Boosting your Organisation's Cyber Resilience

Joint Publication 22-01

Executive summary

Based on the continuously increasing threat level ENISA, The EU Agency for Cybersecurity, and CERT-EU, the CERT of all the EU institutions, bodies and agencies, strongly encourage all public and private sector organisations in the EU to apply, at a minimum, the cybersecurity best practices hereunder.

ENISA and CERT-EU remain confident that, by applying this set of recommendations in a consistent, systematic manner, organisations in the EU will be able to substantially improve their cybersecurity posture and enhance their overall attack resilience.

Best practices

The following best practices may complement but do not replace guidance issued by your national or governmental cybersecurity authority. They are provided in no particular order. Organisations should prioritise their actions according to their specific business needs.

1. **Ensure remotely accessible services require multi-factor authentication (MFA).**

   These include, but are not limited to, VPN services, external facing corporate portals (extranets) and email access (e.g. OWA or Exchange Online). If possible, avoid using SMS and voice calls to provide one-time codes and consider deploying phishing resistant tokens such as smart cards and FIDO2 (Fast IDentity Online) security keys.

2. **Ensure users do not re-use passwords, encourage users to use Multiple Factor Authentication (MFA) whenever supported by an application (on social media for instance)**

Threat actors often compromise organisations by performing credential stuffing attacks. These attacks use credentials obtained from previous data breaches, such as leaked user names and passwords, against another unrelated service. These attacks are made possible because users tend to re-use the same username/password combination. Users are therefore encouraged to never reuse a password. In addition, users are advised to use trusted leak checkers to see if their personal email addresses are present in any known data breach and to change immediately any compromised password on the relevant websites and/or applications. The use of a corporate password manager should be encouraged whenever possible.

3. **Ensure all software is up-to-date**

   Updates addressing known vulnerabilities should be prioritised. Reengineering vulnerability management processes is also needed and recommended in order to deploy high and critical severity patches as quickly as possible.
   Ensure all actions related to patching of endpoints and servers have been completed (e.g. system reboots).

   Remember to strongly encourage your users to patch their personal systems at home and as regularly as possible (e.g. computers, smartphones, tablets, connected devices like TV sets, videogame consoles, home routers, etc.).

4. **Tightly control third party access to your internal networks and systems**.

   This will improve your ability to prevent and detect potential attacks should a third party be compromised and used as a beachhead to breach your organisation.

5. **Pay special attention to hardening your cloud environments** before moving critical loads to the Cloud.

   Use the strong security controls available on cloud platforms and separate cloud system management from on-premise system management to ensure threat actors cannot jump from one environment to the other because of discrepancies in security controls.

6. **Review your data backup strategy** and use the so-called 3-2-1 rule approach

   Addressed to organisations, the rule consists in keeping three complete copies of their data, with two of them locally stored but on different types of media, and at least one copy stored off-site. Your organisation's backup strategy should be fully aligned with your business needs by setting explicit recovery time (RTOs) and recovery point objectives (RPOs).

   Ensure access to backups is controlled, limited and logged.
   Confirm your restore procedures are well documented and tested regularly.

   Given the proliferation of ransomware attacks, it is strongly recommended to increase the frequency of backups for critical data. The latest storage technologies facilitate rapid backups of almost any data set in a matter of minutes.

   Users should be trained to save data only on storage devices allowed by your cybersecurity policy or, if applicable, on the corporate cloud storage and not on their workstations. In addition, you should ensure that your backup software itself is up to date.

7. **Change all default credentials** and disable protocols that do not support multi-factor authentication or use weak authentication (e.g. cleartext passwords, or outdated and vulnerable authentication or encryption protocols).

8. **Employ appropriate network segmentation** and restrictions to limit access and utilise additional attributes (such as device information, environment and access paths) when making access decisions.

9. **Conduct regular training** to ensure that IT and system administrators have a solid understanding of your organisation's security policy and associated procedures.

Vigilantly monitoring the misuse of sysadmin tools can help you prevent attackers from breaching your network and moving laterally.

10. **Create a resilient email security environment** by enabling antispam filtering, adding a secure email gateway configured to automatically follow field-tested policies and playbooks designed to prevent malicious emails from reaching mailboxes.

11. **Organise regular cyber awareness events** to train your users on common phishing techniques (e.g. identifying spoofed/suspicious messages) and the effects of phishing attacks.

12. **Protect your web assets from denial-of-service attacks.**

    Using a CDN (Content Delivery Network) will expand your web assets' footprint across multiple servers or use the native high-availability features of cloud platforms.

    Automate the disaster recovery runbooks for on-premise systems and ensure that you can move workloads to the disaster recovery site with a single click if possible.

13. **Block or severely limit internet access for servers** or other devices that are seldom rebooted, as they are coveted by threat actors for establishing backdoors and creating persistent beacons to Command and Control (C2) infrastructure.

14. **Make sure you have the procedures to reach out and swiftly communicate with your CSIRT.** Contact details can be found on the matching websites available via https://csirtsnetwork.eu/.

Publications

CSIRT publications

For best practices issued by your relevant CSIRT, please refer to their local websites.

CERT-EU Security Advisories

You may also refer to CERT-EU's Security Advisories for information about critical vulnerabilities.

ENISA publications

You may also refer to the following ENISA publications for additional information:

- ENISA Threat Landscape 2021, issued in October 2021.
- Guidance on Secure Backups, including the 3-2-1 rule, issued on 1 September 2021.
- Proactive Detection, section on monitoring, pp. 12 - 18, issued on 26 May 2020.
- Proactive detection – Measures and information sources, issued on 26 May 2020.
- How to set up CSIRT and SOC, issued on 10 December 2020.
- Standards and tools for exchange and processing of actionable information, issued on 19 January 2015.

History

14/02/2022 - 1.0 Initial Release