Annual Report 2024

Date	**17 March 2025**
Author(s)	Michael Connelly, Chris van 't Hof
Version	1.0
Status	Final

Content

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Introduction

The mission of the DIVD, as stated on our website, is “We aim to make the digital world safer by reporting vulnerabilities we find in digital systems to the people who can fix them.” The vulnerabilities we report may have been discovered by our own researchers or be reported by third parties. What we then do with this is quite unique: we attempt to discover the contact details of people or organisations affected, and we email them. We do this with a team of 162 volunteers as of the end of 2024.

Managing the important work we do with a large and diverse team is only possible with a strong vision to create a safe and supportive environment that allows the volunteers to collaborate with each other and the broader cybersecurity community, and to provide the necessary structure, funding and IT resources to achieve the vision.

The self-professed “voluntary fire brigade of the internet”, the DIVD is independent, having complete freedom to choose which cases are taken on and how they are handled. The Code of Conduct, which all staff members must sign and to which the researchers and CSIRT team strictly adhere, is central to this. The DIVD’s work is recognized by the Dutch government, and the unsolicited ethical hacking activities carried out are protected under Dutch law. This is the cornerstone of the safe environment offered to the volunteers.

In August 2023, the DIVD board set out a broad and ambitious vision based on nine pillars:

1. Safe and familiar environment
2. Ethical values and new initiatives
3. Robust organisational structure
4. Automated and documented processes
5. Strategic planning and implementation
6. Transparency, innovation, and collaboration
7. Personal development and appreciation
8. Financial independence and stability
9. Robust risk management

These pillars were to be implemented in the transition from DIVD 2.0 to 3.0. This transition started in 2023, but in 2024, it really gathered momentum. The change from a siloed to a matrix model was initiated by launching the Project Office, with the idea that skills and resources from the various departments could be enlisted flexibly. This flexibility makes it easier to enlist help for the projects; however, the downside is that since people only have a limited number of hours per week to give, they can leave a hole in the department where they came from. This is just one example of the challenge of running an organisation where there are lots of people doing small amounts of work to reach a bigger goal.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Growth and leadership

The DIVD is its people. The growth of the DIVD, in size, capability, and in reputation is a story of personal growth in the volunteers driving it. By 2023, it had outgrown the flat organisation it had been in previous years, and it needed some structure through departmental heads. The core departments (CSIRT, Research, and IT) were more structured, but two departments desperately needed a head. The new Head of People & Culture and Head of Communications saw problems, took the initiative, and offered to help. In a voluntary organisation nobody is forced to work. We are 100% reliant on people willing to give their time and dedication. These two individuals took the lead of these departments, presented a vision to the rest of the management, and made a huge impact on the organisation.

Project Power-Up: Leveling Up Our Operations

Setting up the Project Office took a lot of time and energy from many departments. It was more than just finding project managers. IT did a fantastic job setting up Jira and Confluence as a project platform. Processes had to be made and communicated, and people trained. Projects are vital to the DIVD as they are a crucial funding source, such as the “CVD in the energy sector” project planned for 2025. The Project Office will bring a professional structured approach that will help ensure success and help with Pillar 8: financial independence and stability.

The Human Touch

Another department that made great strides in 2024 was People and Culture. P&C bridges many pillars listed above (1, 2, 3, 6, and 7), but the main focus was to take charge of the onboarding. The department ensured that everyone who joined landed in a place where they belong, knew what they were going to do, and brought back the onboarding time from months to a few weeks and sometimes even days. The number of volunteers still grew by more than 60 in 2024, and each volunteer needs some hours of work by the managers, by IT, by someone from P&C; these people are also volunteers with jobs, families and (hopefully) also a personal life.

Keeping the workforce happy and productive and managing steady growth are the biggest challenges, and there has been significant progress in this area throughout the year. Balancing the need to provide a space for people to grow in their skills and deliver really important work, we emphasized the rule that all volunteers commit at least four hours per week to the DIVD. Towards the end of 2024, the decision was made to advertise vacancies in the DIVD instead of taking someone on and trying to find a home. This is all part of the continuous growth in numbers, capabilities, and operational maturity going into 2025.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Ctrl + Alt + Defend: How IT Keeps Us Running

Information Technology is core to the DIVD operations and as the organisation grew, the IT had to scale. 2024 saw many changes and improvements:

