Connect2Trust

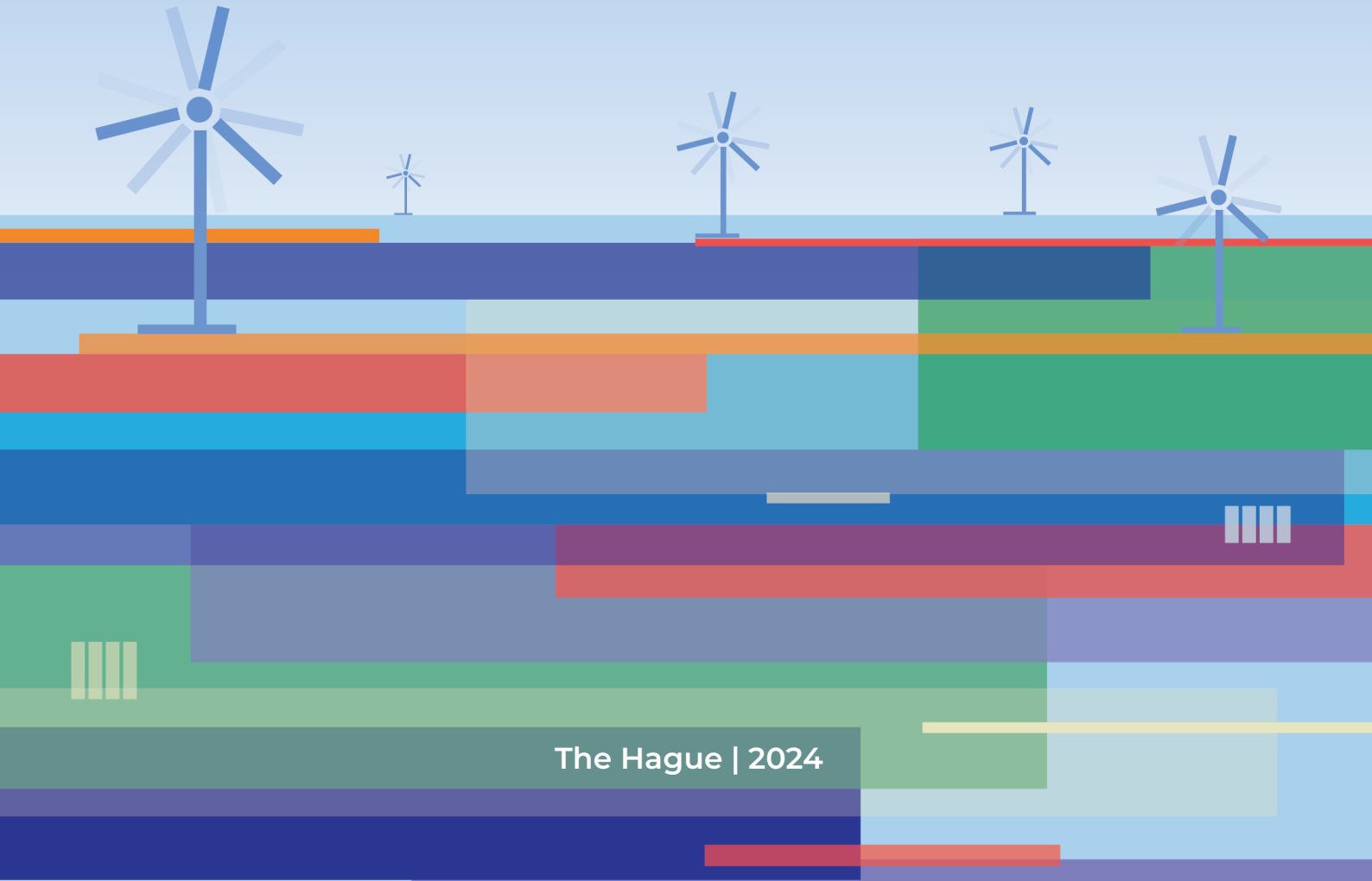
CyberPeace Institute

The Hague Humanity Hub

SHADOWSERVER

Cyber Resilience for NGOs: A Collective Intelligence Effort

Threat Landscape Report



The Hague | 2024

This project was supported by funding from the Cyber Resilience Subsidy Scheme of the Dutch Enterprise Agency (Rijksdienst voor Ondernemend Nederland, RVO). The Cyber Resilience Subsidy Scheme promotes initiatives that enhance cybersecurity and resilience, enabling organizations to address evolving cyber threats effectively. More information about the program is available at Cyber Resilience Subsidy Scheme.

Table of Contents

Authors & Project Partners **3**

Executive Summary **4**

1. Introduction **6**

2. Research Methodology **7**

3. Dutch NGO Cybersecurity Maturity **10**

3.1 Overall Maturity 11

3.2 Identify 12

3.3 Protect 13

3.4 Detect 16

3.5 Respond 18

3.6 Recover 18

4. NGO vulnerabilities **20**

4.1 Vulnerabilities and Incidents Affecting Selected NGOs 20

4.1.1 Network and Infrastructure Security 23

4.1.2 Application and Data Security 25

4.1.3 Known Vulnerabilities and Compliance 26

4.1.4 Incidents 28

4.2 Expanded Vulnerability Analysis of Dutch NGOs 31

4.2.1 Analysis & Findings 32

5. Recommendations **36**

6. Glossary **39**

7. Appendixes **42**

Appendix 1: Survey Questions 42

Appendix 2 - Research Questions 44

Authors & Project Partners

Project Lead

The **Hague Humanity Hub** (hereafter Humanity Hub or Hub) is a not-for-profit foundation that supports and strengthens the ecosystem for a more peaceful and just world. The Hub facilitates connections and innovation by offering the necessary ingredients for chance encounters, new alliances, inspirational collaborations, and the exchange of knowledge. Its community and network of partners encompass more than 200 organizations in and around The Hague working on themes such as humanitarian response, development aid, peacebuilding and access to justice.

Report Authors

The **CyberPeace Institute** is a Geneva-based foundation protecting the most vulnerable in cyberspace. Independent and neutral, the Institute investigates and analyzes the human impact of systemic cyber threats, delivers free cybersecurity assistance, tracks the enforcement of international laws and norms and forecasts threats to cyber peace. The Institute manages the CyberPeace Builders, a programme that matches over 1,200 cybersecurity experts from industry to nonprofits around the world.

The mission of **Stichting The Shadowserver Foundation Europe** (hereafter Shadowserver) is to make the internet more secure by bringing to light vulnerabilities, malicious activity and emerging threats. Shadowserver is the world's largest provider of free public benefit cyber threat intelligence. Shadowserver investigates malicious Internet activity, collecting large volumes of malware and related analysis and meta data, and shares infection and malicious data with appropriate network owners.

The **Connect2Trust Foundation** (hereafter Connect2Trust) is a cross-sector partnership between (inter)national companies active in the Netherlands. Connect2Trust provides a safe and trusted environment within which private parties who are part of Connect2Trust can analyze and exchange sensitive and confidential information about cyberthreats and best practices, together with (cyber)security-challenged government parties.

Executive Summary

Non-Governmental Organizations (NGOs) are vital in delivering essential services to vulnerable populations, yet their growing reliance on digital infrastructure has made them increasingly susceptible to cyberattacks. This report, produced under the Cyber Resilience for NGOs: A Collective Intelligence Effort project, analyzes the cybersecurity challenges faced by Dutch NGOs. With contributions from The Hague Humanity hub, the CyberPeace Institute, Connect2Trust, and ShadowServer, the study assesses the cyber threat landscape of NGOs, pinpointing critical risks and vulnerabilities that impact their operations.

Key Findings

Key Finding 1

Cybersecurity Maturity

Dutch NGOs show diverse levels of cybersecurity maturity, averaging a score of 49.9 out of 100 based on the General Cyber Security Assessment (GCSA) conducted by the CyberPeace Institute. While some organizations have implemented basic cybersecurity measures, most still face significant gaps, especially in asset management, incident response, and data protection. Worryingly, only **32% of NGOs use MFA for accessing critical systems** like email, cloud services or financial tools. Another key data found is that **only 36% of NGOs conduct phishing simulations**, a practical tool for training. Only a minority have advanced levels of preparedness, with the majority operating below an optimal security threshold.

Key Finding 2

Vulnerabilities

A range of technical vulnerabilities is evident across both small and large NGOs. Exposure of remote administration protocols, such as Remote Desktop Protocol (RDP), is seen widely across the sector, allowing potential attackers direct access to critical systems if unsecured. Additionally, database services like MySQL and file transfer protocols (FTP) are exposed in both small and large organizations, heightening the risk of unauthorized access. Larger NGOs have further vulnerabilities in high-severity Exchange server configurations, a known target for cyber attackers, although no Exchange servers were detected in smaller NGOs.

Key Finding 3

Incident Detection and Response

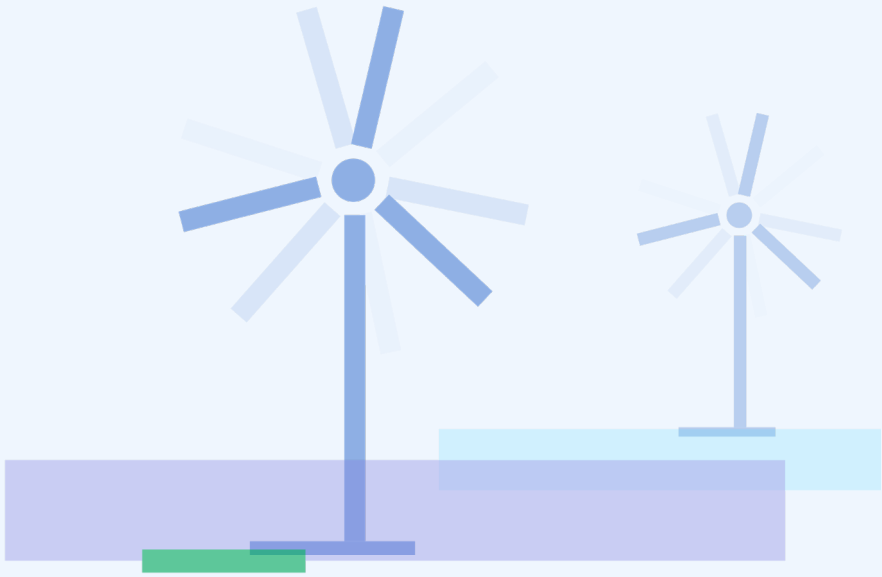
Limited incident response and detection capabilities remain a challenge, with only a fraction of NGOs having robust plans. **Roughly 36% don't monitor for potential data leaks, and 72% lack comprehensive oversight of their cloud services**, leaving them vulnerable to undetected breaches. This deficiency in detection mechanisms elevates the risk of undetected intrusions and prolonged operational impacts.

Key Finding 4

Threat Landscape

Dutch NGOs face persistent risks from ransomware, social engineering, and disinformation. Although publicly disclosed cyber incidents are few, credential leaks and malware infections indicate substantial exposure. Between October 2023 and October 2024, **43% of the NGOs surveyed experienced credential theft**, primarily due to infostealer malware, underscoring significant ongoing risk to their data security and operations.

This report highlights the pressing need for strengthened cybersecurity resilience among NGOs to protect their essential missions and reinforce their defenses against a rapidly evolving threat landscape.



1. Introduction

Non-governmental organizations (NGOs) play a pivotal role in addressing societal challenges, providing critical services to vulnerable populations in areas such as humanitarian aid, human rights advocacy, and social cohesion. Numerous NGOs operating in and out of the Netherlands are at the forefront of these activities. However, as their operations become increasingly digital, these organizations have become prime targets for cyberattacks, complicating their mission to assist those in need.

