Jaarverslag 2022

Datum	15 maart 2023
Auteur	Chris van 't Hof
Versie	0.9. Tekst goedgekeurd door bestuur op 15 maart, financieel verslag volgt nog

Samenvatting

DIVD is in 2022 flink gegroeid. Niet zozeer in aantallen vrijwilligers (van 80 naar 96), maar vooral in de hoeveel werk dat is verricht: van 24 naar 40 onderzoeken, van 98,757 naar 185,942 notificaties en van 0 naar 8 deeltijd betaalde krachten. Daarmee is ook de jaarlijkse omzet en de impact van en de erkenning voor het werk van DIVD dit jaar groter geworden.

1. Het instituut

DIVD heeft als missie het veiliger maken van de digitale wereld door het doen van onderzoek naar digitale kwetsbaarheden in informatiesystemen, gevonden digitale kwetsbaarheden melden bij betrokkenen en hulp bieden bij het oplossen ervan. 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.

Hieruit volgt de strategie dat we zoveel mogelijk capabele experts aan ons binden en die ondersteunen vanuit de afdelingen Research en CSIRT. In de praktijk zijn er bij Research drie onderzoekslijnen: scannen en melden op bekende kwetsbaarheden (CVEs), onderzoek naar nieuwe kwetsbaarheden (Zero-days) en gelekte credentials (gebruikersnaam, wachtwoord combinaties of bronnen die gewoon open online staan). De bevindingen van Research worden gemeld naar potentiële slachtoffers van kwetsbaarheden via onze afdeling CSIRT. Dit gaat direct via mail en indirect via onze Trusted Information Sharing Partners van DIVD en binnen Nederland steeds meer via het Nederlandse Security Meldpunt. Dit is het kernproces waarin onze missie en visie samenkomen.

Dit kernproces wordt vervolgens ondersteund door de afdelingen IT services, HRM, Communications, Finance en Governance, Risk & Compliance. Die afdelingen groeien mee met de groei van het aantal vrijwilligers. Directeur en afdelingshoofden waren in 2022 deels betaalde functies omdat zij het werk oppakken dat door vrijwilligers blijft liggen en zij ook een zekere resultaatverplichting hebben.

Vanaf 1 januari 2022 waren er deels betaalde functies voor de directeur (0,4 fte), Head of Research (0,4 fte), Head of CSIRT (0,2 fte) en administratie (0,2 fte, uitbesteed aan LunaVia). In werkelijkheid lag het aantal gewerkte uren veel hoger, vandaar deels betaalde

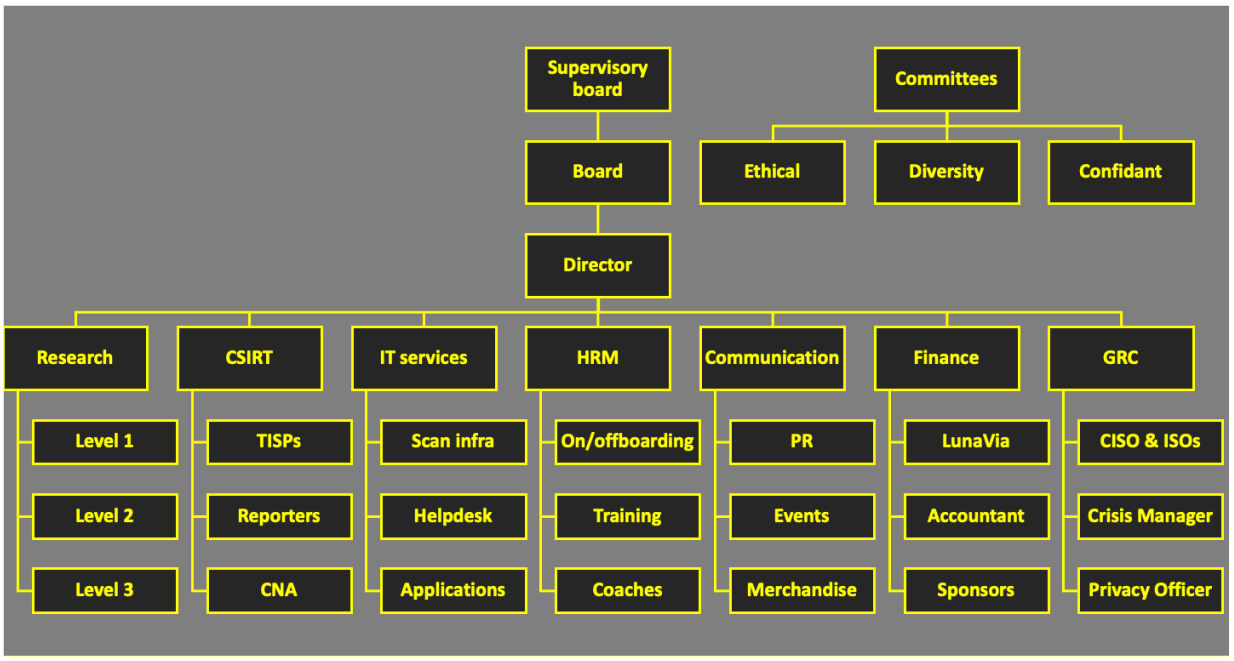
functies. Deze werden gefinancierd uit een subsidie van DTC. Vanaf 1 april waren er ook deels betaalde functies voor de afdelingshoofden HRM, Operations (ICT) en Communication. Elk 0,2 fte en een crisismanager voor 0,1 fte. Deze werden gefinancierd uit giften van twee filantropische fondsen: Adessium en Limelight.

Het kernproces bleef uitgevoerd worden door de vrijwilligers. Dit om de missie puur te houden. Zo werkt dat ook bij andere vrijwilligersorganisaties zoals het Rode Kruis, Bits of Freedom of de brandweer. Je wordt vrijwilliger om een maatschappelijk doel te dienen en voor je persoonlijke ontwikkeling.

