herbert Bos, uitgebreid met een vertegenwoordiger uit de hackerswereld: Chantal Stekelenburg.

6. Samenwerking

DIVD is in essentie een samenwerkingsverband van security-onderzoekers. Onderzoekers die ook in hun eigen tijd zoeken naar kwetsbaarheden en dit melden bij degenen die deze kwetsbaarheden kunnen verhelpen. Vaak zijn ze al werkzaam bij een securitybedrijf, maar kunnen of mogen geen meldingen doen namens hun werkgever omdat de getroffene geen klant is. Bij DIVD kunnen ze dat wel doen.

Deze individuele onderzoekers vinden vaak dezelfde kwetsbaarheden, wat leidt tot dubbel werk en verwarring bij ontvangers van meldingen. DIVD verzorgt voor hen een samenwerkingsplatform om hun bevindingen te vergelijken, eventuele onkosten te vergoeden, gezamenlijk naar buiten te treden, te leren van elkaars werkwijze en bovenal ook veel plezier te beleven aan het vervullen van deze maatschappelijke taak. DIVD is aanspreekpunt voor getroffen organisaties en partijen die meehelpen kwetsbaarheden te fixen, zodat dubbel werk wordt voorkomen en hiaten worden opgevuld.

De werkgevers van onze deelnemers zijn trots dat ook hun experts belangeloos bijdragen aan een veiliger internet voor iedereen en staan toe dat zij hier veel tijd in steken, ook tijdens werktijd. DIVD ziet hen dan ook als sponsoring partners in de samenwerking. Daarnaast zijn er steeds meer sponsoring partners die DIVD steunen met hardware, software licenties, diensten of gewoon giften via onze donatiepagina.

Een derde vorm van partnership zijn de zogeheten Trusted Information Sharing Partners. DIVD stuurt in eerste instantie meldingen van gevonden kwetsbaarheden direct aan de gevonden potentiële slachtoffers via hun info@, security@ en abuse@ mailadressen maar vervolgens nogmaals via deze TISPs. Enkele zijn: NBIP voor providers, Z-CERT 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 en NCSC voor Rijk en Vitaal.

Internationaal werken we samen met CISA US, NCSC UK, Shadowserver, Have I Been Pwned en veel onafhankelijke onderzoekers. Aan wie we onze meldingen doorzetten hangt af van het soort onderzoek en de potentiële slachtoffers.

Op 27 september 2021 lanceerde een aantal private partijen van het Anti Abuse Netwerk, een coalitie van 30 organisaties, het plan om vanuit het bedrijfsleven een Clearinghouse op te zetten om meldingen door te geven aan getroffenen. Eind 2021 werd besloten dat hiervoor een stichting wordt opgericht onder de naam Nederlands Security Meldpunt, dat 14 februari 2022 wordt gelanceerd. Connect2Trust, NBIP, DIVD, AMS-IX en SurfCERT. nemen hierin het voortouw.

7. Media en optredens in 2021

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

- 25 januari Astrid Oosenbrug "Niet lullen, maar patchen" KPN SecureID
- 8 juli Lennaert Oudshoorn, "NOS op 3 Tech Podcast"
- 20 augustus. Chris van 't Hof, Lennaert Oudshoorn, Wietse Boonstra, Victor Gevers en Astrid Oosenbrug: "Hack Talk 18: scan, meld, fix" Club Worm, Rotterdam.
- 1 september Lennaert Oudshoorn: "BNR'S Big Five" radio interview
- 2 september Frank Breedijk: "How we scan and report vulnerabilities on the internet" NLNOG Day 2021
- 7 september, Victor Gevers en Raymond bierens "Keynote 600 minutes cyber Security"
- 17 september, Chris van 't Hof, Tom Wolters, Casper Kuijper, Fleur van Leusden, Jan Los en Joris de Vis "Hack Talk 19: gelekt…" Club Worm, Rotterdam.
- 27 september Chris van 't Hof, Lennaert Oudshoorn en Frank Breedijk: "Hack the Hague" Gemeentehuis Den Haag

- 12 oktober Lennaert Oudshoorn en Chris van ‘t Hof: “Hoe het DIVD jouw organisatie scant en kwetsbaarheden meldt“ OVerheidsbrede Cyberoefening, Ministerie Binnenlandse Zaken.
- 28 oktober Frank Breedijk “Fireside chat” for Akamai partner Sumit 2021
- 3 november Frank Breedijk “Hub Sessie Cybersecurity” Management Events (TBX)

DIVD is in 2021 veel genoemd in de nationale en internationale media.

