

CC-DRIVER

Researching cybercriminality to design new methods to prevent, investigate and mitigate cybercriminal behaviour.

Policy Brief No. 12

April 2023

Who is this for?

This policy brief concerns shows the readiness of Civil Society Organisations (CSOs) and Small Medium Enterprises (SMEs) to withstand cyber-attacks.

Highlights

- 1 An online cybercriminality self-assessment questionnaire was created for Small Medium Enterprises (SMEs) and Civil Society Organizations (CSOs).
- 2 Respondents anonymously filled-in the questionnaire and received a free individual self-assessment that includes recommendations to prevent damages.
- 3 The overall statistics from the anonymous responses showed SMEs and CSOs are still vulnerable to ransomware.
- 4 A check list to protect against ransomware is presented.
- 5 The cybercriminality self-assessment questionnaire link is publicly available.





Cybercrime self-assessment questionnaire results

Cybercrime self-assessment questionnaire design

Cybercriminals often target small businesses for a variety of reasons, such as stealing sensitive data, holding data ransom for a large pay-out, or using the business's computer resources for illegal activities. Some common types of cyber-attacks, that small businesses may face, include phishing scams, malware infections, and ransomware attacks.

It is important for small businesses to take proactive measures to protect themselves against cyber threats. This includes implementing strong security measures such as firewalls, antivirus software, and data encryption, as well as educating employees on best practices for safe online behaviour. It is also important for small businesses to have a plan in place in case of a cyber-attack, including regular data backups and a strategy for responding to security incidents.

Cybersecurity helps to protect sensitive information such as personal data, financial data, and intellectual property from unauthorized access or theft. This information can be used for identity theft, fraud, or other malicious activities if not properly secured.

As part of CC-Driver project a cybersecurity self-assessment questionnaire was developed, so that SMEs and CSOs can assess their cyber security for free.

CC-Driver project delivered:

- The Self-Assessment questionnaire (SAQ) application to design questionnaires, track, and see statistics in a graphical mode. The SAQ application is independent of the content of the questionnaire itself. This tool can be used to define any type of self-assessment questionnaires, not only related to security. Many companies, not only those involved in the project, can use this tool.
- The content comprised of the questionnaire itself. The questionnaire contains 45 questions with predefined options for the answers. The questionnaire was structured around the following topics:
 - use of cybersecurity defences,
 - organisational measures,
 - cost-benefit considerations,
 - awareness of fundamental rights such as the rights to privacy,
 - protection of personal data and the free movement of persons.

The questionnaire was disseminated on-line and received 104 anonymous responses. Each SME or CSO received a comprehensive report with their security posture. The application doesn't store any data regarding the respondents. Each respondent has to download their report immediately after filling in.

The questionnaire was designed to give a unique view of the security posture. Each question contains guidelines based on the choice the respondent made. When the report is generated, the respondent receives an overall score and improvement recommendations based on the choices made at each question. The recommendations are very clear, and they specify industry best practices and provide





an explanation and alternatives. At the end the respondent will have a comprehensive report about their security posture.

The self-assessment questionnaire content was created taking into account the most common attack vectors. We have chosen the most well-known sources that publish attack vectors and the latest charts for 2021, as presented in Table 1.

| Attack vector | Source | Comments |
|---|-----------------------|---|
| A01:2021 – Broken Access Control | OWA21 | The OWASP top 10 details technical attacks against applications. They represent the top 10 most used attack vectors and might change over time. These categories show the technical methods used, though for some, the initial attack vector might be some sort of social engineering. For example, A01 – Broken Access Control might start with a phishing email where the attacker tricks the user to give-up his credentials. After that the attacker will use the credentials to log-in into the application. |
| A02:2021 – Cryptographic Failures | | |
| A03:2021 – Injection | | |
| A04:2021 – Insecure Design | | |
| A05:2021 – Security Misconfiguration | | |
| A06:2021 – Vulnerable and Outdated Components | | |
| A07:2021 – Identification and Authentication Failures | | |
| A08:2021 – Software and Data Integrity Failures | | |
| A09:2021 – Security Logging and Monitoring Failures | | |
| A10:2021 – Server-Side Request Forgery (SSRF) | | |
| Highly targeted phishing campaigns | SAN21 | SANS proposes a mix of social attacks (phishing, mobile), with pure technical attacks for the others. Mobile devices started to be attacked because of the 2FA codes used for authentication. Most mobile attacks consist in tricking the user to reset their own password by pressing the reset link on an unsolicited SMS or SIM swapping. |
| Finding vulnerabilities in software (including security products) | | |
| Mobile device attacks | | |
| Persistent and Promiscuous Web Agents | | |
| Email attacks | PRF21 | The state of the phish report contains only social attacks that refer to how phishing campaigns are being disseminated. |
| Social media attacks | | |
| Smishing attacks | | |
| Vishing attacks | | |
| USB drops | | |
| Compromised credentials | BAL19 | |
| Weak and stolen credentials | | |