Dat het onderzoek wordt verricht door vrijwilligers spreekt ook in ons voordeel in het geval iemand niet gediend is van het ongevraagd scannen en melden van kwetsbaarheden en aangifte doet van computervredebreuk of het schenden van de AVG. In diverse rechtszaken binnen de Nederlandse jurisprudentie is dit namelijk een belangrijk criterium geweest de gedaagde vrij te pleiten van strafvervolging. Daar is ook onze Code of Conduct op gebaseerd. Zodra een onderzoeker betaald wordt, kan discussie ontstaan over dat maatschappelijk belang, wat we hiermee voorkomen.

2. Ontwikkelingen per afdeling

DIVD is in 2022 gegroeid van 80 naar 96 mensen: 5 in het bestuur, 5 in de Raad van Toezicht, 1 directeur met 3 externen voor kantoorondersteuning, 38 bij Research, 11 bij CSIRT, 15 bij IT Services, 10 bij Governance Risk & Compliance, 2 bij Communicatie, 2 bij HRM en 3 in de ethische commissie. Die groei was lager dan verwacht (120) omdat er ook veel vrijwilligers tijdens het jaar afvielen, of gewoon niet op gang zijn gekomen. We zijn ook strenger geworden op passieve vrijwilligers. We hebben geprobeerd die actiever te betrekken en als ze na diverse verzoeken nog niet aan de slag zijn gegaan, hebben we ze gevraagd de organisatie te verlaten. Daarnaast zijn er ook vrijwilligers van DIVD overgestapt naar een van de andere stichtingen binnen DIVD.family.



2.1. Bestuur en Raad van Toezicht

Het bestuur van DIVD bestaat op 1 januari 2023 uit vijf personen: voorzitter, secretaris, penningmeester en twee algemeen bestuursleden. De bestuursleden zijn voor 5 jaar benoemd en kunnen tussentijds van functie wijzigen. RvT telt ook vijf leden. Op 26 september 2022 verliep de drie-jaarlijkse termijn van vier van de vijf leden. Die zijn op eigen verzoek allen herbenoemd, een vijfde lid dat begin 2022 was toegetreden heeft de rol van secretaris op zich genomen.

2.2. Directie

DIVD heeft sinds 1 januari 2022 een directeur: Chris van 't Hof. Hij geeft leiding aan het MT en rapporteert aan het bestuur. Hij leidt de wekelijkse MT-bijeenkomsten en wordt daarbij ondersteund door een directiesecretaris die de agenda opstelt en notuleert. De directeur gaat ook over de fondsenwerving en financiën en wordt hierin bijgestaan door een boekhouder met wie hij elke twee weken alle inkomsten en uitgaven doorneemt en dat elke vier weken doet met de penningmeester erbij, ter controle. Voor de jaarrekening heeft hij een controller en over 2022 volgt ook een accountantscontrole. Dit is ook verplicht vanwege de subsidies die DIVD ontvangt.

2.3. Research

De afdeling Research groeide van 30 naar 38 medewerkers met Victor Gevers vanaf 1 januari als Head of Research. In 2022 zijn 40 onderzoeken afgerond. Vergeleken met de 24 in 2021 is dat een flinke groei groei, al moet daar wel bij gezegd worden dat onderzoeken onderling moeilijk te vergelijken zijn. Wel kan gesteld worden dat er per onderzoeker meer werk is verricht.

Onderzoeksresultaten

We onderscheiden drie onderzoekslijnen. De eerste is het scannen op bekend gemaakt kwetsbaarheden, de Common Vulnerabilities and Exposures, CVEs. De lijsten met IP-adressen waar een kwetsbaarheid is gevonden, wordt doorgestuurd naar CSIRT om die te melden. De tweede onderzoekslijn bestaat uit het vinden en melden van gelekte credentials (gebruikersnamen en wachtwoorden) en bronnen die open staan. De derde lijn is het onderzoek naar nieuwe kwetsbaarheden, oftewel Zero-days, om die te melden bij de vendoren, erop te scannen en melden. In bijlage 1 staat een lijst van alle onderzoeken die in 2022 zijn verricht.

De onderzoekers

Binnen de afdeling Research is in 2022 intensiever ingezet op het goed begeleiden van nieuwe onderzoekers om meer onderzoek gedaan te krijgen en goede onderzoekers vast te houden. De een komt binnen met onderzoekservaring en wil leren scannen, de ander komt binnen met een eigen onderzoek dat wordt opgenomen in ons portfolio en opgeschaald met andere onderzoekers.

Onderzoekers die zich aanmelden ondergaan eerst een screening, ondertekenen vervolgens een vrijwilligersovereenkomst en daarmee de Code of Conduct. Voor dit level is minimaal een Essential Security Certificaat nodig van Certified Secure. Vervolgens starten ze met een praktijkopdracht. Als ze dit goed doorlopen hebben treden ze toe als Researcher level 1 en kunnen ze een case oppakken die zich al in het openbare domein bevindt, bijvoorbeeld data gelekt op social media. Hebben ze een eerste case goed afgesloten,kunnen ze zich aanmelden voor Research level 2, waar de meer spannende data wordt verwerkt: grote scans, maar ook gelekte credentials en Zero-days.

Voor Research level 2 is minimaal 15 jaar ervaring of een OCSP van Offensive Security of CSC Security Specialist van Certified Secure nodig. Daarnaast moet de onderzoeker op zijn minst een level 1 case geheel zelfstandig of een grotere level 1 case als case lead hebben gedraaid. Voor onderzoekers die korter een jaar level 1 zijn of redelijk

nieuw zijn in ons netwerk, vindt er ook een screening plaats die afgenomen wordt door Head of Research.