Cyberattacks on NGOs have surged, affecting both major organizations as well as smaller groups. Microsoft reported in 2021 that NGOs were the second-most targeted sector by nation-state threat actors between July 2020 and June 2021.[1] Further research has tracked 500 confirmed attacks on NGOs since 2016 resulting in tens of millions of euros in stolen funds and more than a billion of data records stolen. Despite their crucial role, many NGOs lack the necessary resources to mitigate these cyber threats effectively.

In line with other Dutch initiatives such as CyberSecure The Hague, Connect2Peace and Beyond 125, that emphasize the importance of strengthening the cybersecurity of under-resourced organizations, this report aims to raise awareness among Dutch NGOs, their donors and public authorities about the urgent need to bolster the cybersecurity of those protecting the most vulnerable.

This report is part of a project made possible by the Dutch Digital Trust Center (DTC) and funded by the Netherlands Enterprise Agency (RVO), called 'The Cyber Resilience for NGOs: A Collective Intelligence Effort'. The project is implemented by a consortium of partners including the CyberPeace Institute, the Hague Humanity Hub, the ShadowServer Foundation and Connect2Trust.

More specifically, this report presents an assessment of the current level of cyber resilience in the NGO sector, identifying key risks, vulnerabilities, prominent threat actors, and the impact of cyberattacks on operations and beneficiaries. Additionally, the project aims to enhance the cyber preparedness of Dutch NGOs through crisis response simulations.

2. Research Methodology

This report is based on data sourced and analyzed by the CyberPeace Institute, Connect2Trust and ShadowServer through four primary channels:

- **Primary data** through direct engagement with NGOs in the Netherlands. This data was collected via surveys, interviews, focus groups, and testimonials drawn from the CyberPeace Institute's work with NGOs. The data has been anonymized to respect the privacy and security of the participating NGOs.
- **Secondary sources** from open sources, including passive scanning of digital assets by ShadowServer to identify risks or vulnerabilities and open-source intelligence (OSINT) techniques. Additionally, data has been gathered by Connect2Trust and other trusted cybersecurity partners to provide further insights, including telemetry data, data breaches, leaks, and cybersecurity ratings.

To assess the cyber resilience and readiness of NGOs, the methodology employed a **mixed-methods approach**. This approach combined qualitative and quantitative data collection and analysis to provide a comprehensive, fact-based understanding of the cybersecurity challenges facing the NGO sector.

The data collection for this report focuses on NGOs based in the Netherlands. A survey was distributed among participating NGOs, consisting of a series of questions designed to measure cybersecurity maturity across key categories. These categories align with cybersecurity best practices and assess critical areas such as asset management, incident response, and data protection.

In line with the scope of the project, the research also involved an in-depth analysis of threats faced by NGOs in the country. The report examines the types of attacks NGOs have encountered (e.g., ransomware, social engineering, disinformation), the actors behind these attacks, and the vulnerabilities that have been exploited. The collected data also informs crisis response exercises that are being developed to help NGOs better prepare for and respond to cyber incidents.

The **General Cyber Security Assessment (GCSA)** tool developed by the CyberPeace Institute was adapted to guide NGOs in assessing their cybersecurity maturity. This tool, based on industry standards such as the NIST Cybersecurity Framework, enables NGOs to evaluate their cybersecurity posture and identify areas for improvement.

Additionally, this report draws on insights provided by cybersecurity partners such as Connect2Trust, including data from vulnerability scanning and threat intelligence platforms such as Bitsight[2], Kaduu[3] and Shadowserver[4]. These insights offer a technical perspective on the current vulnerabilities affecting NGOs in the Netherlands.

Shadowserver collects various daily Internet scale datasets[5] as a result of Internet-wide scanning, sinkholing/disruption of malicious infrastructure (with the support of Law Enforcement Agencies and/or private industry), sensor based and malware collection based observations.

The collected data allows Shadowserver to obtain "the big picture" of cybersecurity issues across the Netherlands which includes NGOs in the Netherlands as well. Specifically, Shadowserver checks daily for the following:

- Endpoint attack surface, broken down by the identified device vendor, type, as well as service
- Vulnerability exposure by current threat and attack vector
- Observed exploitation and other attacks
- Compromised systems
- Malware infections as seen in the sinkhole data
- Distributed Denial of Service (DDoS) attack activity
- Blocklisted resources

Please note Shadowserver attempts to track the most relevant threats and vulnerabilities that are currently exploited on the Internet, but the list is by no means exhaustive.

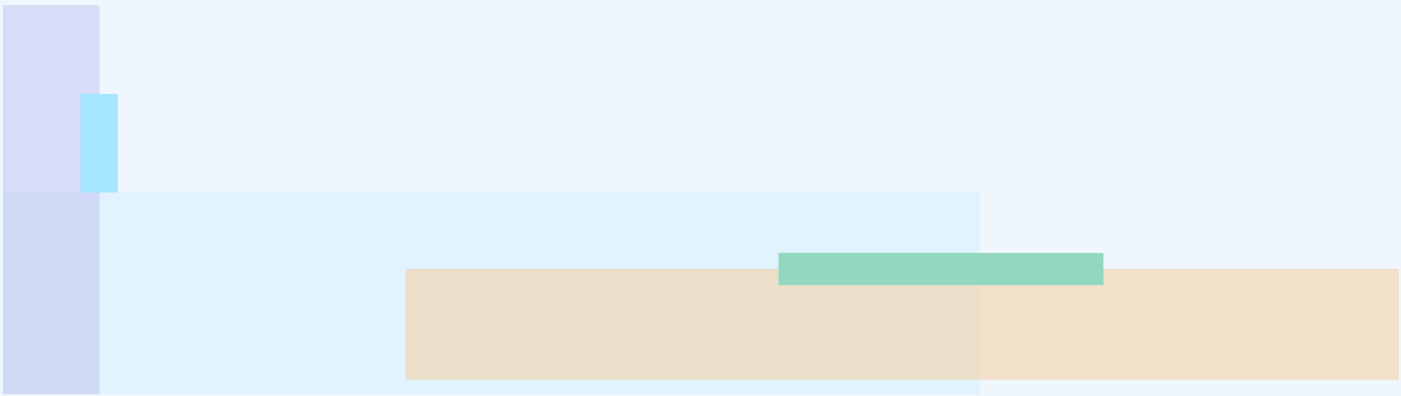
Limitations

While this study provides valuable insights into the cybersecurity landscape of Dutch NGOs, several limitations should be noted. As part of the initial project scope, 30 NGOs were onboarded into the program, however only 25 submitted their answers to the GCSA survey by the given deadline. Furthermore, the sample size is relatively small, focused on NGOs operating mostly in and around the Hague (26 in The Hague, 1 in Utrecht, 2 in Amsterdam and 1 in Delft), which may limit the generalizability of the findings. Other NGOs with different operational profiles and resources may face distinct challenges not captured in this study. Additionally, the communication and outreach of the project

were mostly done in English which may have kept some organizations from engaging due to the language barrier.

Moreover, NGOs may be hesitant to share detailed information about cybersecurity incidents due to concerns about reputational damage, lack of regulatory obligations, or limited awareness of the risks associated with such disclosures. As a result, some of the insights drawn from the study may not fully capture the extent of the vulnerabilities NGOs face.

Finally, the use of open-source intelligence and passive scanning techniques may provide only a partial view of the NGO cybersecurity landscape. While these methods help identify certain risks, a more in-depth, active engagement with NGO systems would provide a fuller picture of their cybersecurity posture, which was beyond the scope of this study.



3. Dutch NGO Cybersecurity Maturity

The NGOs covered in this report are all based in the Netherlands, though many of them have extensive international operations and branches across different regions. While their headquarters remain rooted in the Netherlands, their work often spans across continents, addressing critical global challenges. Some of these organizations are relatively small, with fewer than 20 staff members, while others employ hundreds, managing complex international programs and partnerships. The size of these NGOs often correlates with their mission and geographic scope, with smaller organizations focusing on specialized issues, while the larger ones operate on a global scale with widespread networks and collaborative projects.

Despite being Dutch-based, the international footprint of these NGOs is vast. They work in various regions, including Europe, Asia, Africa, and the Americas, addressing issues like human rights advocacy, conflict resolution, environmental protection, and humanitarian aid in some of the most challenging areas of the world. Others maintain a more regional focus, concentrating on areas like Central Asia or Sub-Saharan Africa, while coordinating from their Dutch offices. Even organizations with a primary focus on Dutch or European affairs contribute to global initiatives through partnerships with international NGOs, governments, and multilateral institutions, making their influence and impact truly global while maintaining a strong Dutch presence.

The missions of these Dutch NGOs are diverse, yet they share a common commitment to addressing pressing global challenges. Some focus on protecting the environment, combating wildlife crime, or tackling climate change, while others work in conflict prevention, human rights advocacy, and the promotion of transparency and anti-corruption measures. Many of these organizations are dedicated to alleviating suffering and improving the livelihoods of vulnerable populations, whether through providing humanitarian aid in conflict zones or supporting sustainable development and public health initiatives in developing regions. The Dutch origin of these NGOs serves as a foundation for their international work, but their reach extends far beyond national borders.

In terms of funding, these Dutch NGOs rely on a variety of sources to sustain their work. Many receive grants from governmental bodies, international agencies, and private foundations, while others depend on project-based funding linked to specific initiatives. Public donations

also play a crucial role, particularly for those organizations engaged in advocacy or grassroots efforts. While some larger NGOs benefit from institutional support from multilateral organizations or corporate partnerships, smaller Dutch NGOs often operate with limited resources, relying on grants and individual donors to continue their important work. Despite the differences in size and funding models, all of these Dutch NGOs share a commitment to securing sustainable financial support to advance their missions both at home and abroad.

3.1 Overall maturity

The cybersecurity maturity of the 25 NGOs surveyed in the Netherlands shows a moderate level overall, with the average maturity score being **49.9 out of 100**. This indicates that while some organizations have implemented basic cybersecurity measures, there are significant gaps in overall preparedness. The minimum score of **25** in the group reveals that some NGOs are struggling with cybersecurity practices, potentially leaving them highly vulnerable to threats.

A closer look at the data reveals that half of the surveyed NGOs have a maturity score below **46.7** (the median), suggesting that a significant portion of the group is operating below an optimal security level. This raises concerns about the ability of these organizations to handle cybersecurity risks, especially in key areas like asset management, incident response, and detection. The upper quartile (top 25%) scored **60** or higher, indicating that some NGOs are more advanced and proactive in their cybersecurity practices, possibly having well-established policies and protective measures in place.

The highest score achieved was **81.7**, showing that some NGOs are closer to cybersecurity resilience. However, the large spread of scores, with a standard deviation of **16.1**, highlights considerable variability in cybersecurity maturity across the group. This suggests that while some NGOs are progressing, others are lagging significantly, potentially due to limited resources, lack of expertise, or insufficient prioritization of cybersecurity.