25-1-202	ZDnet	Dutch COVID-19 patient data sold on the criminal underground
6-3-202	Vice	We vroegen een hacker wat hij stemt en wat de beste cyberpartijen zijn
9-3-202	Financieel Dagblad	Nederlandse bedrijven wacht nieuwe aanvalsgolf met gijzelsoftware
9-3-202	The Record	More than 46,000 Exchange servers still unpatched
11-3-202	AG Connect	DIVD: Nederland patcht Exchange-gat relatief snel
11-3-202	Bleeping computer	CISA: No federal civilian agency hacked in Exchange attacks, so far
12-3-202	AG Connect	Iedere twee uur verdubbeling in Exchange-aanvalspogingen
12-3-202	Heise	Exchange-Hack: Welche Maßnahmen Unternehmen jetzt ergreifen müssen
17-3-202	AG Connect	Duizenden extra Exchange-servers kwetsbaar
20-3-202	AG Connect	Microsoft Defender Antivirus schermt Exchange-gat automatisch af
25-3-202	Volkskrant	In het Twitteraccount van president Donald Trump: de hack die het Witte Huis glashard ontkende
2-4-202	Security	NCSC mag dreigingsinformatie met Connect2Trust gaan delen
10-5-202	Computable	Hulde voor de 'helpende hacker'
11-5-202	Security.nl	Kwetsbaarheid in Vembu BDR Suite maakt remote code execution mogelijk
4-7-202	NOS	Nederlandse ethische hackers probeerden ransomware-aanval te voorkomen'
4-7-202	VN	Nederlandse hackers probeerden aanval met gijzelsoftware te voorkomen
4-7-202	BleepingComputer	Kaseya was fixing zero-day just as REvil ransomware sprung their attack
4-7-202	The Record	Kaseya zero-day involved in ransomware attack, patches coming
4-7-202	Bloomsberg	Mass Ransomware Hack Used IT Software Flaw, Researchers Say
4-7-202	Volkskrant	Zelfs de supermarkt is doelwit van Russische hackers: ‘Een van de ingrijpendste aanvallen ooit’
4-7-202	Eindhovens Dagblad	Op een haar na voorkwamen Nederlandse vrijwilligers wereldwijde cyberaanval van beruchte Russische criminelen op duizenden bedrijven

5-7-202	The Hacker News	REvil Used 0-Day in Kaseya Ransomware Attack, Demands $70 Million Ransom
5-7-202	Fortune	Hackers in Saturday's 'sophisticated' ransomware attack targeted flaw in IT management software
5-7-202	Gigazine	IT管理サービス「Kaseya」を標的にしたランサムウェアの大規模攻撃で多数の企業に間接的影響
5-7-202	NL Times	Dutch team was a day away from saving Kaseya when hackers struck; Ransomware demand hits $70 million
5-7-202	AGconnect	Ransomwaregat in Kaseya was al ontdekt en gemeld, door DIVD
5-7-202	Computable	Massale ransomware-aanval via Kaseya
5-7-202	BN de Stem	Op een haar na voorkwamen Nederlandse vrijwilligers wereldwijde cyberaanval van beruchte Russische criminelen op duizenden bedrijven
5-7-202	Trouw	Nederlandse vrijwilligers hadden de wereldwijde ransomware-aanval bijna voorkomen
5-7-202	SANS Daily	Special Podcast: Kaseya VSA REvil Ransomware Incident
7-7-202	Wall Street Journal	Software Firm at Center of Ransomware Attack Was Warned of Cyber Flaw in April
7-7-202	Wired	How REvil Ransomware Took Out Thousands of Business at Once
10-7-202	HSD	The Dutch Institute for Vulnerability Disclosure (DIVD) is Doing Good for BV Nederland
3-8-202	Financieel Dagblad	Was de megahack via Kaseya te voorkomen?
15-12-202	AG Connect	Nederlandse Log4Shell-scantool dankzij DIVD en DTACT
24-12-202	AG Connect	DIVD, cybersecurity vanuit maatschappelijke betrokkenheid

Financieel verslag 2021

Ten opzicht van vorig jaar zijn de inkomsten en uitgaven vertienvoudigd. Beide jaren hebben een sluitende begroting.

	2020	2021
Inkomsten		
Inkomsten uit eigen fondsenwerving	€ 8.000,00	€ 2.000,00
Inkomsten uit particuliere giften	€ -	€ 5.618,21
Inkomsten giften organisaties	€ 200,00	€ 91.044,34
Inkomsten uit subsidies	€ -	€ -
Inkomsten uit lezingen	€ 2.420,00	€ 2.315,00
Overige inkomsten	€ -	€ 3.000,00
Totale inkomsten	€ 10.620,00	€ 103.977,55
Bestedingen		
Bankkosten	€ 173,48	€ 347,01
BTW afdracht	€ 789,00	€ 105,00
Internet en website	€ 18,74	€ 3.919,08
Kantoorkosten	€ -	€ 4.866,06
Kosten beheer en administratie	€ 968,00	€ 8.232,00
Advieskosten	€ -	€ 18.305,32
Uitkering vrijwilligers	€ -	€ 2.000,00
Representatie Kosten	€ -	€ 2.029,17
Verzekering	€ 1.064,80	€ -
Reservering Opbouw Fonds/CSIRT		€ 50.000,00
Algemene kosten	€ 57,00	€ 12,35
Voorschot loon	€ -	€ 6.453,66
Licentie kosten	€ -	€ 326,05
Liquide middelen	€ 7.548,98	€ 7.381,85
Totale kosten/bestedingen	€ 10.620,00	€ 103.977,55