- **Jira Migration**: Successfully transitioned from Trello to Jira despite challenges.
- **VMware Migration**: This is an ongoing project.
- **Security Operations Center (SOC)**: Established a SOC team, expanded forensic readiness, and integrated ELK (Elasticsearch).
- **Identity and Access Management (IAM)**: Currently being implemented with cross-departmental collaboration.
- **Configuration Management Database (CMDB)**: Centralizing IT configuration data for better decision-making.
- **Jira Service Management**: Transitioning away from Zammad to integrate Jira with Confluence.
- **Monthly Patching**: Regular updates to reduce vulnerabilities.
- **Backup Optimization**: Improving strategies to ensure business continuity.
- **Case-Specific Scan Servers**: Developing infrastructure-as-code solutions for on-demand server provisioning.
- **External Data Exchange Server**: Implemented security measures for external data transfers.
- **Teleport Implementation**: Enhancing privileged access security and simplifying management.
- **General Infrastructure Enhancements**: These include DNS, DHCP, out-of-band management, a MISP server (for sharing threat intelligence), and other enhancements for the SIEM.

Building and maintaining such a diverse and complex infrastructure needs a wide range of skills plus time and money. The staffing of the IT department is one of the biggest challenges. Many people are drawn to the DIVD because they want to do more ethical hacking. However, doing normal IT for the DIVD can be too much like their day job. To acquire and retain talent, the IT team has several initiatives:

- **Knowledge Sharing & Hackathons**: Organise internal events to share knowledge and have fun. Encourage everyone to attend, regardless of department.
- **Pizza Nights** are a great way to get to know your colleagues over food and a beer. Most people only see each other online.
- **Skill Development**: Focus on training programs for the SOC team and improving IT documentation.

Other ways of acquiring the skills that were discussed but not yet tried include insourcing or using services from sponsors and partners, hiring freelance staff, or outsourcing critical functions. Expanding the IT service, one way or another, will be an ongoing challenge for 2025.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

How the Homo Cyberneticus meets compliance

The DIVD tends to attract a certain type of person (homo cyberneticus). These people excel at the core function of the DIVD: to find and share vulnerabilities. However, words like structure, compliance, process documentation, etc., are not usually part of their daily lexicon. To interface with the government, sponsors, and law enforcement, a certain measure of those things is needed. To meet this demand, the GRC department was formed. They have a CISO who set up the Information Security Management System (ISMS) for ISO27001 compliance and a DPO currently working on GDPR (AVG in the Netherlands) compliance. Much progress has been made, but there is still much to do. Risk analysis, business continuity, and alignment with IT remain big challenges. Here, the DIVD runs into its perennial challenge. Volunteers only work a few hours weekly and want to do something different from their day job. Many ISO27001 and GDPR tasks are famously time-consuming. On the other hand, most DIVD volunteers are experts in one or more aspects of information security, so we are in a good position to get ourselves sorted out.

Finding things that work in the DIVD is often a trial-and-error process. Helping new members get up to speed has always been (and always will be) a challenge.. so a buddy system was created. This has been successful and seems to be well-received by new starters. One initiative in 2024 was to establish a team of coaches - available to members to guide them through personal challenges. The coaches were found, and the service was advertised, but only one person used this initiative.

Spreading the Word to Homo Ordinarius

Informing the world of the vulnerabilities we find, fanfaring our successes, and enticing partners and sponsors are the domains of our communications department. Growing from two staff at the start of 2024 to six at the end, the effectiveness and quality of our communications, press releases, and website made great progress. One of the major challenges was spreading a message that is - in essence - “nerdy” to an audience that is, well, less nerdy. Such a message might inform people about a vulnerability and advise them on what to do. The messages were not getting a good response rate. An in-house anthropologist identified a new sub-species - the Homo Cyberneticus - that found a natural home within the DIVD. Translating the messages to the general public - the Homo Ordinarius - became the mission of the new Communications department.

Still, spreading the word is also the responsibility of all people at DIVD. Especially during cyber security and hacker events, we can see an abundance of black and yellow shirts engaging with the crowd, both on and off stage. The absolute highlight was our own partner event; see the cover picture. Attachment 1 gives an overview of events where our people presented and our coverage in the Dutch media.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Partnerships

DIVD's network of partnerships has been growing steadily. We distinguish three forms of partnerships: financial contributions, free services, and collaboration.

Sponsors

Concerning financial contribution, the two major partners of 2024 were NCTV and Adessium. Smaller but more structural contributions came mainly from cyber security companies, such as Protect4S, ESET, and Secura. Right before the turn of the year, Accenture also joined, providing structural financial support and workforce. Incidental donations come through our donation page on SUPP or just a back transfer, mostly from companies we helped out and want to express their gratitude to or individuals who support our cause.

