Annual Report 2025

Date	24 March 2026
Authors	Gerard Janssen and DIVD MT
Version	1.0
Status	Public

Content

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

Introduction

DIVD describes itself as a “volunteer fire brigade of the internet.” Its mission is to improve digital security by identifying vulnerabilities in information systems, reporting these issues, and supporting organisations in resolving them. Vulnerabilities may be identified by DIVD itself or reported by third parties.

DIVD actively identifies and contacts individuals or organisations responsible for vulnerable systems to notify them, provide advice, and assist with remediation. A distinctive aspect of DIVD’s work is that this support is provided proactively and free of charge. DIVD offers assistance to any affected organisation and collaborates with a broad range of national and international partners.

DIVD operates as an independent organisation and has full autonomy in determining which cases to investigate and how they are handled. The work of DIVD is recognised by the Dutch government. All members agree to a Code of Conduct that governs the activities of both researchers and the CSIRT team. This agreement is part of the volunteer contract.

The organisation’s unsolicited ethical hacking activities are protected under Dutch jurisprudence and supported by appropriate insurance arrangements. This framework provides a safe working environment for volunteers and represents a unique model internationally.

At the end of 2025, DIVD had 172 volunteers. During the year, 40 volunteers left the organisation and 49 new volunteers joined. While 2024 marked a transition from an earlier organisational structure to a more professionalised model, 2025 was characterised by organisational stability.

In August 2023, the DIVD board set out a broad and ambitious vision for 2026, based on nine pillars:

1. Safe and familiar environment
2. Ethical values and new initiatives
3. Robust organisational structure

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

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

Over the past two years, significant progress has been made across most of these pillars. DIVD has evolved into a safe and trusted environment for volunteers, partners, and the organisations it supports. At the same time, the organisation is increasingly recognised as an authority within the global Coordinated Vulnerability Disclosure ecosystem.

Advanced analysis

DIVD continues to expand its activities across sectors, focusing on areas where it provides distinctive value. These include large-scale vulnerability scanning, credential exposure investigations, coordinated vulnerability disclosure, and the development of its role as a CVE Numbering Authority (CNA).

Through these activities, DIVD contributes to a safer digital ecosystem in the Netherlands and beyond. Governmental organisations such as the NCSC, have adopted similar practices, inspired by the working methods developed by DIVD, In this sense, DIVD has become a victim of its own success.

However, these organisations operate within well-defined regulatory frameworks. The NCSC and the other entities do not engage in active attacks on individual servers or broader digital infrastructure. These regulatory constraints also apply to the use of both weaponised and non-weaponised scripts. The deployment of such tools is required to remain within clearly established legal and operational boundaries at all times.

Against this background, the added value of DIVD does not primarily reside in the execution of standard scanning activities, but rather in the performance of more advanced and complex analyses. A distinguishing characteristic of DIVD is the level of knowledge and expertise embedded within the organisation, particularly with regard to the development of fingerprints: code that is used to scan for vulnerable software. These fingerprints constitute

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

an important analytical instrument and are based on the specialised capabilities and experience that DIVD has developed over time.

Changing geopolitical landscape

The DIVD operates in a rapidly changing geopolitical and digital environment characterized by increasing cyber threats, shifting international dependencies, and growing pressure on critical infrastructure. In this context, independent actors capable of identifying vulnerabilities and facilitating responsible disclosure play an increasingly important role in strengthening the resilience of the digital domain.

At the same time, in an era of (grey zone) warfare, maintaining impartiality and independence has become increasingly challenging. Limited financial resources further constrain our ability to continue our activities, while our research and findings carry the potential to significantly impact international security.

Financial instability

One of the nine pillars remains unresolved: financial independence and stability. With temporary funding scheduled to end in 2026, the organisation faces a critical moment. Several future scenarios are conceivable, ranging from the development of DIVD into a fully institutionalised organisation with a structural role in the cybersecurity landscape to a significant reduction in activities and a return to a small volunteer-based hackerspace model.
In 2026, our primary focus is on the repositioning of DIVD. The choices made in the coming years will determine whether the unique model developed by DIVD can continue to scale its societal impact.