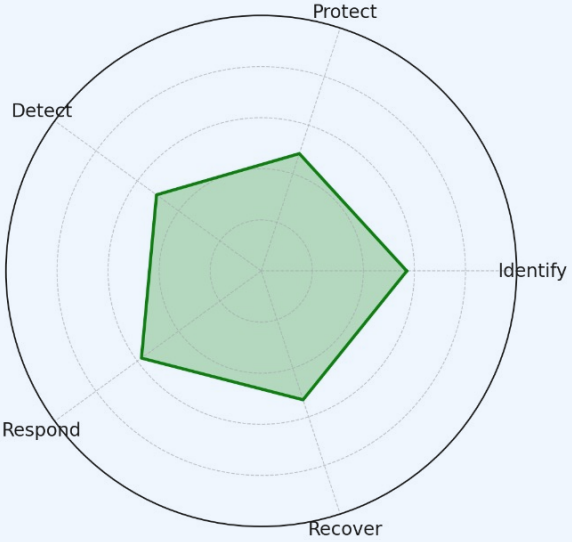


Figure 1: Cybersecurity maturity levels

3.2 Identify

The **Identify** function, as outlined by the NIST Cybersecurity Framework, is foundational for building a robust cybersecurity program, focusing on understanding the assets, risks, and governance structures that are key to security efforts. The NGOs surveyed show a mixed level of maturity in this category, with several areas needing improvement. For instance, when asked if they had an up-to-date assets inventory, only **32%** of the organizations (8 out of 25 respondents) confirmed they had one, while **48%** were only partially compliant, and **20%** lacked this entirely. This statistic shows that almost half of the NGOs have only partially mapped their assets, which puts them at risk, as they may not be fully aware of all the potential vulnerabilities within their infrastructure.

A core part of the Identify category is recognizing critical functions necessary for service delivery, particularly when working with vulnerable populations. Only **40%** of the NGOs (10 out of 25) reported having identified their critical functions, while **44%** were partially compliant, and **16%** had not yet started this process. Without a clear understanding of these essential functions, organizations face the risk of disruptions in service delivery during a cyber incident, potentially jeopardizing their ability to provide critical support. This is particularly concerning for NGOs working in sensitive sectors, where service continuity is vital for supporting at-risk communities.

In terms of governance, the survey reveals that only **28%** of NGOs (7 out of 25) have a comprehensive cybersecurity policy, while **52%** are still working on partial implementations, and **20%** lack one entirely. These numbers point to significant gaps in governance structures, suggesting that most organizations do not have formalized policies to guide cybersecurity practices. Without such policies, staff behavior and data handling practices may be inconsistent, increasing the risk of internal vulnerabilities. A clear cybersecurity policy is essential for setting standards across the organization and ensuring staff are aware of their responsibilities in protecting digital assets.

Data protection policies, another key aspect of the Identify function, show similar levels of underdevelopment. Only **28%** of the NGOs (7 out of 25) have fully implemented a data protection policy, with **48%** reporting partial compliance and **24%** lacking one. This is concerning, especially given the sensitivity of the data many NGOs handle, such as personal information of vulnerable populations. Without a formal data protection

policy, these organizations are more exposed to data breaches, which can lead to both legal and reputational risks, particularly in an era where data privacy regulations are tightening globally.

In more specialized areas, such as vulnerability disclosure policies and AI guidance, the numbers are even lower. Only **16%** of NGOs (4 out of 25) have a vulnerability disclosure policy, with **56%** having partially implemented one and **28%** lacking it entirely. For AI guidance policies, the figures are similarly low, with only **12%** (3 out of 25) having a full policy, **56%** with partial adoption, and **32%** without any policy in place. These statistics show that NGOs are still in the early stages of adopting forward-looking cybersecurity measures to manage emerging threats, further highlighting the need for more structured approaches in this area.

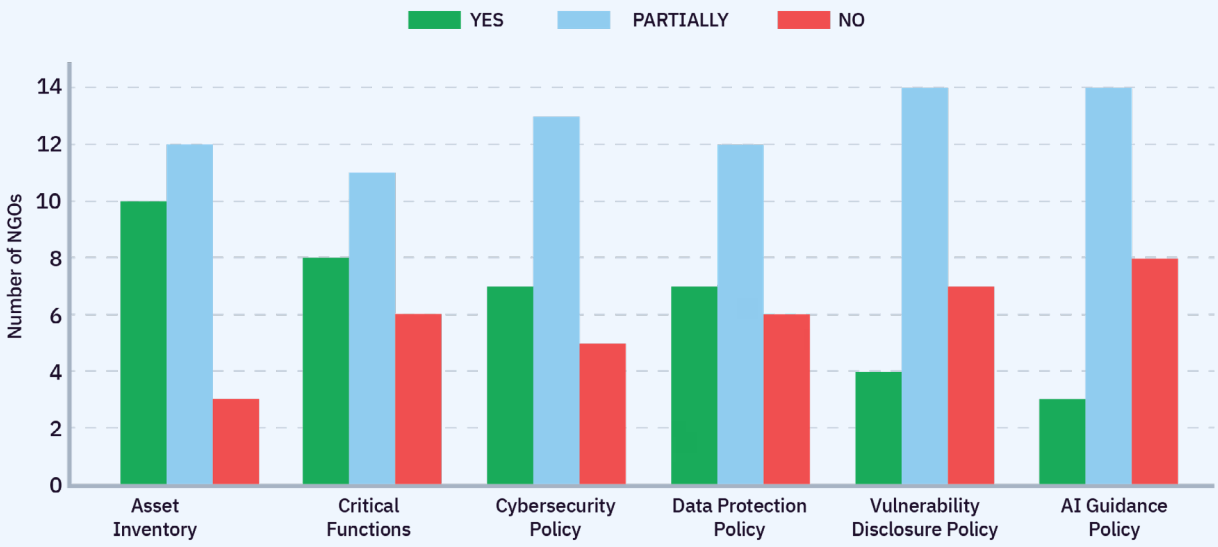


Figure 2: NGO Compliance Levels in Identify Category

3.3 Protect

The **Protect** function, which focuses on access control, training, data security, and the implementation of protective technologies, is the largest and most comprehensive area surveyed. Despite its importance, many NGOs in the Netherlands struggle with achieving full maturity in this category. When asked if they ensure adequate management of user accounts (such as account creation, updates, and suppression for people who join or leave the organization), only **36%** (9 out of 25) responded with full compliance, while **48%** reported partial compliance, and **16%** did not have such measures in place. This is a concerning trend, as poor

user account management can lead to insider threats or unauthorized access, especially when former employees still have access to critical systems.

The question of access privileges based on user roles also highlights gaps in access control across the NGOs. Only **32%** of the organizations (8 out of 25) have a process for assigning access based on roles and responsibilities, while **52%** are only partially compliant and **16%** do not follow this practice at all. This indicates that a significant portion of NGOs may grant excessive privileges to users who do not require them, increasing the risk of accidental or malicious data exposure. Properly defining user roles and restricting access based on need-to-know principles is crucial for reducing the attack surface within an organization.

Asset configuration and security also reveal a mixed picture.

40% of the NGOs (10 out of 25) ensure that all physical and digital assets are up-to-date and adequately configured.

44% report partial compliance and **16%** not addressing this at all. This lack of comprehensive configuration management could leave systems vulnerable to exploitation, as unpatched systems or improperly configured devices are common attack vectors. Furthermore, the secure disposal of hardware and software assets was another area of concern, with **36%** of NGOs (9 out of 25) confirming they follow secure disposal practices, **44%** partially compliant, and **20%** not addressing this. Without secure disposal, old hardware or data can be easily recovered by malicious actors, presenting a significant risk.

In terms of endpoint security, the numbers improve slightly but still leave room for growth. **48%** of NGOs (12 out of 25) report that their computers, laptops, and mobile devices are protected with up-to-date security software, such as antivirus programs, while **40%** are partially compliant, and **12%** do not have this in place. While nearly half of the NGOs are on track with basic endpoint protection, the fact that the other half are either only partially compliant or completely lacking protection reveals a major vulnerability in defending against malware, phishing attacks, and other threats. Similarly, only **36%** of NGOs (9 out of 25) have firewalls installed between their internal network and the internet, while **48%** are partially compliant and **16%** have no firewall. Firewalls are essential for blocking unauthorized access and preventing

external attacks, so their absence in several organizations indicates a serious security gap.

The use of multi-factor authentication (MFA) remains underutilized, despite being a highly effective measure for securing sensitive systems. Only **32%** of NGOs (8 out of 25) use MFA for accessing critical systems like email, cloud services, or financial tools. Another **40%** have partially implemented MFA, and **28%** are not using it at all. This low adoption rate of MFA is concerning, especially as phishing attacks and credential theft become more prevalent. A similar pattern is seen with the use of password managers, where only **28%** (7 out of 25) of NGOs use them, **40%** are partially compliant.

32% do not have any system in place to manage passwords securely.

Without a password manager, organizations are more prone to password reuse and weak passwords, making them vulnerable to brute-force attacks or credential stuffing.

Cybersecurity training, an essential element of the Protect function, is similarly underdeveloped.

44% of the NGOs (11 out of 25) provide regular cybersecurity training to their employees and volunteers.

36% have only partially implemented training programs, and **20%** offer no training at all. Given that human error is one of the leading causes of cybersecurity incidents, regular training is critical for raising awareness about threats like phishing, social engineering, and proper password hygiene. Phishing simulations, a practical tool for training, are conducted by only **36%** of NGOs (9 out of 25), with **44%** doing so partially and **20%** not conducting any simulations. This highlights a missed opportunity to prepare staff for common cyberattacks, further weakening the overall protective measures.

Data security also shows room for improvement. Only **32%** of NGOs (8 out of 25) have implemented encryption to protect sensitive data, with another **44%** partially compliant and **24%** lacking encryption entirely. This presents a major risk, particularly for NGOs that handle personal or confidential information, as unencrypted data is more easily compromised in the event of a breach. Moreover, only **36%** (9 out of 25) of NGOs are using secure channels, such as encrypted email or

file transfer protocols, to share sensitive data, while **44%** are partially compliant, and **20%** do not use secure channels at all. The lack of secure communication tools further exposes organizations to the risk of data interception during transmission, particularly in remote or collaborative work environments.

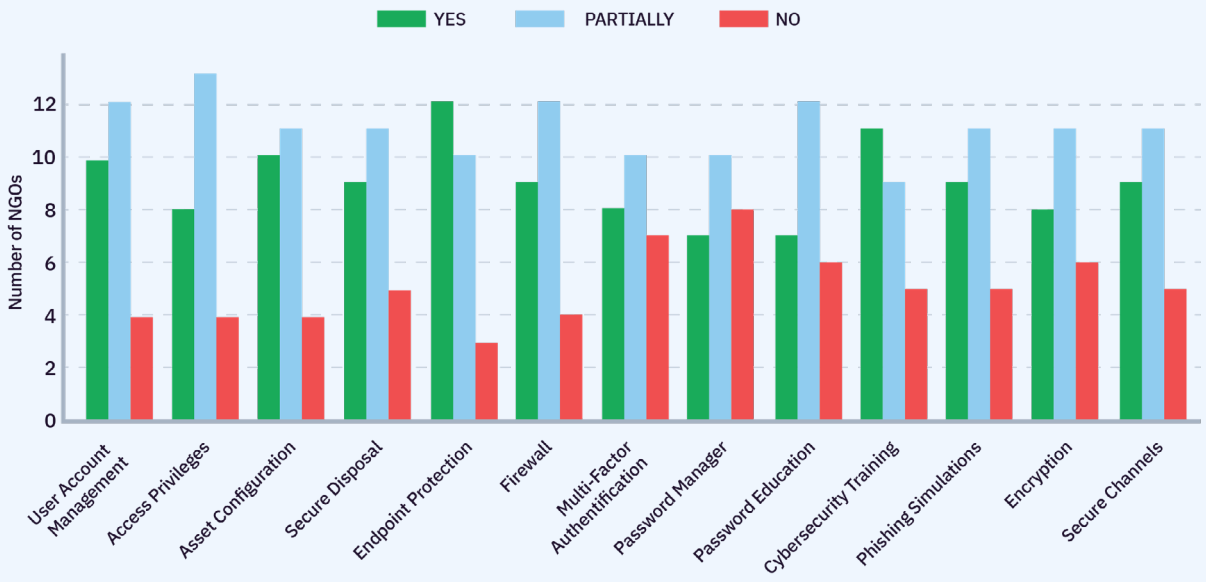


Figure 3: NGO Compliance Levels in Protect Category

In conclusion, the Protect category reveals a patchy cybersecurity landscape among NGOs, with a significant number of organizations struggling to fully implement protective measures. While some NGOs have made progress in areas like endpoint security and training, there are widespread gaps in access control, encryption, and multi-factor authentication. The mixed levels of compliance across the category suggest that NGOs require more support, training, and resources to strengthen their protective measures and reduce the likelihood of cyber incidents. The overall lack of full compliance in critical areas like user account management and asset configuration demonstrates the need for more comprehensive policies and procedures to bolster their defenses.