Services

The second category, free services, comes in many forms. A2B hosts our servers for half the price, BIT sends our notification emails without charges, Schouten Zekerheid is our free insurance intermediary, and Randstad hosted our Partner Event for free. Many vendors support DIVD with free charity licenses, such as Google (workspace), Microsoft (Slack), Rapid7 (scanning data), Red Sift (onDMARC), Cyber (ticket handling), and Pomerium (IAM). With Linprofs, we have a contract for updating our servers, and it also allows its Lead Architect to spend some more hours on DIVD without charge.

This actually counts for many of our volunteers: their employees support DIVD by allowing their employers to do some extra for our cause during work time. They are, more informally, very valuable partners of DIVD. Special mention here for Schuberg Philis, which has been supporting us from the start.

Collabs

In the third category, collaborations, the picture becomes even more colorful. DIVD had something valuable to offer: scan data on vulnerabilities no one has. Organizations working in the same field are very willing to help improve our data and forward notifications to their constituencies. For example Fox-IT helped out in some cases with fingerprinting vulnerable devices, so we can scan them, or even handed us their own scan data. The Dutch police were so kind to provide us with databases with stolen credentials so we could notify the victims. Shadow Server helps forward lists of vulnerable IPs to Gov CERTs not yet in contact with. But that list is growing.

2024 was a productive year for strategic partnerships, essential to DIVD's mission of staying connected with governments and academia. DIVD maintained and expanded relationships with 36 government CSIRTs and 9 Dutch universities, including 10 new government collaborations and 5 new academic connections.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

There are currently 36 countries where citizens and ISPs, after receiving our notification, also got one from their GovCERT/CSIRT. With 20 of them, we also formed a partnership, as they provide valuable information. These are Belgium, Germany, Denmark, Finland, Austria, Poland, Portugal, Slovenia, Slovakia, Estonia, Hungary, Ireland, UK and US. During 2024, we added Brazil, Singapore, Taiwan, Australia and Japan. Most of these government working relations are maintained through the dissemination of vulnerability intelligence and in-person contact at cybersecurity conferences, resulting in occasional contact between these various governments and the DIVD CSIRT.

In academia, relationships are maintained through guest lectures and research collaborations, such as the NWO THESEUS project led by a consortium of Dutch universities and various lectures on the topic of ethics in cybersecurity. While structural funding through research grants is a future goal, this is not yet a reality. However, DIVD is increasingly being approached to partake in research consortia that could eventually lead to such funding, with 2024 showing a strong increase in such requests.

Major achievements

The DIVD celebrated its first full year as a CVE Numbering Authority. We assigned numbers to and published 28 CVEs throughout 2024. There are several CVEs that have still not been published, as there is a process to follow before they get released. Vendors are given the chance to respond first. 2024 saw the total caseload handled by DIVD grow to 52 (up from 37 in 2023), and a total of 508,391 IP addresses were notified of critical vulnerabilities in systems that they owned. Not all the cases are about vulnerabilities, and in two notable cases, the DIVD undertook the gargantuan task of informing 26 million victims of their stolen credentials. Below is a list of some of the notable cases of 2024. For a full list, please visit our website: Cases | DIVD CSIRT

DIVD-2024-00005 - FortiOS Remote Code Execution

The year started strong with one of DIVD's biggest investigations up to that point. FortiOS, an operating system developed by Fortinet to support its products, had a critical vulnerability that allowed adversaries to completely compromise Fortinet edge devices with ease. The targeting of edge devices has been a recent trend in attacker behavior, making this case a prime example of DIVD's contribution to global cyber resilience. For big cases like this one, we like to collaborate with other parties. As such, DIVD sought collaboration with Fox-IT's Security Research Team (SRT) to scan for vulnerable instances. With Fox-IT's help, 377.633 vulnerable hosts were found and notified worldwide.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

DIVD-2024-00011 - Six vulnerabilities in Enphase IQ Gateway devices

It's all in the title. DIVD discovered six vulnerabilities in the Enphase IQ Gateway. The vulnerabilities could be combined into an Unauthenticated Remote Command Execution attack. What homo-ordinarius-speak for this is: "A hacker could completely take over your home solar panel system." The doomsday scenario is that bad actors could simultaneously and repeatedly turn off and on thousands of solar panels, causing massive outages in the national power grid. The vendor patched their devices within 24 hours.

DIVD-2024-00014 - Qlik Sense Remote Code Execution

This case is part of DIVD's collaboration with Project Melissa. Project Melissa is, in turn, a collaboration between Cyberveilig Nederland (representing most Dutch cybersecurity companies), the Dutch police, the Public Prosecutors Office, and the NCSC. The goal of Project Melissa is to protect the Netherlands from ransomware gangs. For this case, the Melissa team identified systems with a vulnerability in Qlik Sense, a system used for data analytics, some of which were already compromised by the Cactus ransomware gang.