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

Growth and leadership

As a fully volunteer-driven organisation, DIVD continually faces the challenge of attracting and retaining the right mix of skills. Volunteers often choose to contribute in areas different from their professional expertise, which can create gaps in critical operational roles such as infrastructure management. To address this, at the end of 2024, the organisation introduced targeted recruitment for clearly defined roles.

This approach enabled DIVD to engage volunteers based on specific skills and to integrate new members more effectively within the organisation. The impact became evident in 2025: the IT Services department grew from 9 to 50 participants. A similar targeted recruitment effort was applied to the CSIRT team, which had been operating with too few experienced members. This team was successfully strengthened as well.

Organisational development also focused on inclusion and professional growth. In 2024, a Diversity and Inclusion Officer was appointed. This contributed to a significant increase in diversity, with the number of female volunteers doubling from 11 in 2024 to 22 in 2025.

A Training Coordinator was also appointed to support the professional development of volunteers and to help experienced members expand their expertise within the organisation.
By 2025, the professionalisation efforts of previous years had begun to take clearer shape. The institute grew modestly, from 164 to 172 people. This period, therefore, marked not only growth in numbers but also an important step in the organisation's maturation and professionalisation.

The day-to-day management of the institute is led by director C. van 't Hof, who heads the management team. This team oversees the departments CSIRT, Research & Development, IT Services, People & Culture, Project Office, Marketing & Communications, and Governance, Risk & Compliance (GRC).

Over the past year, the Board has undergone several changes. In 2025, Shairesh Algoe succeeded Inge Bryan as Chair. Otto Hulst was appointed Treasurer, Eleonora Petridou continued as Secretary, and Tom van Deal remained as valued strategist and commercial

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

advisor. In January 2025, the institute also established an Advisory Board and welcomed Jaya Baloo, Inge Bryan, Samaneh Tajalizadehkoob, Piotr Kijewski, and Daan Dia to further strengthen its strategic guidance.

How IT Keeps Us Running

Information Technology is core to the DIVD operations, and as the organisation has grown, 2025 saw many changes and improvements:

- VMware Migration: This is an ongoing project. The goal is to transition to 'infrastructure as code'.
- Security Operations Center (SOC): Established a SOC team, expanded forensic readiness, and integrated ELK (Elasticsearch).
- Identity and Access Management (IAM): IT&Services will take care of an improved Identity and Access Management.
- Configuration Management Database (CMDB): Centralizing IT configuration data for better decision-making.
- Jira Service Management: Integrate Jira with Confluence.
- Monthly Patching: Regular updates to reduce vulnerabilities.
- Backup Optimisation: Improving strategies to ensure business continuity. Backups are made of the Google work environment, in case of 'when the shit hits the fan'.
- 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.
- Red Teaming: A team hunting for vulnerabilities in their own environment and also helping the SOC-team in identifying weak spots.

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

Building and maintaining such a diverse and complex infrastructure requires a broad range of skills. Professionals with these skills are in high demand and highly valued. IT Services aim to attract and retain them to DIVD by organising:

- 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 IT services, one way or another, will be an ongoing challenge in 2026.

Communication

Informing the public about the vulnerabilities the DIVD discovers, communicating the achievements, and engaging partners and sponsors are key responsibilities of the Communications department. The team decreased from six members at the beginning of 2025 to four by the end of the year.

One of the department's principal challenges was translating highly technical cybersecurity information into messages that are accessible to a broader audience. Communications about vulnerabilities often need to inform affected parties and provide clear guidance on appropriate actions.

Over the past year, the communication department supported researchers on several occasions with the responsible disclosure of vulnerabilities and data leaks. In addition, it renewed the partner event with a format that offers more opportunities for collaboration between partners.