3.4 Detect

The **Detect** function, which focuses on the timely discovery of cybersecurity events through continuous monitoring and detection processes, shows significant room for improvement among the surveyed NGOs. When asked if they have the capability to monitor the dark web for potential data leaks, only **20%** (5 out of 25) of the NGOs responded that they have this capacity, while **44%** reported

partial implementation, and **36%** lack this capability altogether. This is concerning, as monitoring the dark web can help organizations identify stolen data or credentials that could be used in attacks against them. Without this capability, many NGOs may be unaware of potential threats lurking in the digital underground.

Log monitoring is another critical aspect of the Detect function, helping organizations track user and system activities to identify suspicious behavior. Only **28%** of NGOs (7 out of 25) reported having the capacity to monitor log activity.

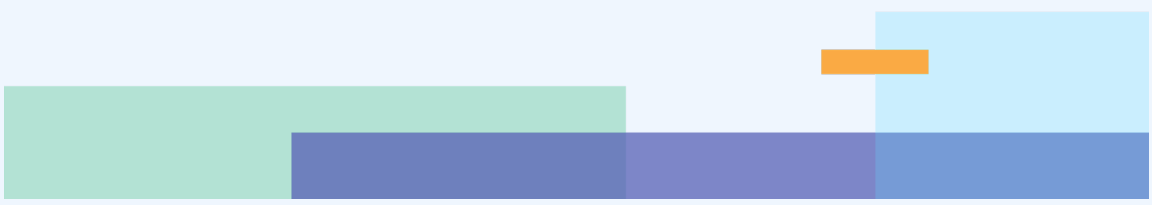
48% are partially compliant,

24% do not monitor log activity at all.

This lack of robust monitoring tools puts organizations at risk of delayed detection of intrusions or other security incidents, which could allow attackers to remain inside the network undetected for extended periods.

Finally, the use of cloud services is widespread among NGOs, but monitoring those services for security purposes is inconsistent. Only **32%** of the NGOs (8 out of 25) have a comprehensive list of the cloud services they use and actively monitor them, while **52%** are partially compliant, and **16%** lack this oversight entirely. Given the reliance on cloud-based tools for communication, file storage, and financial operations, not having a clear understanding of or monitoring for potential risks within these services can lead to vulnerabilities. This lack of visibility into cloud environments weakens the overall detection capabilities of NGOs.

In summary, the Detect function remains underdeveloped in many NGOs, with a majority of organizations only partially implementing monitoring processes or entirely lacking them. This gap in detection measures could allow cyber incidents to go unnoticed, exposing the organization to greater risk. Strengthening the ability to detect threats in real-time, particularly through enhanced log monitoring and cloud service oversight, would significantly improve the cybersecurity posture of these NGOs.



3.5 Respond

The **Respond** function, which focuses on incident response and the ability to mitigate the impact of cybersecurity events, is relatively underdeveloped among the surveyed NGOs. Only **28%** of organizations (7 out of 25) reported having a formal incident response plan in place, while **52%** have partial measures.

20% of the NGOs completely lack an incident response plan.

This is particularly concerning, as an incident response plan is essential for quickly addressing and mitigating the effects of cyberattacks. Without a structured plan, organizations may struggle to effectively manage incidents, leading to longer recovery times and potentially more significant damage to their operations.

The lack of comprehensive incident response capabilities is indicative of broader issues within the NGOs' overall cybersecurity preparedness. Organizations without a formal plan are at a higher risk of failing to contain and recover from security breaches. Those with only partial plans may not be prepared for more complex or large-scale incidents, leaving gaps in their response strategies.

In conclusion, the Respond function is one of the weakest areas for the NGOs, with only a minority fully equipped to handle cyber incidents. Developing and formalizing incident response plans should be a priority for these organizations to ensure they can effectively manage and recover from security events, minimizing damage to their operations and reputation.

3.6 Recover

The **Recover** function, which focuses on recovery planning and the ability to restore services after a cybersecurity incident, shows some promising developments but still leaves room for growth among the surveyed NGOs. When asked if they are backing up critical functional data, **40%** of NGOs (10 out of 25) reported full compliance, while **44%** indicated partial compliance, and **16%** did not have backup systems in place. While a good portion of organizations are backing up their data, there is still a notable number of NGOs that may be vulnerable to data loss, particularly in the event of a ransomware attack or hardware failure.

In terms of securely storing and verifying backups for restoration, **32%** of NGOs (8 out of 25) have comprehensive systems in place, while **52%** partially comply, and **16%** do not verify or securely store backups. This shows that while many organizations have some level of backup, they may not be fully equipped to ensure data can be recovered quickly and securely following an incident. Regularly testing backups is crucial to ensure that data recovery is seamless when needed.

Finally, when asked if they have a disaster recovery plan in place, **36%** of NGOs (9 out of 25) confirmed they have one, with another **48%** reporting partial compliance, and **16%** lacking such a plan. Having a well-defined disaster recovery plan is essential for NGOs to resume operations quickly after a cybersecurity incident.

28% of the NGOs reported having cyber insurance coverage, which can help mitigate financial losses following an attack.

While this is a positive step, the relatively low uptake suggests that many NGOs may not yet recognize the financial risks associated with cyber incidents.

In summary, the Recover function shows moderate levels of preparedness among NGOs, particularly regarding data backup and disaster recovery planning. However, the lack of comprehensive recovery strategies and regular testing of backup systems indicates that many organizations may still face challenges in quickly restoring operations after an attack. Improving backup verification processes and disaster recovery planning will be essential to enhance resilience.

In conclusion, the overall cybersecurity maturity of the NGOs surveyed reveals a landscape where many organizations are making progress but still face significant gaps in preparedness. While some NGOs have implemented basic cybersecurity practices, particularly in areas like data recovery and backup, there is a clear need for improvement across the board. Key functions such as Detect, Respond, and Protect show that many NGOs lack sufficient monitoring, incident response plans, and protective measures like multi-factor authentication and encryption. The disparity between organizations in their cybersecurity readiness is concerning, particularly given the reliance of these organizations on technology to support vulnerable communities. To improve resilience, NGOs need to focus on developing more robust governance policies, increasing employee training, and strengthening their detection and response capabilities to mitigate cyber threats effectively.

4. NGO vulnerabilities and incidents

In today's digital landscape, technology is an inevitable asset for every sector, including nonprofits, rather than a mere option. However, this dependence also exposes them to various vulnerabilities, threatening their safety and privacy. This section provides an in-depth analysis of the vulnerabilities affecting NGOs. The analysis covers critical areas such as network and infrastructure security, application and data security, and recorded vulnerabilities. The data is derived from open-source research and insights from a trusted network of partner organizations, offering a comprehensive view of the security landscape.

This research comprises two main sections, providing a complementary overview of the vulnerabilities NGOs may have in their current environments, and those they have been exposed to over the last year. Section 4.1 focuses on the cohort of NGOs onboarded into the programme, and section 4.2 looks at a wider group of Dutch NGOs.

4.1 Vulnerabilities & incidents affecting selected NGOs

This section provides an analysis of the infrastructure of the selected NGOs in the program, identifying a range of vulnerabilities affecting them.The scope of organizations was initially set to 30 in total. However, during the data gathering phase it was found that two of the organizations did not have sufficient information, due to their small web footprints, to obtain high confidence data regarding general security weaknesses.

Shadowserver attempts to track the most relevant threats and vulnerabilities that are currently exploited on the Internet, but the list is by no means exhaustive. Connect2Trust therefore not only notifies of vulnerabilities identified through passive scanning by organizations like ShadowServer and the Dutch Institute for Vulnerability Disclosures, but also those that can not be passively scanned. In total, Connect2Trust ended 2023 with 28,902 published CVEs, up over 15% from the 25,081 CVEs published in 2022.

On average, there were 79.18 CVEs published per day. October was the month with the most CVEs published, with 2,690 or 9.3% of all CVEs for the year. Tuesdays were the top publishing days, with 6,438 CVEs or 22.3% of all CVEs published. January 26th had the most CVEs published in a single day, with 348. This is relevant because for each vulnerability, the receiving NGO has to decide for themselves if the CVE applies to

them or their infrastructure provider.

Needless to say, the more infrastructure is used by an NGO for their daily work, the more CVEs have to be handled by their service provider. Quick actions on vulnerabilities, that can be identified through passive scanning, are especially important and require urgent action because a cyber actor may use the same techniques to identify and access an organization through this vulnerability. Luckily, research for this report found that much of the infrastructure used by the participating 28 NGOs is hosted by large external parties as shown in Figure 7 below for the NGOs that participated in this project.

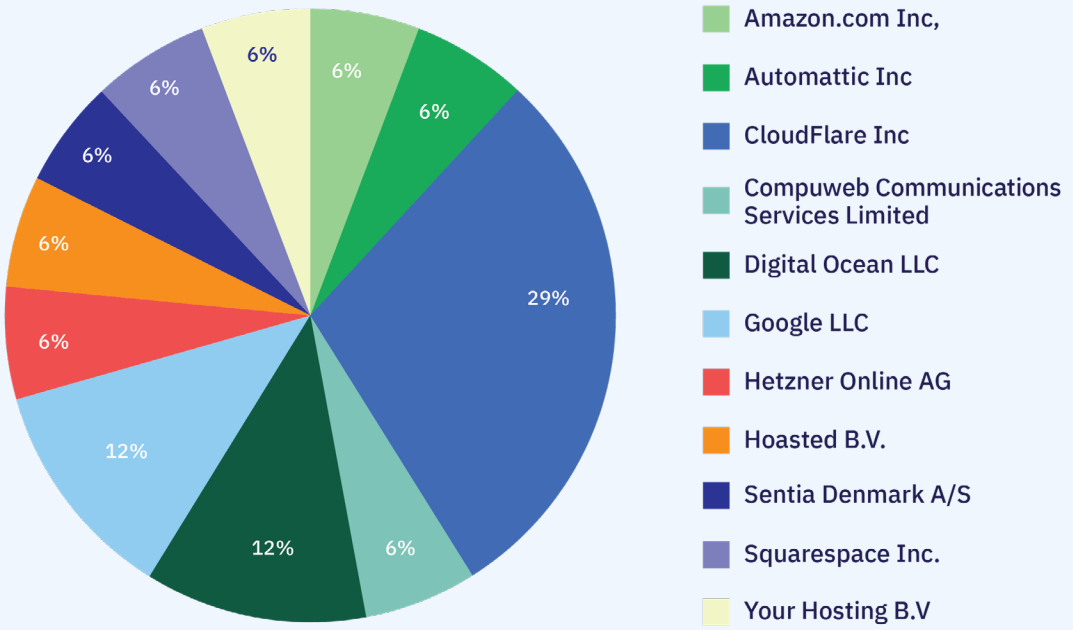


Figure 4: Overview of infrastructure used by participating NGO's

The largest third party for infrastructure in the diagram is **Cloudflare** Inc (29,4%). Together with DigitalOcean LLC and Google LLC (each 11,8 %), these three suppliers cover **53%** of the infrastructure of the participating NGOs. A possible explanation is that each of these three suppliers have specific programs for NGOs:

- Founded in 2014, Project Galileo is **Cloudflare**'s response to devastating cyber attacks launched against important yet vulnerable targets, like artistic groups, humanitarian organizations, and the voices of political dissent. Through Project Galileo, Cloudflare provides free, robust security to organizations that are the targets of DDoS and other cyber attacks, including journalists, social activists, and minority groups. Such organizations often face attacks from powerful and entrenched opponents, yet operate on limited budgets.