| Attack vector | Source | Comments |
|-----------------------------------|-----------------------|--|
| Malicious insiders | | The Balbix report details the most common technical attack vectors, which can be divided into the same categories identified by OWASP. |
| Missing or poor encryption | | |
| Misconfiguration | | |
| Ransomware | | |
| Phishing | | |
| Trust relationships | | |
| Zero-day vulnerabilities | | |
| Brute force attacks | | |
| DDoS | | |
| Denial of Service (DDoS and DDoS) | VER21 | Verizon lists the most prevalent technical attacks and separately social engineering. |
| Lost and stolen assets | | |
| Miscellaneous errors | | |
| Privilege misuse | | |
| Social engineering | | |
| System intrusion | | |
| Basic web application attacks | | |
| Everything else | | |
| Phishing | SSC21 | This report lists, besides the most common application attack vectors, malicious insiders and remote workforce. These two things can help an attacker succeed with the common attack vectors. A malicious insider might install malware himself or use inside information to create a very credible phishing campaign. The remote workforce is more susceptible to phishing campaigns and needs more training. |
| Malware | | |
| Ransomware | | |
| Denial of Service (DDoS) Attacks | | |
| Compromised Credentials | | |
| Malicious Insiders | | |
| Misconfiguration | | |
| A Lack of Encryption | | |
| Web Application Attacks | | |
| Your Remote Workforce | | |
| Compromised Credentials | UPG21 | |
| Weak Credentials | | |





| Attack vector | Source | Comments |
|---|-----------------------|---|
| Malicious Insiders | | The Upguard post details the most common technical attack vectors, which can be divided into the same categories identified by OWASP. |
| Missing or Poor Encryption | | |
| Misconfiguration | | |
| Ransomware | | |
| Phishing | | |
| Vulnerabilities | | |
| Brute Force | | |
| Distributed Denial of Service (DDoS) | | |
| SQL Injections | | |
| Trojans | | |
| Cross-Site Scripting (XSS) | | |
| Session Hijacking | | |
| Man-in-the-Middle Attacks | | |
| Third and Fourth-Party Vendors | | |
| Supply chain compromise | DIG21 | Dig8ital blog post lists one the hardest to catch methods of attack supply chain compromise. This is a method that compromised the supply chain of the intended target using common technical attack vectors. |
| Malware | | |
| Ransomware | | |
| Phishing | | |
| Threats from within | | |
| Malware | RAP21 | The Rapid7 post details the most common technical attack vectors, which can be divided into the same categories identified by OWASP. |
| Phishing | | |
| SQL Injection Attack | | |
| Cross-Site Scripting (XSS) | | |
| Denial of Service (DoS) | | |
| Session Hijacking and Man-in-the-Middle Attacks | | |
| Credential Reuse | | |

Table 1 Attack vector sources





Campaign statistics

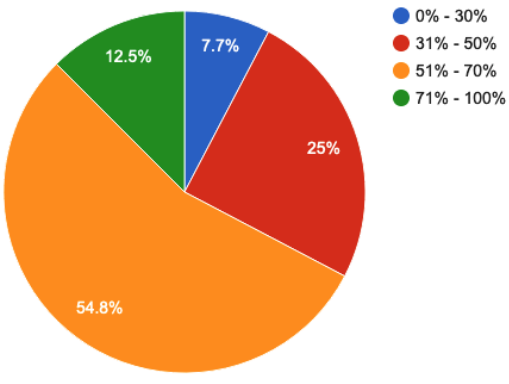
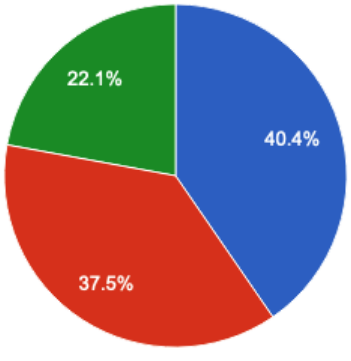
The SAQ application allows for the creation of campaigns. A campaign uses one questionnaire and can be disseminated to a group of people using the unique link associated with the campaign. Using the link, the respondents can fill-in the questions anonymously, without needing to create an account in the application.

