ERRORES, CONFIGURACIONES INCORRECTAS Y PRÁCTICAS DE SEGURIDAD DEFICIENTES

Co-funded by the European Union

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

Socios

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

Co-funded by the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.

Tabla de Contenidos

Co-funded by the European Union

FACTSHEET – ERRORES, CONFIGURACIONES INCORRECTAS Y PRÁCTICAS DE SEGURIDAD DEFICIENTES

1. Definición

Son vulnerabilidades internas y errores humanos inintencionados, tales como configuraciones incorrectas o prácticas de seguridad deficientes, que pueden provocar incidentes de seguridad y filtraciones de datos1. Ejemplos de vulnerabilidades incluyen contraseñas débiles, privilegios excesivos para los usuarios, la falta de aplicación de parches y la omisión de la encriptación.

2. Relevancia general

Los asuntos de seguridad revisten importancia dado que facilitan a los criminales el comprometimiento de sistemas con relativa facilidad. La mayoría de las filtraciones de datos son atribuibles a errores humanos o a configuraciones inadecuadas, lo que subraya la relevancia de implementar prácticas internas de ciberseguridad sólidas y de considerar los factores humanos en la postura de seguridad general.

De acuerdo con IBM2, los errores humanos representan más del 20% de todas las violaciones de seguridad, lo que implica un costo significativo para las organizaciones, que asciende a millones. La configuración inadecuada puede resultar en una exposición prolongada. Por ejemplo, un servidor que no está configurado adecuadamente puede exponer datos sensibles durante un período prolongado antes de que se detecte la vulnerabilidad. En consecuencia, la corrección de errores y la garantía de que se sigan procedimientos seguros constituyen aspectos fundamentales de la ciberseguridad para las empresas.

3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados

Las configuraciones incorrectas en el ámbito de la salud tienen un impacto directo en la seguridad de los pacientes, la privacidad y la calidad de la atención. Cuando se presentan tales situaciones, se pueden generar riesgos significativos que afectan no solo la integridad de los datos, sino también la confianza en los sistemas de atención médica. La afectación de los dispositivos médicos puede dar lugar a errores en la administración de medicamentos, así como a retrasos en las alarmas y fallos en el funcionamiento de los servicios de monitorización.

La divulgación de información sensible contenida en los registros de pacientes podría constituir una violación de las normativas del GDPR y HIPAA, lo que a su vez podría menoscabar la confianza del público en los profesionales de la salud.

En última instancia, una deficiente higiene cibernética, como el uso de software obsoleto o la asignación inadecuada de permisos de usuario, puede facilitar la infiltración de atacantes en las redes, interrumpir las operaciones hospitalarias, retrasar los procedimientos y disminuir la calidad de la atención. La violación de datos de SingHealth en Singapur, ocurrida en 2018, implicó configuraciones inadecuadas en los controles de acceso a la red, lo que comprometió la información personal de salud de 1.5 millones de pacientes3.

4. ¿Qué puedo hacer como profesional sanitario?

- Seguir los protocolos y orientaciones organizacionales de seguridad.
- Utilizar accesos seguros mediante el inicio de sesión en la plataforma en la nube del hospital, con contraseñas seguras y la autentificación en dos pasos.
- Informar inmediatamente de cualquier comportamiento inusual o error de configuración potencial al equipo informático.
- Realizar formaciones sobre ciberseguridad y mantenerse al día sobre cómo se manifiestan este tipo de ataques para reducir el error humano.

5. Más información

5.1 Materiales de aprendizaje

- 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 Vídeos Relacionados

Este vídeo frece consejos prácticos y breves para mantener su ordenador y sus datos a salvo de ataques de ingeniería social, phishing y otros riesgos cibernéticos comunes en entornos laborales.

Buenas prácticas de ciberseguridad
https://www.youtube.com/shorts/Ru4wPjNQkLU

El siguiente vídeo ofrece una guía práctica para profesionales de la salud sobre cómo implementar medidas básicas de ciberseguridad para proteger la información digital de los pacientes.

¿Cómo proteger la salud digital de pacientes?
https://youtu.be/zAKT1rpf5n0?si=1qQ8fBK-qyrdDi6T

5. 3 Enlaces Relevantes

Según el Instituto Nacional de Ciberseguridad (INCIBE), el 68% de los incidentes de ciberseguridad en el sector sanitario se deben a configuraciones incorrectas o desactualizadas en sistemas y dispositivos. https://www.incibe.es/incibe-cert/blog/ciberseguridad-en-el-sector-salud-caracteristicas-amenazas-y-recomendaciones

Un artículo de SIB Prodasa destaca errores comunes en la gestión de datos sanitarios, como la falta de formación en protección de datos para el personal sanitario, lo que puede llevar a fugas de información accidental y comprometer la confidencialidad de los pacientes. https://sibprodasa.es/es/los-4-errores-comunes-en-la-gestion-de-datos-sanitarios-y-como-evitarlos-con-una-asesoria-especializada

6. Bibliografía

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

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.