- **Google** helps nonprofits collaborate more effectively with smart, secure business apps like Gmail, Docs, Calendar, Drive, and Google Meet.
- **DigitalOcean**'s program for Nonprofits & Social Enterprises offers web hosting for nonprofits and social enterprises to grow their digital presence.

The additional benefit of these suppliers providing discounts to NGOs is that this also helps to reduce the attack surface of the NGOs. By using third-party infrastructure, a large portion of vulnerability management for infrastructure is left to the third party instead of the NGOs themselves. This is evident in the small number of IP addresses used by the participating NGOs: 65% use a single IP address, and 24% use two. Only two NGOs use more, with one having three IP addresses and another having four.

In addition to identifying the parties responsible for managing vulnerabilities, it is also useful to determine the expected timeline for reasonable vulnerability remediation. Due to confidentiality of the participating NGOs, the time it took each of them to resolve the issues outlined in the previous paragraphs, are not disclosed. Also, the limited number of 28 participating NGOs and their time to respond cannot be considered to represent the overall NGO community. However, to set a baseline in responding to vulnerabilities, Connect2Trust assessed the average and longest time to respond to a Shadowserver notification in 2023 amongst 1490 organizations in The Netherlands ranging from NGOs to multinationals.

Table 1 shows the notifications that were done by Connect2Trust based upon Shadowserver notifications received via the Dutch National Cyber Security Center in 2023.

Affected infrastructure	Percentage	Average # days to resolve	Longest # days to resolve
Compromised Website	66,67%	12 days	30 days
Event Honeypot Ddos AMP	0,53%	1 day	1 day
Event Sinkhole	1,59%	3 days	3 days
Open DNS	2,65%	1,7 days	2 days
Vulnerable Exchange Server	28,57%	7,7 days	23 days
Total	100%	7,8 days	

Table 1. Affected infrastructure and resolve of Shadowserver notifications in 2023 by Connect2Trust

Table 1 shows the majority of the incidents were related to compromised websites, followed by vulnerable Exchange servers. The latter is of lesser relevance to the NGOs, as they often use discount programs that include secured Exchange servers by the service providers. The other vulnerabilities relate to affected infrastructures that are often hosted by third parties as shown in Figure 7. This means that the response to a Shadowserver notification regarding infrastructure lies with either the NGO, its supplier, or both, depending on the contractual agreements that were made by the NGO. Table 1 also shows the average time to respond amongst those Dutch organizations and the longest it took to resolve each of them.

4.1.1 Network and infrastructure security

DNSSEC

During the time period of 9 August 2024 to 9 October 2024, DNSSEC was found to **not** be configured on the domains of **93%** (26/28) of the NGOS.

The Domain Name System (DNS) is used to resolve human readable hostnames to IP addresses so that users are directed to the appropriate website they request via their browser. It is possible for attackers to tamper with responses to DNS queries and redirect users to malicious websites. DNS Security Extensions (DNSSEC) help to prevent this. By adding cryptographic signatures to DNS Records, DNS servers can authenticate responses, reducing the chances of MITM attacks and spoofing.

Encryption (SSL certificates/configuration)

Issues with SSL certificates were found in **46%** (13/28) of NGOs, with **29%** (8/28) using self-signed certificates, and **29%** (8/28) having expired certificates on at least one domain in their infrastructure. SSL configuration issues were found in **79%** (22/28) of the NGOs, with **54%** (15/28) allowing deprecated and insecure encryption protocols including TLSv1.0, TLSv1.1, and SSLv3.

Secure Socket Layer is a protocol used for encryption. SSL certificates and configurations secure connections between resources like websites and requesting users' browsers. This helps prevent threats such as MITM attacks resulting from vulnerabilities introduced by outdated protocols or phishing attacks taking advantage of browser trust errors from expired or self-signed certificates to direct users to similar looking untrusted domains.

Internet exposed ports and services

Over the last year, **18%** (5/28) NGOs were observed to have a range of ports and services publicly exposed to the internet. Ports are common targets in attacks, with some being higher risk than others. Access to specific ports can provide direct access to internal systems if unsecured. Exposed services included Remote Desktop Protocol (MS RDP), MySQL databases, unencrypted file-sharing services, and insecure email protocols, all of which can be exploited by potential threat actors.

These exposures present serious risk. The National Institute of Standards and Technology (NIST) recommends that servers should be reviewed and any unnecessary services, application and network protocols should be disabled or removed as a preventative strategy. This includes FTP, email protocols, remote access.[6]

Exposed Ports Over the Last Year:

- **MS RDP:** 2 NGOs had Remote Desktop Protocol exposed.
- **MYSQL:** 2 NGOs had exposed MySQL databases.
- **SMTP without STARTTLS:** 1 NGO had an insecure email protocol exposed.
- **FTP without AUTH TLS:** 1 NGO had an encrypted file-sharing service exposed.

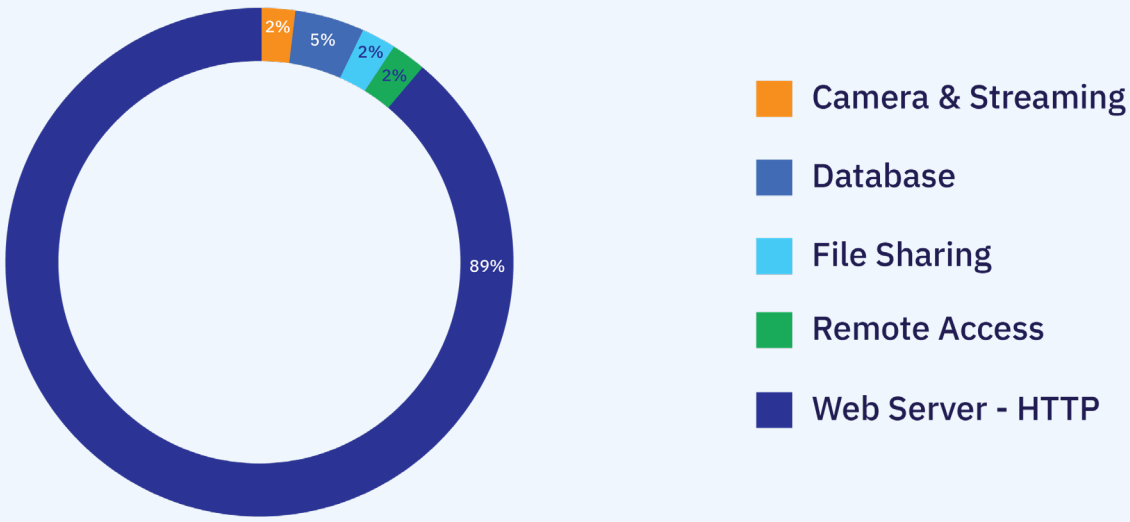


Figure 5: Ports and Services at high risk of compromise detected in NGOs

Exposures between August 2024 and October 2024:

- **HTTP Web Server Ports:** 12 NGOs (43%) have left the HTTP port (80) open. While many of these have an automatic redirect to HTTPS (port 443), 10 of these NGOs lack a firewall or similar security appliance to control access to port 80, which can expose sensitive server information. Although there may be reasons to keep the HTTP port open (e.g., for legacy systems), it should still be secured behind a firewall and configured not to reveal server version information.

- **MySQL Databases:** 2 NGOs (7%) had mysql database ports exposed to the internet. This may present risks of brute force attacks to gain access to sensitive data or malware deployment on vulnerable servers.

- **Camera Login Portal:** 1 NGO had a CCTV camera administration login portal exposed. This might present the risk of attacks such as credential stuffing to gain access to the device for surveillance purposes. If the device is unpatched, vulnerabilities may also be exploited to deploy malware.

- **MS RDP:** 1 NGO had a Microsoft Remote Desktop Protocol (MS RDP) exposed, which is used to access computers remotely over a network. Exposing this service poses the potential risk of attacks like brute forcing to gain access to the computer, or man-in-the middle (MITM) attacks to gain access to the unencrypted information transmitted over the network. The Cybersecurity & Infrastructure Security Agency (CISA) lists this as one of the high risk services commonly exploited[7] in cyberattacks, including ransomware campaigns[8].

- **FTP without AUTH TLS:** 1 NGO had FTP without AUTH TLS exposed, leaving their file transfer process vulnerable to threats. This is another service identified by CISA as commonly used in ransomware campaigns to gain access to sensitive data.

4.1.2 Application and data security

Email security was identified as a significant challenge for the reviewed NGOs with **82%** (23/28) experiencing issues with SPF and DKIM configurations. In 22 of these cases (**79%** of NGOs) the DKIM public keys were shorter than the recommended[9] length, which can weaken email security and increase vulnerability to spoofing. Furthermore, ineffectively configured or missing SPF records were identified at **25%** (7/28) of NGOs. In these cases the main issue was also that the configuration was not according to best practices, leading to problems like DNS lookup errors.

Web application security also presented a significant vulnerability with the majority of NGOs. **93%** (26/28) were identified as lacking recommended HTTP security headers on their web applications, leaving them potentially vulnerable to threats including injection and cross site scripting attacks. More than half of NGOs had no security headers at all, which significantly impacts their resilience to a wide variety of web based attacks.

Additionally, **79%** (22/28) of NGOs did not have properly configured CSFR (Cross-Site Request Forgery) tokens, making them more susceptible to cross-site request forgery attacks. Lacking correctly configured CSFR tokens exposes the organization to unauthorized actions carried out on behalf of legitimate users.

Compounding this issue, **46%** (13/28) of NGOs had improperly configured content security policy (CSP), which is intended to restrict the origin of resources like javascript. This could make them more vulnerable to threats including cross site scripting (XSS) attacks. In addition, **25%** (7/28) of the NGOs were identified as using web apps with dependencies on one or more javascript libraries with known vulnerabilities.

4.1.3 Known Vulnerabilities and Compliance

Between August and October 2024, 286 potential vulnerabilities were detected across the 28 NGOs analyzed. Of these, the Common Vulnerability Scoring System[10] (CVSS) scores show 27 as critical, 57 as high, 84 as medium and 6 as low severity vulnerabilities on the NGOs' internet facing infrastructure.

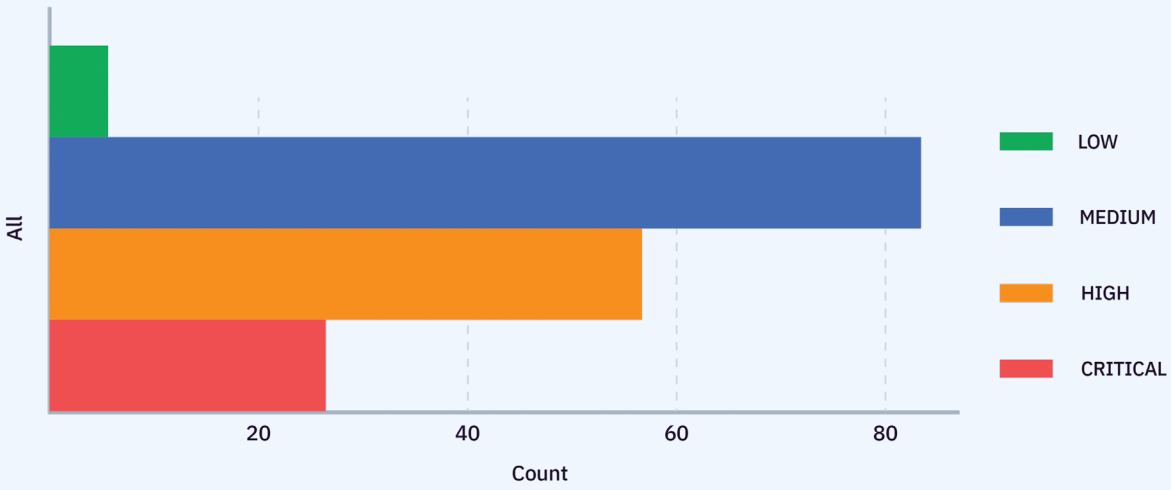


Figure 6: Number of CVEs detected in NGOs grouped by severity.