Onderzoekers werken altijd in teams, onder leiding van een case lead, zodat ze hulp krijgen, maar ook gecontroleerd worden. Toegang tot data en onderzoeken is case based en wordt beheerd door de case lead. Ze kunnen dus alleen bij hun onderzoeken, niet bij alle. De resultaten van onderzoek bestaan in de regel uit een lijst IP-adressen waar een specifieke kwetsbaarheid is gevonden. Die gaat naar de afdeling CSIRT (Computer Security Incident Response Team) die de potentiële slachtoffers meldt dat ze kwetsbaar zijn, met advies over hoe dat op te lossen. De scans worden periodiek herhaald om de lijst te actualiseren.

2.4. CSIRT

De kwetsbaarheden die door de afdeling Research zijn gevonden, resulteerden bij de afdeling CSIRT in 185,942 notificaties. Dat is vergeleken met de 98,757 in 2021 bijna een verdubbeling. Daarnaast heeft CSIRT er nieuwe taken bij gekregen als CVE Numbering Authority en relatiebeheer met doordelers van onze meldingen. Bij aanvang van 2022 gingen we er vanuit dat de afdeling CSIRT in omvang zou meegroeien met research. Dat is niet gebeurt. Op 1 januari 2022 telde deze afdeling 13 medewerkers, op 1 januari 2023 slechts 11. Niettemin heeft deze afdeling goed gefunctioneerd en zijn er geen noemenswaardige vertragingen geweest in het meldproces. Dat kan gelegen zijn in het feit dat de vrijwilligers zich niet echt aan het onderscheid tussen de afdelingen houden en researchers ook regelmatig het meldingsproces op zich nemen. Maar het komt vooral ook doordat deze afdeling onder het nieuwe hoofd CSIRT Lennaert Oudshoorn de werkprocessen heeft geprofessionaliseerd.

Case management en verbeteren meldingen

In 2022 zijn veel processen bij CSIRT gestandaardiseerd en gedocumenteerd, waardoor overdracht van werk werd vergemakkelijkt.. Zo is er een toolkit ontwikkeld die helpt werkzaamheden die voor elke case herhaalt worden te automatiseren. Om meldingen op de juiste plek te krijgen zijn nationaal en internationaal verschillende initiatieven opgezet. Om maximaal gebruik te maken van deze kanalen nam de afdeling CSIRT ook een deel operationeel relatiebeheer op zich met partijen waar wij meldingen naar doorzetten. Voorbeelden hiervan zijn DTC, NCSC, Z-CERT en SURF. Met de komst van het Security

Meldpunt[1] in Nederland is het doordelen aan deze en andere partijen efficiënter verlopen en hadden onze meldingen meer impact omdat getroffenen die krijgen van een partij die ze al kennen.

Inwerken nieuwe CSIRT-ers

In 2022 is meerdere malen de CSIRT inwerk training gegeven. Deze training is verplicht voor alle CSIRT vrijwilligers en optioneel voor anderen. Deze training is inmiddels door 35 van de 52 mensen die hiervoor zijn aangemeld gevolgd.

Registratie CVEs

In 2022 is DIVD een CVE Numbering Authority geworden. We kunnen zelf nieuwe kwetsbaarheden registreren in het online Mitre overzicht van Common Vulnerabilities and Exposures. Deze taak is belegd bij het CSIRT en wordt uitgevoerd door het CNA-Administrators team. Om deze werkzaamheden uit te kunnen voeren is er een verplichte training, momenteel hebben drie CSIRT deelnemers deze training afgerond. In 2022 zijn in totaal 27 CVEs door DIVD geregistreerd, waarvan er 8 nog gereserveerd staan en niet gepubliceerd zijn.

2.5. IT services

De afdeling IT services is in 2022 gegroeid van 8 naar 15 vrijwilligers en wordt geleid door Head of IT services Casper Kuiper. De afdeling bestaat uit verschillende kennisgroepen namelijk Helpdesk, Linux, Networking, Virtualization, IAM, Automation, Crypto en Security. Elke kennisgroep heeft een eigen Team Lead. Die is vraagbaak voor de overige leden van de kennisgroep en verantwoordelijk voor het toewijzen van taken aan de teamleden. DIVD vrijwilligers kunnen lid zijn van meerdere kennisgroepen als de kennis van het individuele lid toereikend is.

Vooralsnog gebruikt DIVD voor de kantoorautomatisering (KA) voornamelijk SaaS diensten en krijgt DIVD steeds meer soft- en hardware in-kind van sponsoren. Maar ook dat moet gekoppeld en onderhouden worden. DIVD een eigen AS (50559) met eigen routers, firewalls, switches en servers. Deze omgeving wordt vooral gebruikt voor het scannen van

[1] Security Meldpunt is geen stichting die direct gelieerd is aan DIVD. Er zijn wel DIVD-ers bij aangesloten en er zit iemand van DIVD in het huidige bestuur.

het hele internet op kwetsbaarheden en het verwerken van de resultaten en heeft heel 2022 gefunctioneerd zonder enige noemenswaardige incidenten.

Onderdeel van IT-services is ook het development-team. Dat is uitgegroeid tot vijf mensen van diverse disciplines. Het doel van het development-team is onderzoek naar en ontwikkeling van software die de dagelijkse werkzaamheden van de verschillende DIVD-afdelingen kunnen ondersteunen. Het development-team heeft gedurende 2022 onder andere een bijdrage geleverd bij het uitzoeken van een geschikt ticketsysteem, software gemaakt om de zogenaamde security.txt-bestanden gestructureerd te kunnen lezen en om het website-register van de Rijksoverheid uit te kunnen lezen. In het laatste kwartaal zijn er stappen gezet om automatisering met betrekking tot het CSIRT te gaan ontwikkelen. Hierbij willen we een architectuur opzetten waardoor researchers gemakkelijker en sneller hun werk kunnen uitvoeren.