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

Partnerships

In 2025, DIVD's primary funder was the NCTV, which had awarded the organisation a three-year subsidy that expired this year. This funding enabled significant professionalisation, including the establishment of a well-functioning Management Team, the creation of clear departmental structures, and the streamlining of supporting processes. These objectives were successfully achieved. However, no replacement funding has yet been secured. Structural funding from the cybersecurity sector remains very low. Some annual donations from IT companies remained and are listed on the website.

During 2025, DIVD increasingly expanded its collaboration with project partners. Within the energy domain, the organisation received financial support from the SIDN Fund, Topsector Energie, and The Green Village. In addition, a growing network of knowledge and collaboration partners joined DIVD, contributing to joint research initiatives and the organisation of events. Who we collaborate with and in what way can be viewed on divd.nl/partners.

Research

In 2025, a comprehensive reorganisation of the R&D department was initiated. Research activities have been structured around defined focus areas, replacing the previous approach of conducting individual, stand-alone studies. All activities are focused on the primary objective of enhancing safety in the Netherlands. Collaboration with the NCSC has been intensified to support and strengthen each other.

The primary focus areas include energy, as well as newly established research lines in healthcare and water management. In addition, a dedicated focus area titled "Exposed" has been introduced, concentrating on the use of open-source information. The DIVD also established a dedicated SAP research line. SAP (Systems, Applications, and Products in Data Processing) is an integrated enterprise software platform that supports core business processes.

In addition, the CVE-CNA has grown from three to seven members and will be set up as a separate division in 2026, operating as a fully independent department within the organisational structure.

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

Governance, Risk & Compliance

The GRC team consists of a Privacy Officer, Data Protection Officer, Crisis Manager, Contract Lawyer and CISO. Except for the CISO role, the team's composition remained stable throughout 2025. The DIVD conducted a comprehensive review of our Risk Register. This update included identifying emerging threats relevant to our institute and its people, and implementing robust mitigation strategies to proactively address operational and security risks.

To ensure full transparency regarding data handling, the DIVD officially published a privacy statement for volunteers and staff. This document outlines how the DIVD protects personal data in alignment with GDPR.

The DIVD successfully updated the volunteer agreement. This modernized contract ensures that the rights and responsibilities of both the organisation and our volunteers are clearly defined, providing better legal protection for everyone involved.

The GRC team acted as a strategic advisor on several internal cases, providing guidance on ethical dilemmas, compliance issues, and risk-based decision-making.

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

Major achievements

In 2025, the CSIRT department handled 18 cases, resulting in a total of 46,405 notifications concerning vulnerable IP addresses. This is substantially lower than in 2024 (52 cases, 508,391 IP addresses).

The processing of data from victims whose usernames and passwords had been stolen was substantially higher: 1,568,436,120 in 2025, compared to 26 million in 2024. Due to this enormous number, not everyone was notified, and the DIVD adopted a different approach.

The DIVD CNA (CVE Numbering Authority) processed 70 cases, of which 47 were specifically related to the energy track. This is more than in 2024 (28).

Here are some more detailed descriptions of DIVD cases. For a full list, please visit our website: csirt.divd.nl/cases.

Victim notification cases

DIVD-2025-00018 - VICTIM NOTIFICATION OPERATION ENDGAME 2.0

Operation Endgame 2.0 continues the international anti-botnet effort led by Dutch police and partners including Germany, France, Denmark, the United States, and the United Kingdom, with support from Europol and Eurojust. The operation generated new intelligence that was shared with organisations such as Have I Been Pwned, Spamhaus, and DIVD. The dataset includes usernames, redacted passwords, and usage dates from the Latrodectus botnet, as well as stealer logs containing credentials, related URLs, and theft timestamps, likely originating from compromised browser password managers.

DIVD-2025-00041 - VICTIM NOTIFICATION OPERATION ENDGAME S03E01

In November 2025, an international law-enforcement coalition led by the Dutch National Police conducted another phase of Operation Endgame, seizing 1,025 botnet servers worldwide. During the operation, large datasets of stolen credentials were recovered and shared with organisations including DIVD, Have I Been Pwned, Spamhaus, NCSC, DTC, and others to support victim notification. One dataset from the Rhadamanthys infostealer alone contains over 93 million records and more than 5 million unique email addresses, including

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

usernames, redacted passwords, URLs, timestamps, and sometimes device and IP information.