Of the critical vulnerabilities, **74%** are as a result of outdated Apache HTTP servers that may expose NGOs to increased risk to a range of threats, including remote code execution, information disclosure, and HTTP request smuggling attacks.

When software and systems are not routinely upgraded and patched, resulting vulnerabilities may expose organizations to a variety of attacks that leverage these weaknesses to exploit internet facing infrastructure. CISA emphasizes unpatched systems as being a key exploitable security weakness for actors looking to gain initial access to systems.[11]

Known Exploited Vulnerabilities

Based on the versions in the banners returned by the scanned hosts, at least **18%** (5/28) of the NGOs have potentially been exposed to Common Vulnerabilities and Exposures (CVEs) that appear on CISA's Known Exploited Vulnerabilities (KEV) list as a result of vulnerable software and configurations. This includes CVE-2021-40438[12] and CVE-2023-44487[13] affecting 11% and 7% of NGOs respectively. *(A version based assessment does not make definite assertions on the versions actually running and on whether they are vulnerable or not. For example, many Linux distributions issue patches for vulnerabilities without updating version numbers of the affected software.)*

	Vulnerability Name	CVSS	Details	Affected NGO's
CVE ID	CVE-2021-40438	9.0	Apache HTTP Server-Side Request Forgery (SSRF) (Affected: Apache HTTP Server version)	11% (3/28)
	CVE-2023-44487	7.5	HTTP/2 Rapid Reset Attack Vulnerability (Affected: F5 big ip firewall)	7% (2/28)
	CVE-2019-0211	7.8	Apache HTTP Server Privilege Escalation Vulnerability (affected: Apache HTTP Server version - Unix)	4% (1/28)
	CVE-2024-4577	9.8	PHP-CGI OS Command Injection Vulnerability (Affected: PHP version on Windows)	4% (1/28)

Table 2: CISA KEV listed CVE's present in NGO environments

Remediation status

The majority of detected unpatched vulnerabilities have remained in NGO environments unpatched for up to 2 years. The oldest vulnerability (POODLE (CVE-2014-3566)[14]) was first detected on NGO infrastructure 4 years ago (2020).

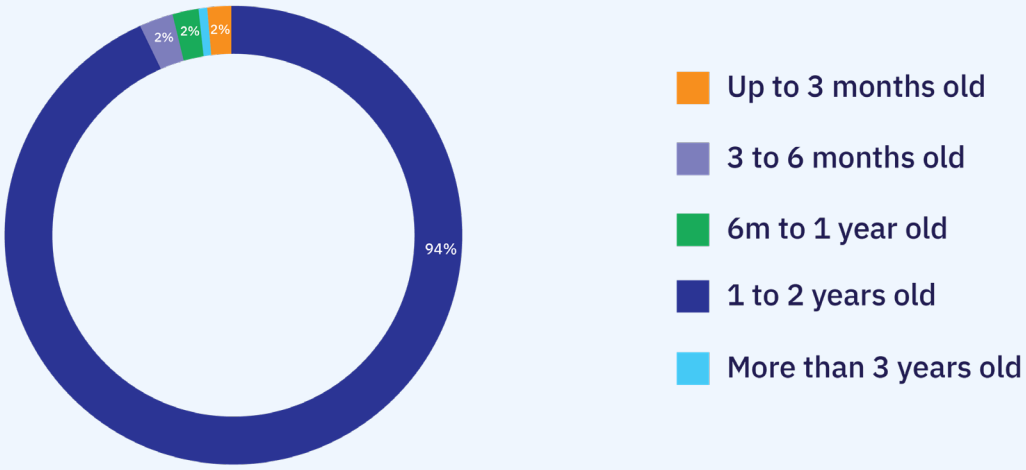


Figure 7: Remediation status

4.1.4 Incidents

Malware infected devices

No C2 communications were detected, across known sinkholes, during the period of August to October 2024 concerning the 28 NGOs. (See the 'Leaked Credentials' section below for indications of infostealer malware located within the NGO environments.)

However, Shadowserver found connections to its sinkholes in December 2023 of numerous malware families concerning the wider group of NGOs in the Netherlands, but assess this is likely due to the fact that the IP hosting a service of an NGO was also used as a VPN gateway by other tenants.

Shadowserver also observed many DNS queries to their sinkholes from multiple NGO hosted infrastructure of what would typically be DNS resolvers used for lookups, which may be indicative of potential infections on networks (or related networks). Note these may also come from researchers, shared hosting, security platforms or benign crawlers so effectively false positives.

Leaked credentials

Records	#Leaks Published	Affected NGOs	# Accounts
4,117	315	13	286

Between October 2023 and October 2024, **43%** (13/30) of the 30 NGOs had at least one stolen account with a password published on the darkweb. This includes sites such as onion domains and other hacker forums. In total, 4117 records were found in 315 leaked files or lists published on these forums. These records included 286 accounts in total across 13 NGOs. Of these, 51 accounts at 33% (10/30) of the NGOs were found to be for their own platforms.

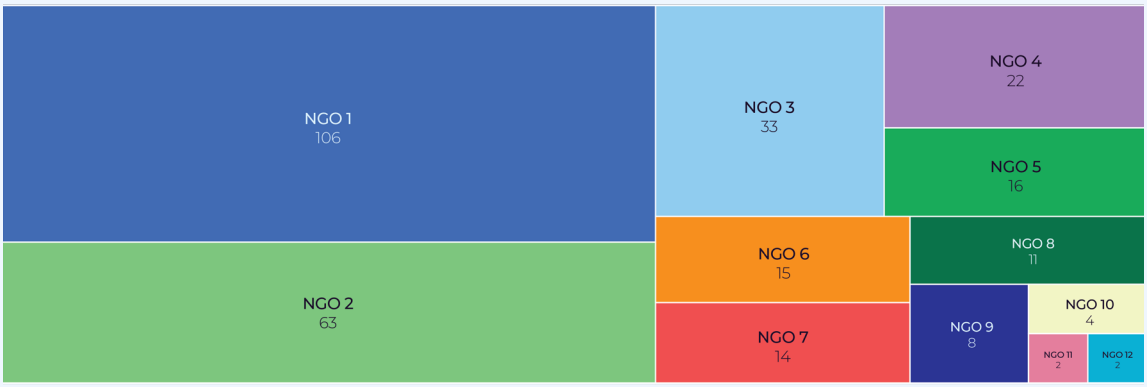


Figure 8: Distribution of unique accounts found by NGO domain

Data shows that not all the NGOs were equally affected by leaked accounts. The distribution of leaked accounts per NGO was not evenly spread, with over **57%** of the total number of accounts with passwords belonging to just two NGO's. Although it is not always possible to determine the origin of leaked credentials, analysis of the naming conventions of the leaked files can provide insights. Data analyzed between October 2024 and October 2024 shows that logs originating from infostealer malware were responsible for over **90%** of records linked to these NGO's.

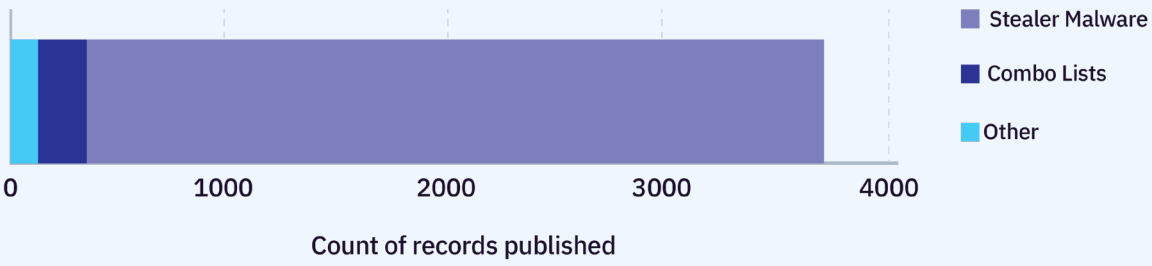


Figure 9: Leaked credential sources by type

Stealer malware was shown to be a major source of leaked credentials, accounting for 209 exfiltrated user accounts at 9 of the 13 affected organizations. This shows that in most cases, credential exposure was linked to the presence of malware in the NGOs' environments. In some cases it was possible to determine the type of stealer malware on the machines, such as Redline and Racoon Stealer, however this was not clear in most instances.

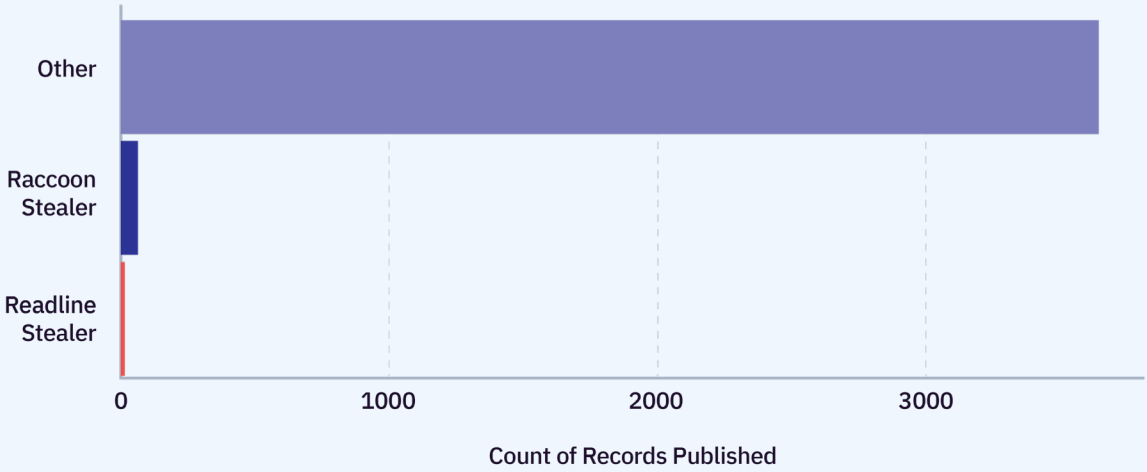


Figure 10: Types of infostealer malware identified from source logs

The presence of malware poses significant risks to the NGOs. Exfiltrated credentials, once shared or sold by malicious actors, may be used to gain unauthorized access to platforms and services containing sensitive data. The credentials could also be used to gain initial access to the internal NGO environments, conduct surveillance of emails, or launch phishing campaigns. Due to the built-in capabilities shared by various strains of stealer malware, such as Redline Stealer, other sensitive data and files may also be harvested from infected machines.

Public incidents

No publicly reported cyber incidents were located within the scope of this research. However, that does not necessarily confirm the absence of incidents. Consideration should be given to the potential for underreporting, as organizations may choose to handle incidents privately without public disclosure for a variety of reasons.

4.2 Expanded Analysis of Dutch NGOs

The analysis was conducted on 219 Dutch NGOs identified by the project partners for the period of September 2023 to September 2024. This approach was chosen to obtain a wider picture of the Dutch NGO ecosystem, beyond just the surveyed NGOs.