Fox-IT had already performed scans, while DIVD spread the IP addresses of these compromised systems to foreign CSIRT teams, who, in turn, informed parties within their jurisdiction. In total, 3100 vulnerable servers were found, of which 122 were already compromised. DIVD helped prevent potential catastrophes at 3,100 organisations.

DIVD-2024-00019 - Victim Notification Operation Endgame

Operation Endgame is a global law-enforcement initiative spanning many European countries, the UK, and the US. Its goal is to infiltrate and shut down botnets. It has been very successful. In one day, 100 servers were taken offline, 2,000 domains were seized, and about five ransomware gangs were effectively shut down. The operation is still ongoing.

The infiltration revealed large numbers of compromised accounts, and DIVD undertook the task of informing them. All 18 million of them! How do you go about informing 18 million people? Emailing them quickly found us on a Google blacklist! We have to be smart about it, identifying organisations and mail providers, informing them of the leak, and letting them pass on the news to their users.

DIVD-2024-00022 - Millions of credentials scraped from Telegram

This is another case of victim notification. An anonymous source contacted the DIVD to say that they had infiltrated some Telegram groups and had retrieved massive amounts of stolen credentials. There was a massive amount of data. DIVD, as usual, was to notify the victims. The data was sorted and prioritized, resulting in 1.2 billion records of "stealer logs", i.e., data stolen from users' compromised

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

computers, containing 68.1 million user accounts with 8.2 million unique email addresses. As before, directly contacting each user was impractical, so the information was spread via foreign CSIRT teams and by notifying as many of the (over three million) domains as possible.

DIVD-2024-00035 - 17 vulnerabilities in Iocharger devices

Researchers discovered 17 vulnerabilities in some models of Iocharger electric vehicle chargers, which, alone or in combination, can lead to full device compromise. Sixteen vulnerabilities have been fixed; one has not yet been fixed. This case, along with Case 11 above, shows the importance of our project “CVD in het energiesysteem”. Homeowners have the right to purchase and install any charging system, battery, solar panel etc. on the market. Many of these products were not designed with security in mind. This presents a major risk to the country.

One Million Total Notifications

The first quarter of 2024 marked a significant milestone for DIVD, surpassing one million vulnerability notifications since its founding in 2019. With an average of 132% annual growth in notifications over the past five years, this achievement underscores both the effort required to improve digital security and the road ahead.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Finance

Pillar 8 of the Board vision is “Financial independence and stability”. DIVD strives for a fixed income stream that is not dependent on one specific source, such as subsidies, donations, or project funds, but a healthy mix. We strive to maintain a solid reputation that has enabled us to retain many permanent funders, allowing us to maintain our IT infrastructure and other essential aspects of our organization. A healthy mix of funding consists of ¼ government subsidies, ¼ charity funds, ¼ donations from companies and private individuals, and ¼ project financing. Of this, ¾ is core funding, and ¼ is project financing. Also, we should build a reserve fund to deal with financial setbacks.

Looking at 2024, the good news is that we have yet again managed to stay within budget, although both income and spending are below planning. Unlike 2023, we had some budget to pay a small staff and organize many more events. The bad news is that the most significant part of the revenues comes from just two sources, Adessium and NCTV, and all income is project-based, not structural. For a detailed financial report, see Attachment 2.

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Attachment 1: DIVD in the media and at events

DIVD in the news

Date	Source	Title
05-01-2024	RTL	'Cyber blijft niet in de digitale wereld, het raakt mensen zelf'
18-01-2024	RTL Nieuws	Cybercriminaliteit blijft stijgen met komst Artificial Intelligence
11-02-2024	NOS 8 uur journaal	Tienduizenden apparaten kwetsbaar
11-02-2024	NOS Nieuwsuur	Tienduizenden apparaten kwetsbaar
28-04-2024	NL Time	Operation Endgame
12-08-2024	Security nl	Enphase-zonnepaneelsystemen via kritieke lekken wereldwijd over te nemen
12-08-2024	FTM	Nederlandse hacker kan stekker uit zonnepanelen trekken en stroomnet platleggen
12-08-2024	Dutch IT Channel	Kwaadwillenden kunnen via zero-days Enphase IQ Gateway overnemen
12-08-2024	BNR	Nederlandse hacker kon miljoenen zonnepanelen uitschakelen
12-08-2024	Beveiligingsnieuws	Grote kwetsbaarheid stroomnet ontdekt
12-08-2024	Tweakers	Onderzoekers konden beheer enphase zonnepanelen overnemen via zes kwetsbaarheden
12-08-2024	Nu	Nederlandse onderzoekers konden van afstand zonnepanelen overnemen
12-08-2024	TechPulse	Ernstige kwetsbaarheden in Enphase-zonnepanelen ontdekt
13-08-2024	EenVandaag	Deze ethische hackers kunnen met gemak miljoenen zonnepanelen uitschakelen: 'Dan heb je een landelijke black-out'
13-08-2024	Aviation Analysts	These ethical hackers could easily disable millions of solar panels: “Then you’d have a national blackout.”
11-11-2024	NPO	Black-out

