ERRORS, MISCONFIGURATIONS AND POOR SECURITY PRACTICES

Co-funded by the European Union

ESCAPE. *Preparing healthcare professionals for cyberattacks*
Project No.2023-1-ES01-KA220-VET-000151536

Partners

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Weser

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

Co-funded by the European Union

FACTSHEET – ERRORS, MISCONFIGURATIONS AND POOR SECURITY PRACTICES

1. Definition

They are internal vulnerabilities and unintentional human errors, such as misconfigurations or inadequate security practices, that can lead to security incidents, including data leaks1. Some examples are weak passwords, excessive user privileges, failure to apply patches, or neglecting encryption.

2. General importance

These problems are relevant because they allow criminals to compromise systems without effort. Most data leaks are caused by human error or poor configuration, which highlights the importance of robust internal cybersecurity practices and human factors in the overall security posture.

According to IBM2, human errors account for more than 20% of all breaches, costing organisations millions. Misconfiguration can also cause long-term exposure. For example, a server that isn't set up correctly can leak sensitive data for months before anyone notices. Therefore, correcting errors and ensuring that safe procedures are followed are both crucial aspects of cybersecurity for companies.

3. Importance in health and care, and impact in quality of care

Errors and misconfigurations in healthcare have a direct impact on patients' safety, privacy, and quality of care. When affecting medical devices, it can cause incorrect drug dosing, delayed alarms, or malfunctioning monitoring services.

Sensitive information from patient records may also be made public, which would violate GDPR and HIPAA regulations and erode public confidence in healthcare professionals.

Ultimately, poor cyber hygiene, like outdated software or improper user permissions, can allow attackers to infiltrate networks, disrupt hospital operations, delay procedures, and reduce the quality of care. The SingHealth breach in Singapore (2018) involved misconfigurations in network access controls, compromising personal health data of 1.5 million patients3.

4. What can I do as a healthcare professional?

- Follow organisational security guidelines and protocols.
- Use secure access by logging in via authorised hospital cloud platforms with strong passwords and two-factor authentication.
- Immediately report any unusual system behaviour or potential misconfigurations to the IT team.
- Take part in cybersecurity training and keep up with how to respond to incidents and the impact of patient data protection to reduce human error.

5. More information

5.1 Learning Materials

- Cybersecurity for your sector (JGT-1)
- Sequential videos for general topics about cybersecurity (JGT-2)
- Web seminars about key aspects of cibersecurity (JGT-3)
- Awareness kit about cibersecurity in enterprises (JGT-4)
- Cybersecurity for SMEs & self-employed (JGT-6)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- Cibersecurity training from National Cryptographic Centre of Spain. Requires National login (JGT-8)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- Educational project on safe and responsible digital use. (IST-41)
- IT Security Requirements and Protective Measures – Tips and Practical Examples (BBS-42)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- A Critical Review on Cybersecurity Awareness Frameworks and Training Models (PRAMMER-30)
- An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context (PRAMMER-31)
- Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that (PRAMMER-32)
- Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview (PRAMMER-33)
- A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia (PRAMMER-34)
- Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach (PRAMMER-35)

5.2 Relevant Videos

The webinar discusses how medical errors in critical care are often predictable and preventable, emphasising the importance of awareness, system improvements, and patient safety practices to reducing harm.

[Webinar] Medical Error, Harm and Patient Safety
https://youtu.be/VB7MsPH_sG8?si=rNpZrED9yTYm7oyu

5. 3 Relevant Links

This article explains how a configuration error in Ireland's COVID-19 vaccination portal (which was built on Salesforce) gave registered users access to internal HSE documents and sensitive personal data belonging to over a million people.

https://www.darkreading.com/cyberattacks-data-breaches/nhs-breach-hse-bug-expose-healthcare-data-british-isles

Misconfigurations made thousands of DICOM imaging servers publicly accessible, exposing patient names, birthdates, disease information, and medical images, affecting systems in multiple countries.

https://www.sharitsec.eu.org/2023/09/critical-dicom-server-misconfigurations.html

Many medical devices have hard-coded credentials or don't have the right authentication, which makes them easy targets for attacks like denial-of-service or tampering.

https://www.csoonline.com/article/568861/insecure-configurations-expose-ge-healthcare-devices-to-attacks.html

6. Bibliography

ENISA threat landscape: Health Sector - CYBIL portal. (2023, 5 julio). Cybil Portal.

https://cybilportal.org/publications/enisa-threat-landscape-health-sector/

Cost of a data breach 2025 | IBM. (s. f.).

https://www.ibm.com/reports/data-breach

Wikipedia contributors. (2025, 7 agosto). 2018 SingHealth data breach. Wikipedia.

https://en.wikipedia.org/wiki/2018_SingHealth_data_breach

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

This project has been co-funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.