The table below details the overall campaign results:

| Item | Comments |
|--|---|
| Campaign name | Self-assessment for SMEs and CSOs |
| Campaign description | Vulnerability Assessment questionnaire SMEs and CSOs |
| No of responses | 104 |
| Campaign start date | June-2022 |
| Maximum score | 10000 |
| No of questions | 45 |
| Average campaign score | 5524.76 (55.25%) |
| Maximum score obtained by a respondent | 9800.0 (98.00%) |
| Minimum score obtained by a respondent | 900.0 (9.00%) |
| No of responses with score over 70% | 13 (12.50%) |
| No of responses with score below 50% | 33 (31.73%) |
| No of questions where more than 50% of people obtained a score below 50% | 10 |
| Questions where more than 50% of people obtained below 50% | <p>Do you have any services enabled that are accessible externally from your internet routers or hardware firewall?</p> <p>Do you review who should have administrative access on a regular basis?</p> <p>Do you have automatic notifications when a user logs-in from a different location then the one he usually does? (Example: he usually logs-in in from US and now suddenly logs-in from China)</p> <p>Do you have automatic notifications and monitoring for privilege escalation (example: when a command is run with "sudo" or administrative account)?</p> <p>Are all of your computers, laptops, tablets and mobile phones protected from malware?</p> <p>Do you run automatic vulnerability scans?</p> |





| Item | Comments | | | | | | | | | | |
|---|---|-------------|------------|----------|-------|-----------|-------|------------|-------|------------|-------|
| | <p>Do you regularly perform scans to identify unauthorized or rogue wireless access points?</p> <p>Have you deployed IDS (Intrusion Detection System) on the wireless network of your organisation?</p> <p>Have you implemented or deployed a DLP (Data Loss Prevention) system?</p> <p>Have you deployed a honeypot system on your internal network as a proactive measure to detect an intruder?</p> | | | | | | | | | | |
| Overall response distribution | <p>Overall response score</p>  <table border="1"><thead><tr><th>Score Range</th><th>Percentage</th></tr></thead><tbody><tr><td>0% - 30%</td><td>7.7%</td></tr><tr><td>31% - 50%</td><td>25%</td></tr><tr><td>51% - 70%</td><td>54.8%</td></tr><tr><td>71% - 100%</td><td>12.5%</td></tr></tbody></table> | Score Range | Percentage | 0% - 30% | 7.7% | 31% - 50% | 25% | 51% - 70% | 54.8% | 71% - 100% | 12.5% |
| Score Range | Percentage | | | | | | | | | | |
| 0% - 30% | 7.7% | | | | | | | | | | |
| 31% - 50% | 25% | | | | | | | | | | |
| 51% - 70% | 54.8% | | | | | | | | | | |
| 71% - 100% | 12.5% | | | | | | | | | | |
| Example of distribution of responses per question | <p>Responses to Question: Phishing is a form of cyber-attack usually by email which aims to trick the user into installing malware or following a link and providing personal information. Do you provide separate training regarding phishing?</p>  <table border="1"><thead><tr><th>Score Range</th><th>Percentage</th></tr></thead><tbody><tr><td>0% - 30%</td><td>40.4%</td></tr><tr><td>31% - 50%</td><td>37.5%</td></tr><tr><td>71% - 100%</td><td>22.1%</td></tr></tbody></table> | Score Range | Percentage | 0% - 30% | 40.4% | 31% - 50% | 37.5% | 71% - 100% | 22.1% | | |
| Score Range | Percentage | | | | | | | | | | |
| 0% - 30% | 40.4% | | | | | | | | | | |
| 31% - 50% | 37.5% | | | | | | | | | | |
| 71% - 100% | 22.1% | | | | | | | | | | |



Conclusions – Results interpretation

We have noticed an improvement in the overall security for SMEs and CSOs. Even if the overall score was close to 56%.