Het development-team werkt op basis van verzoeken vanuit de DIVD-organisatie. Hierbij valt te denken aan verzoeken voor kleine stukjes software die de dagelijkse werkzaamheden kunnen ondersteunen. Mochten er afdelingen binnen de DIVD zijn die dat nodig hebben, dan kunnen ze zich melden in het #development-kanaal in Slack, of een ticket aanmaken via de Helpdesk. Het development-team houdt dan, gegeven de bezetting en vrijwillige basis, contact met de afdeling over de haalbaarheid van het verzoek en de verdere voortgang.

2.6. HRM

DIVD is in 1 april 2022 gestart met een HRM afdeling die zorg draagt voor het onboarden van nieuwe vrijwilligers, bijeenbrengen van vraag- en aanbod in trainingen en persoonlijk welzijn. Door personele onderbezetting zijn die taken onvoldoende ingevuld. In feite betrof het een enkel afdelingshoofd, Jan Los, die hier en daar werd bijgestaan door een wisselende groep vrijwilligers en afdelingshoofden. De coaching structuur, met POP gesprekken werkt niet bij alle vrijwilligers goed en training werd redelijk ad hoc ingevuld op eigen initiatief van de vrijwilligers. De afdeling is er wel in geslaagd een HRM systeem op te zetten waardoor afdelingshoofden een veel beter overzicht hebben van de organisatie.

Mede daardoor is ook het onboardingsproces bij DIVD verbeterd. Aspirant vrijwilligers melden zich veelal zelf aan via een bekende DIVD-er of reageren op een oproep op divd.nl. Vervolgens wordt een Trello kaart voor hen aangemaakt en melden zich daar

DIVD-ers die het sollicitatiegesprek willen voeren. Bij geschiktheid volgt de screening, wordt een vrijwilligersovereenkomst getekend, start de begeleiding binnen de afdeling en stelt de nieuwkomer zich voor op Slack en tijdens de vergadering en krijgen ze het DIVD Handboek met tips om aan de slag te gaan. Het afdelingshoofd is in principe ook begeleider, maar het kan zijn dat een nieuwe DIVD-er na onboarding toch naar een andere afdeling gaat.

DIVD heeft inmiddels ook een samenwerkingsverband met de Security Academy. Enkele DIVD-ers hebben daar de trainingen Certified Information Security Manager en Certified Information Systems Auditor gedaan.

Nieuw dit jaar was de vrijwilligers tevredenheidsenquête die in januari 2023 werd gehouden over het jaar 2022. Voor een zeer ruime meerderheid van de vrijwilligers zijn de organisatiedoelen duidelijk, weten ze bij wie ze terecht kunnen voor hulp, zijn de meetings goed, waarderen ze het MT en bestuur en zijn ze bereid kunnen kennis en vaardigheden aan anderen over te dragen. De onboarding werd door de meesten ervaren als 'neutraal' en het inwerken voor verbetering vatbaar.

Wat de vrijwilligers vooral bindt aan DIVD is dat ze samen met gelijkgestemden onze missie vervullen: het internet veiliger kunnen maken. Op de vraag "Kun je jezelf zijn zonder dat je je veroordeeld voelt?" antwoordde iedereen 'ja'. Daar waar de vrijwilligers verbeterpunten zien stemmen die grotendeels overeen met wat het management zelf ziet: organisatie van de team meetings, samenwerking tussen de teams, en de onboarding en het inwerken nieuwe vrijwilligers.

2.7. Communications

DIVD is 16 februari 2022 gestart met de afdeling Communications, onder leiding van Hoofd Communicatie Lucinda Sterk. Zij heeft de volgende taken opgepakt: verbetering van uitingen via website, mailings en persberichten, Social Media, afstemming van perscontacten, interne communicatie (intranet, Slack, Trello), merchandise, huisstijl en gedeeld relatiebeheer met partners en sponsoren. Daarnaast nam ze ook deel in crisisteams in geval van een incident of groot onderzoek. Eind 2022 is er een communicatieprofessional bijgekomen die het hoofd bijstaat als vrijwilliger.

Onderzoeken worden in de regel afgesloten met een rapport. De afgelopen jaren wist de media DIVD te vinden bij spraakmakende onderzoeken. De afdeling communicatie is daarom meer meegenomen in de eindfase van een rapport zodat een communicatieplan kan worden gemaakt samen met de Case Lead. In geval van media-optredens voert in de regel

de case lead het woord. Dat was zo en zal zo blijven. Bij vragen over het instituut DIVD voerde de directeur of voorzitter het woord. In de bijlage een lijst met vermeldingen van DIVD in de media.

DIVD-ers zijn ook steeds meer te zien als spreker op security evenementen. In de bijlage een lijst hiervan. In 2022 hadden we ook ons eigen evenement: Hack Talk, voor zowel DIVDers als het bredere publiek. Na drie afleveringen moesten we echter constateren dat een publieksevent te veel druk legt op de organisatie. Maar de behoefte om elkaar af en toe fysiek te ontmoeten blijft. Eind 2022 is DIVD zich daarom meer gaan richten op bijeenkomsten voor eigen mensen, zoals meet-ups in de regio.

Wie zich aansluit bij DIVD krijgt een DIVD T-shirt. Zijn ze een jaar aan de slag, dan krijgen ze een hoodie. Die zijn dus alleen voor actieve vrijwilligers, niet voor de verkoop of andere relaties en geven daarmee een zekere exclusiviteit en herkenbaarheid. Gezien de groei van DIVD kon dat niet meer handmatig. We hebben daarom nu een helpdesk om verzoeken af te handelen.