The primary goals are to analyze the Dutch NGO IT infrastructure (using domain names and public facing IP assets) from the point of view of the exposed attack surface to gain a better understanding of threats and potential attacks they may face as well as to get these organizations to subscribe to Shadowserver's free Threat Intelligence and Early Warning Services to help alert them of cybersecurity issues uncovered. This support in the form of alerts will continue after the project comes to an end, thus contributing to the strengthening of the cybersecurity of the subscribed organizations.

Dutch NGO domains and known IP ranges were validated by Shadowserver and Connect2Trust and subsequently checked against Shadowserver datasets.

The study was conducted for Dutch NGO assets from the period of September 2023 to September 2024 in order to obtain a longer term view of the landscape but at the same time keep the period reasonably current to get a more accurate snapshot of the situation. This is in part due to IP churn of organizations being analyzed, which means that the longer the period of investigation the more likely it is the IP was not actually used by the current organization under investigation. An attempt was made to offset this concern through the use of passive DNS records.

Any recorded Shadowserver findings relevant to the 219 Dutch NGOs were subsequently manually analyzed.

4.2.1 Analysis & Findings

The following analysis provides an overview of vulnerabilities which were observed by Shadowserver through passive scanning. Connect2Trust ensures, in collaboration with Shadowserver, that every vulnerability is notified to a registered NGO. However, not all vulnerabilities can be identified by passive scanning because security measures may prevent them from being detected externally, or because no scanning techniques have yet been developed to identify them through passive scanning. Shadowserver collects various daily internet scale datasets as a result of internet-wide scanning, sinkholing/disruption of malicious infrastructure (with the support of law enforcement agencies and/or private industry), sensor based and malware collection based observations.

The collected data allows Shadowserver to obtain “the big picture” of cybersecurity issues across the Netherlands which includes NGOs in the Netherlands as well. Specifically, Shadowserver checks daily for the following:

- Endpoint attack surface, broken down by the identified device vendor, type, as well as service
- Vulnerability exposure by current threat and attack vector
- Observed exploitation and other attacks
- Compromised systems
- Malware infections as seen in the sinkhole data
- Distributed Denial of Service (DDoS) attack activity
- Blocklisted resources

Not surprisingly, Dutch NGOs have a very small externally exposed digital footprint in terms of IT infrastructure. Compared to many other ecosystems, there is a relatively small number of exposed, vulnerable or compromised assets in the Dutch NGO sector. This is primarily linked to the low volume levels of ICT infrastructure per NGO organization which amount to public facing domains and associated single or small CIDRs (mostly web hosting and operations outsourced to anti-DDoS cloud providers, e.g. Cloudflare).

Nevertheless, some NGOs in the Netherlands were found with misconfigurations or vulnerabilities or using software that has a track record of vulnerabilities exploited by ransomware and/or state-sponsored threat actors:

1. Usage of mail/webmail systems such as Microsoft Exchange, RoundCube and Zimbra

At least 2 organizations were observed with exposed Exchange vulnerabilities for extended periods, in one case this, this included CVE-2022-41082[15] and CVE-2023-21529[16]. Another possible case is CVE-2024-21410[17]. This last instance is noted as possible because a mitigation may be in place that cannot be detected. Microsoft Exchange has a long history of critical vulnerabilities associated with it in the past.

At least 3 organizations were observed using Zimbra Collaboration Suite for mail services, though at the time of the scans no critical unpatched vulnerabilities were observed. Zimbra has had multiple frequent critical vulnerabilities associated with it in the past and is a frequent target of threat actors.

At least 2 organizations were observed using RoundCube for their webmail services (apparently hosted by 3rd parties). At the time of the scans, no critical unpatched vulnerabilities were observed. RoundCube has had a number of critical vulnerabilities associated with them in the past, and even if hosted by third parties they may result in theft of all email content. RoundCube is a frequent target of threat actors.

2. Exposed management panels (cPanel/Plesk etc)

At least 15 organizations were observed using cPanel/Plesk web panel services for managing their hosting. A potential security issue may arise if credentials for these panels are not managed securely and vulnerabilities are found in the software that can be exploited. A phpMyAdmin panel was found as well. Note that some of these issues may arise from the fact that the NGOs are using shared hosting providers and do not really have control of these assets in the first place.

3. Poor cybersecurity hygiene: Exposed git assets or basic HTTP authentication

In 1 case an NGO was exposed to .git directories. This can be potentially exploited by attackers if the git directories contain sensitive information, such as credentials. In the case of 2 organizations, usage of Basic HTTP authentication to some of their assets was observed (ie. passwords sent in cleartext to exposed assets).

4. Remote administration protocol exposure (RDP, VNC, SSH)

A number of NGOs used remote administration tools to access their services from the Internet. This included standard Secure Shell access (SSH). While SSH is inherently a secure mechanism for remote access, we observed a number that had known vulnerabilities (difficult to exploit in practice) such as CVE-2024-6387[18] ("regreSSHion") and CVE-2023-48795[19] ("Terrapin attack"). These should normally be patched (41 IPs found during the period of the study). It is recommended to enforce the use of public keys for access to SSH instead of password based authentication.

At least 2 organizations exposed RDP and 1 organization exposed VNC. Enabling remote access via such services requires special care as these are both popular attack vectors used by threat actors. It is recommended to filter external access by restricting external IPs connecting via access control lists/firewalls, ensuring regular patching of the service and employing MFA instead of passwords only.

5. Poor cybersecurity hygiene: Exposed SMB services (allowing for remote file access), MySQL, PostgreSQL and others

At least 2 organizations had exposed Windows SMB services (enabling file sharing), that are a known attack vector. These should not be exposed to the outside internet as this is a popular vector for botnet propagation and other internet attacks (such as the famous WannaCry worm or Petya ransomware).

9 IPs were found to have PostgreSQL exposed (at least 6 organizations).

32 IPs were found to have mySQL exposed (at least 22 organizations).

A plethora of other unnecessary services were found, such as MSMQ/SSDP/portmapper or telnet exposed in organizations, which is also poor cybersecurity practice as it constitutes an attack surface.

Note that some of these issues may arise from the fact that the NGOs are using shared hosting providers and do not really have control of these assets in the first place.

FTP services were found to be commonly exposed. While these may be a part of the services offered by NGOs and deemed a necessity for file transfer, it may be worthwhile re-assessing potential security implications.

6. DDoS (Distributed Denial of Service attacks)

During the period under investigation amplification DDoS attacks were observed against 52 IPs associated with the Dutch NGOs, meaning that multiple Dutch NGOs may have had experienced disruptions or downtime in their services.

7. Spammer list presence

It was found that a number of the mapped IPs were also listed on spam block lists. This may be due to the fact that many of these were co-hosted with other, unrelated infrastructure.

8. Multiple tenants per IPs used by NGOs

Multiple cases of NGOs were found to be hosting their websites as virtual hosts, sharing IPs and likely VPSes/VMs with other parties. In one case, an IP was likely found to be functioning as a VPN/proxy endpoint, connecting their clients to the internet. Some of these were infected with malware and connected to Shadowserver sinkholes. VPSes/VMs were typically exposing other assets, including some mentioned earlier here.

5. Recommendations

To enhance the cybersecurity resilience of Dutch NGOs, a multi-layered approach is recommended. This approach includes implementing governance structures, protective measures, detection capabilities, and additional strategies to safeguard infrastructure and reduce risk exposure.

1. Governance and Asset Management:

- Establish comprehensive cybersecurity governance structures, including cybersecurity policies, asset inventories, and regular risk assessments. Clear policies set standards and practices for staff, while asset inventories allow NGOs to track and secure digital and physical assets effectively.

2. Protection and Access Control:

- **Multi-Factor Authentication (MFA) and Password Management**: Implement MFA for critical systems and use password managers to securely store and enforce unique, complex passwords.

- **Secure Configuration and Disposal**: Ensure assets are up-to-date and configured securely, while establishing secure disposal processes for end-of-life hardware and software.

- **Encryption and Secure Communication**: Implement encryption for data at rest and in transit and use secure channels like encrypted email for sensitive data sharing.

3. Cloud and Hosting Security:

- Choose **dedicated VPS/VMs** instead of shared virtual hosts for cloud hosting to reduce risk.

- **Review and Disable Unused Services** on VPS/VMs at setup, as default services can increase the attack surface. You can do lookups with Shodan or Censys to verify these, and keep all infrastructure updated (Shodan and Censys are commercial tools, but allow also for free domain and IP lookup queries - with limitations).

- Consider switching to secure **cloud-hosted email platforms** instead of self-managed email services, which can be more challenging to secure.

4. Endpoint and Network Security:

- **Remote Administration Protocols**: Limit exposure of protocols like RDP and web-panel tools to the public Internet, ensuring they are patched regularly and have MFA enabled.
- **Implement ACL** (Access Control Lists): creating rules that specify which users or systems can access certain resources, allowing organizations to control network traffic and restrict unauthorized access to sensitive data and systems.

5. Detection and Monitoring:

- **Dark Web Monitoring and Log Analysis**: Invest in dark web monitoring to detect leaked credentials and implement continuous log analysis to identify unusual activities.
- **Cloud Service Oversight**: Maintain an up-to-date inventory of cloud services and monitor them for unusual behavior, given the reliance on cloud tools for collaboration and storage.

6. Incident Response and Recovery:

- **Incident Response Planning**: Develop a formal incident response plan with clear roles, procedures, and communication channels for managing incidents effectively. Regularly test these plans with simulated exercises.
- **Data Backup and Recovery**: Establish secure and regularly tested backups for critical data, and implement a disaster recovery plan to ensure continuity.

7. Training and Awareness:

- **Regular Cybersecurity Training**: Conduct regular cybersecurity training, including phishing simulations, for all staff and volunteers to build awareness of threats and good security practices.

8. DDoS Mitigation:

- Use free **anti-DDoS solutions** offered by large providers tailored for NGOs to mitigate potential DoS/DDoS attacks and reduce downtime.

9. Pre-Deployment Cloud Checks:

- Before deploying cloud infrastructure, check the provider's reputation on abuse handling (such as spam) to prevent potential email service interruptions or restrictions.

10. Recommended free security services:

- **Shadowserver**: NGOs are encouraged to subscribe to free Shadowserver services to gain awareness of possible vulnerabilities by monitoring their infrastructure's exposure.

- **CyberPeace Institute's CyberPeace Builders**: NGOs who are not yet part of the CyberPeace Institute's Cyber Peace Builders programme are encouraged to sign up for free cybersecurity support.

- **TechSoup Global Network Foundation**: TechSoup organizes workshops and webinars, providing awareness around products and technologies. Since 2021, Techsoup Netherlands distributed 275.000 products to its 16.000+ registered non-profit organizations and saved them a total of € 76.000.000. The initiative is supported through a grant from the Digital Trust Center (Ministry of Economic Affairs) and collaborates with SOCIALware and Stichting Donateursbelangen.[20]

By implementing these measures, Dutch NGOs can build a resilient cybersecurity framework, ensuring that their operations are safeguarded against emerging threats.

6. Glossary

1. **ACL (Access Control List):** A set of rules defining permissions for users or systems to access specific resources, controlling who can read, write, or execute.

2. **Anti-DDoS Solutions:** Services offered by large providers to protect organizations from Distributed Denial of Service (DDoS) attacks, which aim to disrupt digital services by overwhelming systems.

3. **Asset Inventory:** A detailed record of all digital and physical assets, essential for tracking and securing infrastructure within an organization.

4. **Cloud and Hosting Security:**

   - Cloud Service Oversight: Monitoring cloud-based tools to maintain security, detect abnormalities, and ensure compliance.

   - Dedicated VPS/VM: Virtual Private Servers or Virtual Machines used in cloud hosting, providing better security than shared hosts by isolating resources for each organization.