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Presentations

Date	Title	Who	Where
30 January	“DIVD @ SIDN Inside”	Chris van ‘t Hof and Henry Schokkenbroek	SIDN Arnhem
9 February	"A black hat in our white hat collective"	Frank Breedijk and Chris van 't Hof	Hacker Hotel, Garderen
10 February	"Empowering Cybersecurity Excellence: Unveiling the DIVD Academy Journey"	Astrid Oosenbrug and Victor Gevers	Hacker Hotel, Garderen
11 February	"Ethical Mass-Exploitation 101"	Ralph Horn and Max van der Horst	Hacker Hotel, Garderen
11 February		Jelle Ursum	Hacker Hotel, Garderen
20 February	"Hacken op het spectrum"	Chris van 't Hof	IT-vitae, Amersfoort
23 February	"Ethical Mass-Exploitation"	Ralph Horn and Max van der Horst	Erasmus Unversiteit, Rotterdam
7 March	"Threat Intelligence on Edge Device Exploitation"	Max van der Horst	TU Delft, Delft
29 March	“How e hack to make the world safer”	Chris van ‘t Hof and Oscar Vlugt	Accenture, Amsterdam.
4 April	"Permission Granted - Legal and Ethical Dimensions of Vulnerability Disclosure"	Max van der Horst	Universiteit Leiden, Leiden
8 April	“What to do when your company gets hacked”	Chris van ‘t Hof and Astrid Oosenbrug	Randstad and CISCO, Amsterdam.
14 May	"Janitorial Work on the Internet"	Ralph Horn and Max van der Horst	TU Delft, Delft
12 June	“DIVD @ WUR”	Winko Erades van den Berg	WUR Campus, Wageningen
19 June	“DIVD @ CISO Lunch”	Chris van ‘t Hof and Victor Gevers	Amstel Hotel, Amsterdam
27 June	“How DIVD makes the World Safer”	Chris van ‘t Hof and Lennaert Oudshoorn	ASML, Meeting Plaza Den Bosch
9 July	"Janitorial Work on the Internet"	Ralph Horn and Max van der Horst	Challenge the Cyber, Reeuwijk

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

4 September	Guestcollege on DIVD	Chris van 't Hof	Hogeschool, Rotterdam
1 October	"Innovating Cybersecurity Education and Ethical Hacking"	Astrid Oosenbrug, Barry van Kampen and Chris van 't Hof	NCSC ONE Conference, The Hague
21 October	"Gastles HackShield Middelbare School Zoetermeer"	Roxane Kortland, Astrid Oosenbrug, Joop ter Wal, Shairesh Algoe, Tabitha Vogelaar, Max van der Horst	Oranje Nassau College, Zoetermeer
27 October	"Entity Designations for Critical Supply Chains"	Chris van 't Hof	KEIO Security Conference, Tokyo
28 October	"Coordinated Vulnerability Disclosure in Japan and the Netherlands"	Chris van 't Hof	JP-CERTCC, Tokyo
5 November	"Partners in Crime"	Max van der Horst & Stan Plasmeijer	KAS Woerden
12 November	"Coordinated Vulnerability Disclosure in Japan and the Netherlands"	Chris van 't Hof	NTT Group, Tokyo
13 November	"Coordinated Vulnerability Disclosure in Japan and the Netherlands"	Chris van 't Hof	Dutch Embassy, Tokyo
16 November	"How DIVD does Coordinated Vulnerability Disclosure for the whole world"	Chris van 't Hof	AV Tokyo
18 November	"Understanding the Ripple Effects of Cybersecurity through Vulnerability Disclosure"	Max van der Horst	TU Delft, Delft
19 December	"Permission Granted - Legal and Ethical Dimensions of Vulnerability Disclosure"	Max van der Horst	European Cyber Conflict Research Initiative, Online
7 November	"How the Black & Yellow Hooded Hackers keep you and your business safe without you even realizing it"	Alan Lucas	Cybersec Netherlands

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl

Attachment 2: Financial Statement

Maanweg 174
2516 AB Den Haag
(+31) 70 - 41 90 309
question@divd.nl
www.divd.nl