In het jaar 2022 is een begin gemaakt met een nieuwe huisstijl. Hiervoor zijn templates ontwikkeld voor powerpointpresentaties en worddocumenten.

2.8. Governance, Risk & Compliance

In 2022 is ook de afdeling Governance, Risk & Compliance (GRC) opgericht. Die controleert DIVD op interne processen op risico's en het voldoen aan wet- en regelgeving en valt direct onder de directeur. Gezien de aard van ons werk ligt de nadruk vooral op informatiebeveiliging. In 2022 is deze afdeling gegroeid van een CISO en Privacy Officer naar een met vijf Security Officers. DIVD heeft ook een Functionaris Gegevensverwerking die eind 2022 is aangemeld bij de Autoriteit Persoonsgegevens. Die functie wordt dus in 2023 operationeel en nader ingevuld.

Het Security Office is in 2022 begonnen met assetmanagement en de invoering van een Information Security Management System (ISMS). De basis hiervan zijn de eisen zoals vastgesteld in de ISO 27001 norm. Hoewel we streven onze implementatie te laten voldoen aan deze eisen is het behalen van de certificering niet een doel op zich. De norm wordt voornamelijk gebruikt als handvat en de onderdelen die het meest belangrijk zijn vanuit risicoperspectief zullen als eerste worden opgepakt.

In 2022 is ook een crisismanager aangesteld die acteert bij de meer controversiële cases, als DIVD zelf in gevaar is en de directeur en de afdeling GRC zal bijstaan in het opstellen van een risk assessment en business continuity plan. Ook hebben we diverse verzekeringen afgesloten om ons in te dekken tegen risico's. DIVD heeft commissies die onafhankelijk en naar eigen inzicht acteren op verschillende niveau's van deze governance structuur.

Voor de Privacy Officer en FG is het bijzondere aan DIVD dat wij door ongevraagd scannen en melden in sommige gevallen ook persoonsgegevens verwerken zonder toestemming. Dat is ook praktisch onmogelijk: pas wanneer iemand kwetsbaar blijkt, zien wij wie dat is. Al in 2021 hebben we Privacy Management Partners hiervoor een Liability Impact Assessment laten doen. Die kwam er in het kort op neer dat we vanuit 'slachtoffernotificatie' best een persoonsgegeven als een mailadres mogen verwerken zonder toestemming, omdat we met onze notificaties een grote privacyschending kunnen voorkomen. Wat we wel kunnen doen voor de ontvangers is hen verwijzen naar onze Code of Conduct en Privacy Statement.

Waar DIVD wel privacy beleid moet voeren als elke andere organisatie is onze medewerkers en partners met wie we samenwerken. Door personele wisselingen is het privacybeleid van DIVD nog niet echt van de grond gekomen. In 2022 is een DPIA en een Privacy Statement opgeleverd, maar die moeten in 2023 nog verder uitgewerkt worden.

Het voornaamste risico voor DIVD is een CVD die niet goed verloopt, gevolgd door een rechtszaak, schadeclaim en reputatie verlies. Hierop wordt al sinds de oprichting van DIVD op gestuurd middels begeleiding van onderzoekers en handhaven van een Code of Conduct. Nieuw is onze bedrijfsaansprakelijkheidsverzekering, met cyberdekking, waardoor we ook voor dit risico verzekerd zijn.

Daarnaast zijn er steeds meer bekende en ook onbekende risico's die door DIVD gemanaged moeten worden. Zo zijn er naast informatiebeveiligingsrisico's door de groei van onze organisatie ook steeds meer financiële, juridische en personeelsrisico's. Eind 2022 is een eerste opzet gemaakt van een risico matrix, met daarin een lijst van 20 risico's, scenario's, verantwoordelijken, maatregelen om risico's tegen te gaan en ze te mitigeren. De maatregelen worden zo opgesteld dat zijn niet alleen effect hebben op de herkende risico's, maar ook bruikbaar zijn om de ons onbekende risico's te voorkomen, dan wel te mitigeren. Deze matrix delen wij los van dit jaarplan en zal in 2023 elk kwartaal geactualiseerd worden.

Naast deze controlerende lijnfuncties, heeft DIVD ook commissies die onafhankelijk en naar eigen inzicht acteren op verschillende niveau's van deze governance structuur. In 2022 is

een Ethische Commissie ingesteld van drie personen die gevraagd en ongevraagd cases toetsen op de DIVD Code of Conduct en, daar waar nodig ook de Code of Conduct actualiseert. Gezien de groei van het aantal cases en verbreding van onze onderzoeks scope, zal deze commissie nog meer betrokken moeten worden bij lopend onderzoek.

DIVD heeft sinds 2022 een vertrouwenspersoon waar DIVDers terecht kunnen met klachten of misstanden ten aanzien anderen binnen de organisatie. Voor 2022 stonden een diversiteitscommissie, die waakt over de samenstelling van ons personeels- en vrijwilligersbestand en een kascommissie die de jaarrekening en toewijzing betalingen controleert in de planning, maar zijn niet gerealiseerd.

3. Samenwerkingsverbanden

DIVD is inmiddels goed ingebed in de cybersecurity wereld via de werkgevers van onze vrijwilligers, de zusterorganisaties in DIVD.family en onze sponsoren.

3.1. De cybersecurity sector

De meeste van onze vrijwilligers hebben een baan in cybersecurity. In de regel zijn hun werkgevers trots dat ook hun mensen bijdragen aan een veiliger internet, begrijpen ze dat zij zich bij DIVD verder kunnen ontwikkelen en wordt actief kennis gedeeld. Daar waar gewenst, kan die werkgever ook een samenwerkingsovereenkomst krijgen van DIVD, waarin is vastgelegd wanneer en wat de persoon doet voor DIVD of de werkgever. Bijzondere vermelding verdient Schuberg Phillis, die DIVD niet alleen bijstaat met menskracht, maar ook een datacenter waar onze scaninfrastructuur is gehuisvest. Verder zijn er steeds meer cyber security bedrijven zoals Fox-IT en Hadrian waarmee DIVD ook samen optrekt in onderzoeken.