5. **Common Vulnerabilities and Exposures (CVE):** A list of known software vulnerabilities standardized to help organizations manage and address security risks.

6. **CyberPeace Builders Program:** An initiative by the CyberPeace Institute that offers free cybersecurity support specifically for under-resourced NGOs.

7. **Data Backup and Recovery:** Regularly backing up data and ensuring it can be restored quickly to prevent data loss in case of an attack.

8. **Data Encryption:** Encoding data to prevent unauthorized access, used for both data at rest and in transit to enhance information security.

9. **Dark Web Monitoring:** The practice of scanning dark web platforms for stolen or leaked data, which can help NGOs detect potential risks to their systems.

10. **Digital Trust Center (DTC):** A Netherlands-based organization focused on improving cybersecurity for businesses and nonprofits, leading projects like this cyber resilience study for NGOs.

11. DNSSEC (Domain Name System Security Extensions): Security measures that add cryptographic signatures to DNS records, helping prevent attacks that redirect users to malicious websites.

12. Firewall: A network security device or software that monitors and filters incoming and outgoing traffic based on predefined security rules.

13. FTP (File Transfer Protocol): A protocol for transferring files, which requires additional security measures like encryption to prevent unauthorized access.

14. GIT: is a popular software version control system used in software development.

15. Incident Response Plan: A defined set of procedures for managing and mitigating cybersecurity incidents to minimize potential harm.

16. Infostealer Malware: Malicious software designed to steal sensitive information, including login credentials, from infected systems.

17. Multi-Factor Authentication (MFA): A security measure requiring multiple forms of verification, such as a password and a text message code, to access systems securely.

18. MySQL: A commonly used database management system; ensuring secure configurations prevents unauthorized access to stored data.

19. NIST Cybersecurity Framework: A widely recognized set of standards and best practices developed by the National Institute of Standards and Technology for managing cybersecurity risks.

20. Passive Scanning: A non-intrusive security assessment method that gathers data about a network, such as open ports and services, without interacting directly with the system.

21. Phishing Simulation: A training exercise that exposes users to simulated phishing attempts, helping them identify and avoid real phishing attacks.

22. Remote Desktop Protocol (RDP): A protocol allowing remote access to Windows computers, often requiring strong security controls due to vulnerabilities that could allow unauthorized access.

23. Sender Policy Framework (SPF): An email authentication protocol that helps prevent email spoofing, thus protecting against phishing and spam.

24. Shadowserver: A nonprofit organization offering free cybersecurity services, including threat intelligence and infrastructure monitoring, helping NGOs detect vulnerabilities.

25. SSL Certificates: Digital certificates that verify a website's identity and encrypt data sent to the server, preventing interception by attackers.

26. Vulnerability Disclosure Policy: Guidelines for reporting and handling cybersecurity vulnerabilities, helping organizations respond quickly to minimize exploitation.

27. Zero Trust Architecture: A security model that requires strict identity verification for every user and device attempting to access resources, regardless of their network location.

7. Appendixes

Appendix 1: Survey questions

1. Identify (Focus on asset management, risk management, and governance)

- **Identify1:** Does your NGO have an up-to-date assets inventory of all your digital and physical assets?
- I**dentify2:** Are your NGO's critical functions for the delivery of essential services to vulnerable populations identified?
- **Identify3:** Does your NGO have a cybersecurity policy?
- **Identify4:** Does your NGO have a data protection policy?
- **Identify5:** Does your NGO have a vulnerability disclosure policy?
- **Identify6:** Does your NGO have an AI guidance policy?

2. Protect (Focus on access control, awareness and training, data security, and protection technologies)

- **Protect1:** Does your NGO ensure adequate management of user accounts of people who join or leave the organization?
- **Protect2:** Does your NGO follow a process to provide access privileges based on user roles and responsibilities?
- **Protect3:** Does your NGO ensure that all physical and digital assets are up-to-date and adequately configured?
- **Protect4:** Does your NGO securely dispose of hardware and software assets that are no longer needed/supported?
- **Protect5:** Are your NGO's endpoints (computers, laptops, mobile devices) protected with up-to-date security software against malware and other cyber threats?
- **Protect6:** Are your NGO's physical assets equipped with a virtual firewall?
- **Protect7:** Does your NGO use multi-factor authentication (MFA) for accessing sensitive data or systems?
- **Protect8:** Does your NGO use a password manager to securely store and manage passwords?
- **Protect9:** Does your NGO educate users to have passwords that are unique and complex?

- **Protect10:** Does your NGO provide cybersecurity training to its employees and volunteers?
- **Protect11:** Did your NGO conduct phishing simulations for all staff?
- **Protect12:** Does your NGO have the capacity to encrypt sensitive data?
- **Protect13:** Is your NGO using secure channels to share sensitive data?

3. Detect (Focus on detection processes, monitoring, and continuous security monitoring)

- **Detect1:** Does your NGO have the capability to monitor the dark web to identify any potential data leaks?
- **Detect2:** Does your NGO have the capacity to monitor logs activity?
- **Detect3:** Does your NGO have a list of all the cloud services it uses for monitoring and security purposes?

4. Respond (Focus on incident response and communications)

- **Respond1:** Does your organization have an incident response plan?

5. Recover (Focus on recovery planning and improvements)

- **Recover1:** Is your NGO backing up its critical functional data?
- **Recover2:** Are your NGO's backups stored securely and verified for restoration?
- **Recover3:** Does your NGO have a disaster recovery plan in place in the event of a cybersecurity incident?
- **Recover4:** Does your organization have cyber insurance coverage?

Note: While spyware and targeted mobile attacks (e.g., Pegasus-style threats) are critical risks, they are not included in this general assessment. Most NGOs benefit first from addressing foundational security measures, such as strong passwords and access control. For those facing advanced threats, support is available through our program once they join, allowing us to assist in a more secure, trusted setting.

Appendix 2 - research questions

Research Questions

NGOs

- What is the size of the NGO being targeted?
- What is the international footprint of the NGO? Which countries / regions do they operate in?
- What is the core mission behind the NGO?
- How is the NGO funded? [Interviews / Research]
- Does the NGO have cyber insurance?
- Does the NGO have a communications strategy in case of a cyberattack?
- What communications / reports were made before, during and after an attack?

Resilience

- How mature is the cyber security posture / hygiene of NGOs?
- How many NGOs have dedicated cybersecurity teams or experts?
- How many NGOs had relevant protection (Anti-virus, SSL Certificates, etc.) ?
- What can be done to improve the cybersecurity posture / hygiene of NGOs?

Threats

- What types of cyberattacks and operations have NGOs faced?
  - Ransomware
  - Data breaches
  - Fraud
  - Surveillance
  - ...
- What are the core outcomes / motivators behind these attacks?
  - Financial,disruption,dataexfiltration,destruction,disinformation
- How many NGOs have data (e.g. usernames / passwords) leaked online?
- How many NGOs have had access to their systems sold / advertised online?

- How many NGOs have been impacted by cyberattacks?
- Have these threats changed over time ?
- Are NGOs in certain sub-sectors / fields affected more than others?
- Which threat actors have been documented as targeting these NGOs?
  - What types of threat actors have been documented as targeting NGOs?
  - Are the motives behind these known?
    - Criminal / financial
    - Political
    - Ideological / activism
    - Other
- What types of malware were used to target NGOs?
- Are attacks on NGOs ever specifically targeted?
- How many of the attacks stemmed from human-error?
- How can we reduce the threat to NGOs from cyberattacks?

Vulnerabilities

- What are the cybersecurity risk ratings of these NGOs?
- How do these ratings compare to NGOs in other countries / regions?
- How have the risk ratings of these NGOs evolved?
- What types of vulnerabilities are being exploited during attacks?
- What vulnerabilities are currently left unpatched on NGOs systems?

Impact and harm

- How have NGOs been impacted by cyberattacks?
  - Financial
    - Ransom paid?
    - Reparation costs?
  - Operational
    - Leading to offlays
    - Services disrupted / duration
  - Reputational
  - Environmental
  - Legal

- Geographical
- Technical / digital / physical assets

- Have people / beneficiaries / employees been harmed as a result of cyberattacks on NGOs?
  - Psychological
  - Physiological
  - Societal
- Have people / beneficiaries of NGOs been impacted as a result of cyberattacks on NGOs?
  - Service disruption
  - Access to critical infrastructure or resources
  - Led to staff being laid-off
- What is the recovery time for an NGO following a disruptive cyberattack?

End Notes

[1] "Microsoft Digital Defense Report 2021," n.d. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2021.

[2] Bitsight. "Cyber Risk Management Solutions," n.d. https://www.bitsight.com/.

[3] Kaduu Cyber Threat Monitoring. "Kaduu I Dark Web Monitoring I Cybersecurity 2024." Kaduu CTI - DARK WEB MONITORING, October 22, 2023. https://kaduu.io/.

[4] Shadowserver. "The Shadowserver Foundation," n.d. https://www.shadowserver.org/.

[5] The insights are based on various large-scale datasets collected by Shadowserver, especially:

- Internet-wide scanning for exposed, misconfigured, abusable, vulnerable or compromised endpoints (whole of IPv4 - 3.7 billion addresses and hitlist based IPv6 scanning - over 1.7 billion addresses)
- Passive sensors, in the form of honeypots, in over 2000 locations worldwide
- Sinkholing data covering over 400 different malware types
- Large-scale malware collection (over 1 million samples unique by hash collected daily, totaling more than 1.9 billion unique by hash malware samples)

[6] Scarfone, Karen, Wayne Jansen, Miles Tracy, and National Institute of Standards and Technology. "Guide to General Server Security." NIST Special Publication 800-123, July 2008. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf.

[7] Cybersecurity and Infrastructure Security Agency CISA. "Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA," December 8, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a.

[8] Cybersecurity and Infrastructure Security Agency CISA. "Misconfigurations and Weaknesses Known to Be Used in Ransomware Campaigns | CISA," n.d. https://www.cisa.gov/stopransomware/misconfigurations-and-weaknesses-known-be-used-ransomware-campaigns.

[9] Rose, Scott, J. Stephen Nightingale, Simson Garfinkel, Ramaswamy Chandramouli, Advanced Network Technology Division, US Census Bureau, and Computer Security Division. "NIST Special Publication 800-177 Revision 1 Trustworthy Email." U.S. Department of Commerce, February 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf.

[10] "NVD - Vulnerability Metrics," n.d. https://nvd.nist.gov/vuln-metrics/cvss.

[11] Cybersecurity and Infrastructure Security Agency CISA. "Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA," December 8, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a.

[12] "NVD - CVE-2021-40438," n.d. https://nvd.nist.gov/vuln/detail/CVE-2021-40438.

[13] "NVD - CVE-2023-44487," n.d. https://nvd.nist.gov/vuln/detail/CVE-2023-44487.

[14] "NVD - Cve-2014-3566," n.d. https://nvd.nist.gov/vuln/detail/cve-2014-3566.

[15] "NVD - CVE-2024-41082," n.d. https://nvd.nist.gov/vuln/detail/CVE-2024-41082.

[16] "NVD - CVE-2023-21529," n.d. https://nvd.nist.gov/vuln/detail/CVE-2023-21529.

[17] "NVD - CVE-2024-21410," n.d. https://nvd.nist.gov/vuln/detail/CVE-2024-21410.

[18] "NVD - CVE-2024-6387," n.d. https://nvd.nist.gov/vuln/detail/CVE-2024-6387.

[19] "NVD - CVE-2023-48795," n.d. https://nvd.nist.gov/vuln/detail/CVE-2023-48795.

[20] Digital Trust Center (Min. Van EZ). "TechSoup Nederland," n.d. https://www.digitaltrustcenter.nl/samenwerkingsverband/techsoup-nederland.