Most companies **excel** now in areas where a few years were problems like:

- 85.6% of respondents mention that their security policy specified a mandatory password composition of: lower case, upper case, symbols, and numbers
- 67,3% of respondents analysed and created a remote work policy as response to COVID-19
- 99% of respondents have firewall between organisation's internal network and internet
- 94,2% of respondents mentioned that their change the default password for devices such routers and for the admin account for applications
- 89,4% of respondents have set in place an emergency account revocation procedure in case of compromise
- 84,6% of respondents installed firewalls on laptops
- 85,6% of respondents have disable "auto-run" on all systems

There are still some **troubling** areas that need improvement like:

- Companies should implement automatic notifications for at least:
 - when a user logs-in from a different location then the one he usually does (Example: he usually logs-in in from US and now suddenly logs-in from China)
 - when a command is run with "sudo" or administrative account – this prevents privilege escalation
- Install anti-virus and anti-malware on everything; on any device the company owns including mobile devices
- Implement IDS at least for critical systems
- Run automatic vulnerability scans at least twice a year for critical systems
- Regular reviews of who has administrator access
- Asset management system – many respondents still use excel for asset management
- The vast majority of respondents don't apply critical security patches in
- A detailed backup policy that includes remote backups and tests – most respondents admitted making automatic backups without testing them or saving the backups on another device, also many respondents admitted that they never had a full restore test.

The most stringent and troubling problem we have identified is the susceptibility of respondents to malware, specifically to ransomware.

This ransomware problem can be solved by implementing the following steps:

- Implementing a clear business continuity plan that contains among other things:
 - A clear chain of command – who's is responsible for what. This should include a core team, with names, updated phone numbers.
 - Define clear backup schedule, locations (including remote locations)
 - Define parameters for backup test
 - Define the date and plan for at least one backup / restore exercise





- Educate employees run tabletops and tests on procedure
- Use two factor authentication for at least critical systems
- Implement a specialised asset and software management system – you can't protect that what you don't know you have.
- Run critical security patches within 14 days of release
- Implement automatic notifications for:
 - Anomalous log-in from a different location than the one expected
 - and privilege escalation
- Implement IDS
- Reduce your company's footprint – only enable what you need, disable any unnecessary services to access the internet. Be careful with internet printers.
- Automatic vulnerability scans for your entire network and for critical applications
- Make regular backups: full backups and differential backups
- Store backups in a remote location
- Run at least one full restore from backup test
- Implement network segregation
- Implement the least privilege access and segregation of duties

As part of our mission to provide long lasting results, even after the project ends, we have made available the questionnaire available for the public. [The vulnerability self-assessment questionnaire is available for free](#) for anyone to make an assessment of their company security posture.

The respondents must save the individual self-assessment report that contains improvement recommendations because the application doesn't collect any personal data, so their response can't be identified in the data base.

References

- [BAL19] Balbix, Most Common Cybersecurity Attack Vectors and Breach Methods, https://www.balbix.com/app/uploads/eBook_Most-Common-Attack-Vectors-and-Breach-Methods.pdf
- [DIG21] Dig8igital, The most common cyber-attacks vectors of 2021, <https://dig8ital.com/resources/library/the-most-common-cyber-attack-vectors-of-2021>
- [OWA21] OWASP, OWASP Top 10 Security Risks & Vulnerabilities, https://owasp.org/Top10/A00_2021_Introduction/
- [PRF21] Proofpoint, State of the Phis 2021 report, <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
- [RAP21] Rapid7, Common Types of Cybersecurity Attacks, <https://www.rapid7.com/fundamentals/types-of-attacks/>
- [SAN21] SANS, Top new attacks and threats report, <https://www.sans.org/blog/sans-2021-threat-report/>
- [SSC21] Security Score Card, Common cyber-attack vectors in 2021, <https://securityscorecard.com/blog/common-cyber-attack-vectors>
- [UPG21] Upguard, What is an Attack Vector? 16 Common Attack Vectors in 2021, <https://www.upguard.com/blog/attack-vector>
- [VER21] Verizon, Data Breach Investigations Report 2021, <https://www.verizon.com/business/resources/reports/dbir/>