3.2. Dienstverleners

DIVD creëert geen dienstverbanden, maar koopt wel diensten in van ZZP'ers en bedrijven. De directeur en de afdelingshoofden van Research, CSIRT, IT service, HRM en Communications kregen in 2022 een overeenkomst van opdracht, variërend van 1 tot 2 dagen per week betaald, terwijl zij allen minstens het dubbele aantal uren maakten. LunaVia heeft DIVD diensten verleend op het gebied van boekhouding, HRM coaching, directie adviseur en

project ondersteuning. LinProfs steunde DIVD met extra uren op de bouw en het onderhoud van onze scaninfrastructuur. Schouten Zekerheid verzorgde onze verzekeringen, zonder hier provisie over te rekenen. En A2B internet zorgt ervoor dat ons AS aangemeld blijft bij RIPE en functioneert.

3.3. Sponsoren

DTC heeft DIVD voor 2022 subsidie verleend om de functies van directeur, Head of Research, Head of CSIRT deels te betalen en LunaVia onze boekhouding te laten doen. Sinds 1 april 2022 wordt DIVD gesteund door twee filantropische fondsen: Limelight en Adessium, waar de andere afdelingshoofden uit betaald werden. Naast financiële steun (zie begroting) hielpen deze fondsen DIVD in 2022 ook met haar professionalisering en ontwikkeling. BIT sponsored DIVD door gratis mailservices ter beschikking te stellen en VMware door een bijdrage aan onze scan infrastructuur. ESET steunt DIVD met jaarlijkse corefunding van 10.000,- euro. Tot slot kwamen er veel kleine incidentele schenkingen binnen via onze sponsorpagina en ontvangt DIVD veel software licenties in-kind.

3.4. Overheid

In de Nederlandse Cybersecurity Strategie wordt het belang van helpende hackers expliciet genoemd. Samenwerking vanuit de overheid met organisaties als DIVD wordt van daaruit steeds meer ondersteund. Zo is in Kamerdebatten over het samengaan van NCSC, DTC en DSP CSIRT in een NL-CERT al gesteld dat samenwerking met DIVD daarbij belangrijk is. Een Kamermotie voor financiële steun voor DIVD werd aangenomen met 128 stemmen voor. De Minister van Justitie en Veiligheid moet daar voor de zomer van 2023 een reactie op geven. Hoe dat concreet uitpakt, is nog moeilijk in te schatten.

De partijen die samen Het Landelijk Dekkend Stelsel vormen werken per case wel eens samen met DIVD en zouden idealiter via het Nederlandse Security Meldpunt onze meldingen moeten doorzetten. Dat verloopt vooralsnog stroef omdat weinigen van hun de IP adressen willen geven aan wie zij kunnen en mogen doordelen. Vooralsnog gaan de meeste meldingen via de ‘abuse-route’, oftewel clean networks van NBIP, waardoor sommige partijen een melding ontvangen via hun ISP.

Ook is veel gesproken met NCSC en andere betrokkenen over Cyclotron, de eventuele opvolger van het LDS. Vooralsnog gaat dat alleen over het delen van dreigingsinformatie (‘er

is een lek in deze software') en niet over doelwit notificaties ('jij, op dit IP adres bent kwetsbaar voor dit lek') en slachtoffer notificatie ('jij bent gehackt'), waardoor dit voor DIVD niet interessant is. Niettemin is de relatie met betrokkenen als NCSC en DTC goed en zullen we in gesprek blijven met deze partijen en per case kijken wat wel of niet gedeeld kan worden. De partijen die deze informatie willen doordelen, kunnen zich aansluiten bij het Nederlandse Security Meldpunt