CNA cases

DIVD-2025-00001 - MULTIPLE VULNERABILITIES IN SICOMM BASEC SERVICE

In late 2021, DIVD researcher Jesse Meijer discovered publicly accessible source code for Sicomm BASEC and identified multiple vulnerabilities. Attempts to report the issues to Sicomm in 2022 and again by DIVD CSIRT in early 2025 received no response. After responsible disclosure deadlines passed, DIVD published the case and issued three CVEs in April 2025. Following a meeting with SicommNet, one vulnerability was patched, while broader remediation and security measures remain unclear.

DIVD-2025-00003 - MULTIPLE VULNERABILITIES IN MENNEKES SMART / PREMIUM CHARGING STATIONS

DIVD researchers Wilco van Beijnum and Harm van der Brik identified multiple vulnerabilities in the firmware of Mennekes Premium Column charging stations, used across Mennekes Smart and Premium chargers. The flaws allow authenticated attackers to execute operating system commands, read arbitrary files, and perform SQL injections against the device database. DIVD registered five vulnerabilities (CVE-2025-22366 to CVE-2025-22370) with CVSS scores ranging from 5.3 to 8.7. These issues affect critical firmware interfaces, including update and configuration components.

DIVD-2025-00009 - SUNGROW'S ISOLARCLOUD MQTT LACKING PERMISSIONS

Harm van den Brink, a DIVD volunteer and researcher at ENCS, discovered a vulnerability in SunGrow's iSolarCloud platform that exposed data from connected devices. Credentials for the underlying MQTT server and an RSA decryption key could be extracted from the website's JavaScript and DOM. This allowed a malicious user to subscribe to all MQTT topics and decrypt device messages. SunGrow patched the vulnerability on 6 June 2025, preventing further exploitation.

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

DIVD-2025-00011 - SEVERE VULNERABILITIES IN GROWATT PORTAL

On behalf of ENCS, DIVD disclosed a vulnerability in Growatt's cloud platform affecting the plant transfer function on oss.growatt.com and server.growatt.com. Due to missing authorization checks, a malicious user with a free installer account could transfer any plant to their account without the owner's knowledge, gaining control over the installation. In theory, an attacker controlling many systems could simultaneously switch them off, potentially disrupting the power grid.

DIVD-2025-00012 - FOUR VULNERABILITIES IN SCHNEIDER ELECTRIC EVLINK WALLBOX

DIVD researcher Wilco van Beijnum discovered four vulnerabilities in the Schneider Electric EVLink Wallbox EV charger. The issues allow authenticated users to read and write arbitrary files, execute code, inject commands through configuration options, and perform stored cross-site scripting via the reporting function. Schneider Electric will not patch the vulnerabilities because the product has reached the end of its commercial life, but has issued a security advisory with mitigation measures and offers a replacement product that is not affected.

DIVD-2025-00022 - SOLAREDGE SE3680H AND SOLAREDGE MONITORING PLATFORM VULNERABILITIES

The DIVD reviewed four publicly disclosed vulnerabilities affecting SolarEdge products. Three issues affect the SE3680H device line and require physical access, including an exposed debug interface, sensitive information leakage through bootloader diagnostics, and risks posed by an outdated Linux kernel. A fourth vulnerability in the SolarEdge Monitoring Platform allows an authenticated user to trigger a cross-site scripting (XSS) issue by providing a crafted report name during a deletion request.

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

Finance

The 2025 financial results show a significant difference between the budget and the actual outcome. This is partly due to NCTV contributions being allocated to previous financial years, and partly because DIVD generated less income than anticipated. Over the course of the year, expenditures were therefore gradually reduced, particularly personnel costs. As of 1 January 2026, the few members of the Management Team who did receive some compensation will be fully volunteers again. A limited budget remains available for project staff. See the attached detailed and checked financial report for 2025.

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