3.5. DIVD.family

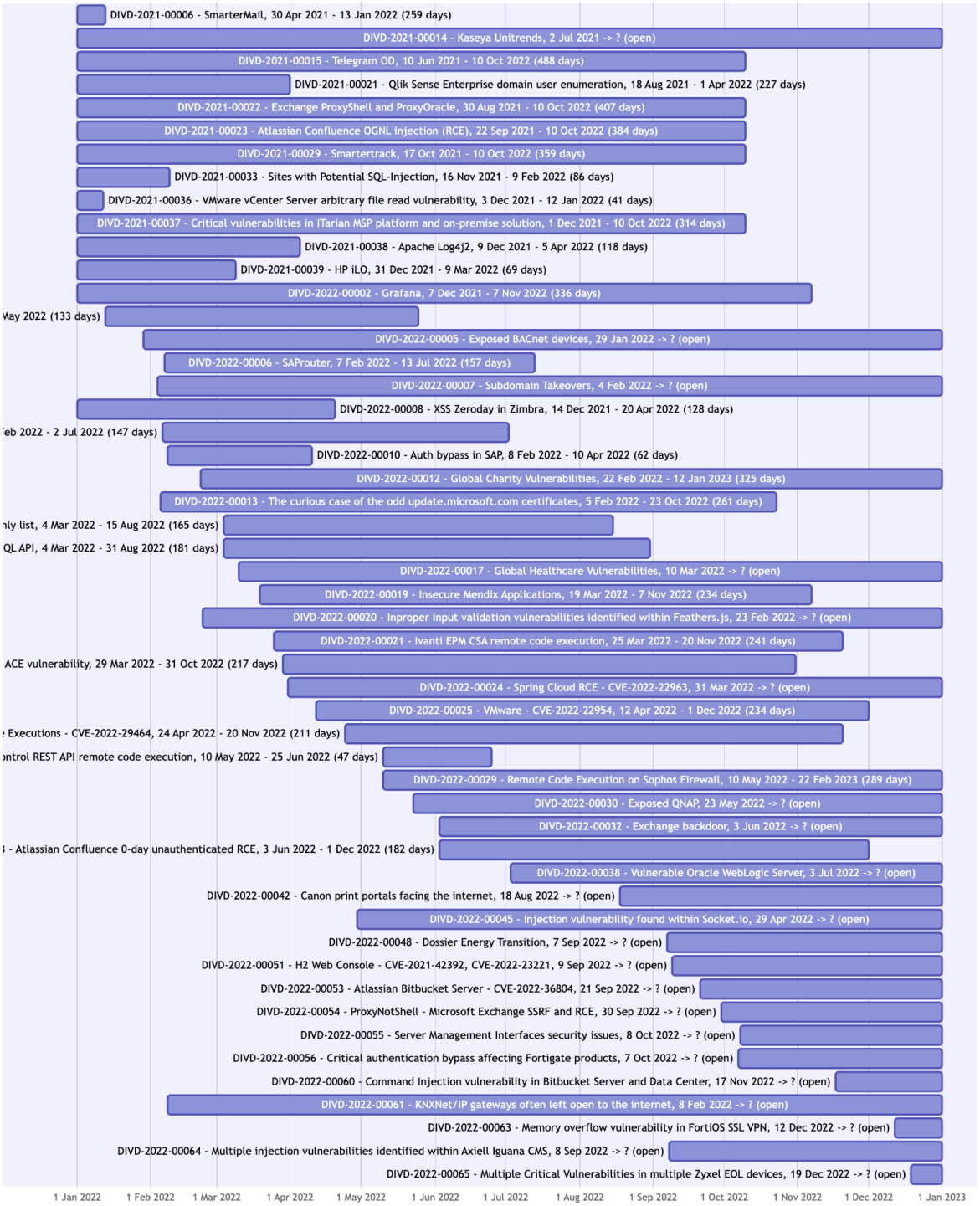
In 2022 zijn stichtingen opgericht waarin taken worden opgepakt die voorheen bij DIVD lagen: DIVD.academy gaat jonge en andere startende hackers opleiden, CSIRT.global gaat een internationaal netwerk opbouwen om doelwitnotificaties te delen, het Nederlands Security Meldpunt doet dat binnen Nederland, het DIVD.fund gaat fondsen werven en projecten financieren die niet binnen het DIVD uitgevoerd kunnen worden en DIVD.charity helpt hackers in financiële moeilijke situaties. Hiermee dragen we de werklast en risico's die bij deze taakuitvoering horen over aan andere entiteiten en kan DIVD zich meer focussen op onze missie.

In 2022 zijn al deze stichtingen zelfstandige juridische entiteiten geworden, met hun eigen begroting en eigen IT omgeving. Samenwerking met deze stichtingen wordt bevorderd doordat daar ook DIVDers werkzaamheden kunnen uitvoeren. Om belangenverstrengeling en conflicten over aansprakelijkheden te voorkomen, wordt door directie en bestuur toegezien op mogelijke rolconflicten. Voor verdere uitwerking van de verschillende stichtingen zie het document DIVD.family.

4. Financieel jaarverslag

Volgt na accountantsverklaring en uitspraak Belastingdienst.

Bijlage 1: onderzoeken 2022



Bijlage 2: DIVD in the media

Datum	Bron	titel
10-1-2022	FD	Overheid weet klein bedrijf nu wel te vinden in strijd tegen hackers.
11-1-2022	FD	Nederlandse hackersgroep wil uitgroeien tot wereldwijde beschermer van het internet
11-1-2022	enterprise times	Huntress donates $100,000 to DIVD Bug Bounty Program
12-1-2022	Tweakers	DIVD krijgt 88.000 euro voor opzetten van bugbountyprogramma
12-1-2022	security.nl	DIVD ontvangt 100.000 dollar voor verdere groei en bugbountyprogramma
12-1-2022	VPNGids	DIVD ontvangt donatie van 100.000 dollar
12-1-2022	Beveiligingsnieuws	Nederlandse hackersgroep gaat wereldwijd internet beschermen
12-1-2022	Fuentitech	Dutch cyber volunteers receive significant funding
12-1-2022	computerweekly	Dutch cyber volunteers receive major funding boost
12-1-2022	agconnect	Ransomware omarmt Log4j-gat voor VM-gijzeling
13-1-2022	theregister	Volunteer Dutch flaw finders bag $100k to forward national bug bounty goal
2-2-2022	Huntress	Leaving the Silo: MSP Vendors Give Back
8-2-2022	Cybersecurityraad	Veilig internet en veilige samenleving via Nederlandse stijl
9-2-2022	ComputerWeekly	How Dutch hackers are working to make the internet safe
18-2-2022	security.nl	Nederlandse onderzoekers scannen 35.000 goede doelen op kwetsbaarheden
23-3-2022	computable	DIVD onderzoekt onveilige Mendix-applicaties
31-3-2022	FD	Opnieuw beveiligingslek in veelgebruikte software
1-4-2022	Beveiligingswereld	Op 15 april nieuw: DIVD Café
1-4-2022	CRN australia	Kaseya taps Macquarie to host cloud apps

4-4-2022	govinfosecurity	Ransomware files episode 6
4-4-2022	agconnect	Serieuze ontwerpfout en achterstallig onderhoud bij Kaseya
26-5-2022	Security.nl	10.000 QNAP eigenaren gewaarschuwd
1-6-2022	Beveiligingswereld	Hoe zorgt het DIVD voor cyberveilige organisaties?
1-6-2022	BNR digitaal	Over CSIRT Global
6-6-2022	Computable	Confluence-gebruikers gealarmeerd voor kwetsbaarheid
5-7-2022	NU.nl	Dit verdient een cybersecurityspecialist
21-7-2022	Security.nl	NCSC ook CVE partij
24-7-2022	Be.Hardware.info	Het wachtwoord van tienduizenden omvormers voor zonnepanelen in Nederland stond jarenlang online
24-7-2022	FTM	Hacker ontdekt lek in zonnepanelen
24-7-2022	world.today-news	Hacker was able to sabotage tens of thousands of solar panels by lying around with password
24-7-2022	RTL4	(Opening 19:30 journaal)
24-7-2022	RTL4	Hacker kon tienduizenden zonnepanelen saboteren door rondslingerend wachtwoord
25-7-2022	Malwaretips	Solarman backend administrator account/password leaked
25-7-2022	VPNGids	Tienduizenden zonnepanelen kwetsbaar door rondslingerend wachtwoord
25-7-2022	Emerce	DIVD legt kwetsbaarheden in zonnepanelen en omvormers bloot
25-7-2022	Gemeente Maassluis	Kan China ons stroomnet platleggen?
25-7-2022	BNR radio	Ik maak me zorgen om cyberveiligheid in de energietransitie
25-7-2022	trlmobile.com	Hacker kon software van zonnepanelen met omvormers Chinese Solarman aanpassen
25-7-2022	A51.nl	(verwijzing naar FTM artikel)
25-7-2022	DutchITchanel	Nederlandse hacker krijgt toegang tot tienduizenden zonnepanelen
25-7-2022	Netherlands.posten.com	Hacker was able to modify software of solar panels with inverters Chinese Solarman

25-7-2022	Tweakers	Hacker kon software van zonnepanelen met omvormers Chinese Solarman aanpassen
25-7-2022	Security.nl	Miljoen omvormers zonnepanelen via gelekt wachtwoord kwetsbaar voor sabotage
25-7-2022	Techpulse.be	Hacker: miljoen zonnepanelen te saboteren via Solarman-software
25-7-2022	Radio1	Nederlandse elektriciteitsnetwerk zeer kwetsbaar voor Chinese sabotage via zonnepanelen
26-7-2022	Databreaches	Responsible disclosure: DIVD describes a “long and windy road” notifying a Chinese firm
26-7-2022	cybercrimeinfo.nl	Het verhaal achter ‘Tienduizenden zonnepanelen kwetsbaar’
26-7-2022	Computable	Ethische hackersorganisatie DIVD gaat internationaal
27-7-2022	informatiebeveiliging.nl	Omvormers zonnepanelen kwetsbaar door gelekt super-adminwachtwoord
28-7-2022	be.hardware.info	Kan China ons electriciteitsnetwerk hacken via zonnepanelen?
3-8-2022	AGConnect	Een cyberaanval in het nieuws: een stappenplan voor elke ict-manager
9-8-2022	Computable	Let op! Er zijn 3200 hackers op de camping
10-8-2022	Solar Magazine	Onderzoekers ‘hacken’ 42.000 Nederlandse installaties met zonnepanelen
10-8-2022	X-BOX	Onderzoekers ‘hacken’ 42.000 Nederlandse installaties met zonnepanelen
1-9-2022	Executive people	KPN Security maakt programma NL-Secure bekend
1-9-2022	Channel Connect	KPN Security maakt programma NL-Secure bekend
4-9-2022	Security.nl	Agentschap Telecom onderzoekt cybersecurity omvormers zonnepanelen
4-9-2022	Tweakers	Agentschap Telecom start onderzoek naar cybersecurity omvormers zonnepanelen
5-9-2022	Solar Magazine	Nieuw onderzoek Agentschap Telecom naar hacken omvormers zonnepanelen
6-9-2022	PV magazine	Niederländische Agentur untersucht Cybersicherheit von

		Photovoltaik-Wechselrichtern nach Hackerangriff
15-9-2022	OWASP	OWASP lecture - The Red Cross of the Internet
26-9-2022	Tweede Kamer	De vaste commissie voor Digitale Zaken over Wet beveiliging netwerk- en informatiesystemen
30-9-2022	FD	Nieuw beveiligingsprobleem in veelgebruikt e-mailsysteem van Microsoft.

Bijlage 3: DIVD op bijeenkomsten

Datum	Waar	Titel	Wie
15-04-2022	Worm Rotterdam	Hack Talk 20: Cyberoorlog	div
14-06-2022	Overheidsbrede Cyberwebinars	Hoe DIVD het hele internet scant op kwetsbaarheden	Chris, Tom, Frank
15-07-2022	Worm Rotterdam	Hack Talk 21: Going Global	div
24-07-2022	MCH2022	IOT: International Outage Technology (Disclosure of DIVD-2022-00009)	Frank
25-07-2022	MCH2022	Scanning and reporting vulnerabilities for the whole IPv4 space. How the Dutch Institute for Vulnerability Disclosure scales up Coordinated Vulnerability Disclosure	Chris, Astrid, Frank, Lennaert
16-09-2022	Worm Rotterdam	Hack Talk 22: The End	div
11-10-2022	PvIB	PvIB meets DIVD	Chris, Shairesh en Max
12-10-2022	Rabobank Security Days	How DIVD hacks and saves the internet	Chris
18-10-2022	OneConference	KaseyaVSA and what DIVD did to prevent the abuse of seven zero-days	Chris, Frank en Lennaert
24-11-2022	Heliview Cyber Security Experience	Hoe DIVD de wereld, en ook uw organisatie hackt en veiliger maakt	Chris
06-12-2022	University Leiden	How we hack the world and get away with it	Chris