Vulnerability Audit and Assessment of (https://ehr-online.co.uk) Baseline Analysis and Plan

Description of the Evaluated Website

The evaluated web application provides a service of electronic health record management. This means the servers and the website will hold information related to patient medical history, medications, laboratory testing, medical imaging, diagnosis, and treatment. In addition, it will hold other personally identifiable information like full name, address, and phone number. In Other words, a core part of this service deals with protected health information according to the UK GDPR regulation, data protection, and Health and Social care Acts (NHS, 2021; ICO.ORG.UK, 2021). A full list of required compliance and certification is presented in Table 1.

TABLE 1 COMPLIANCE CHECKLIST

Item (Regulation / Act / Certification)	Justification
General Data Protection Regulation (GDPR)	Protection of personal data
Data Protection Act 2018 (Anon, 2018)	Protection of personal data
Health and Social Care Act 2008 (Anon, 2019)	Protection of personal data
Limitation Act 1980 (Anon, 1980)	Setting retention time of medical records
Consumer Protection Act 1987 (Anon, 1987)	Managing consumer relation
ISO/IEC 27001 Certification	Managing information security

Security Challenges

Different assets were identified for such an electronic health record system. Each asset has its security challenges (Table 2).

TABLE 2 SECURITY CHALLENGES

Asset Type	Security Challenges
Human Asset	- Protecting usernames and passwords - Security awareness of the users of the system (health care providers). - Phishing - Malware
Web Asset	- Protection against SQL injection - Protection against Cross-site scripting - SSL certificate issues - Cryptographic Failures - Secure Software Life Cycle
Data Asset	- Database configurations - Data encryption - Disaster recovery - Data backup
Physical Asset	- Server configurations - Firewalls

Tools

The following tools will be used for the assessment (Table 3).

TABLE 3 ASSESSMENT TOOLS

Tool	Justification
Nmap	- OS fingerprinting. - Scan for open ports.
Nessus	- Perform basic network scan. -Testing the web application testing for common vulnerabilities.
Wireshark	- To monitor network traffic for suspicious activity.
Social Engineering	- Asses the security awareness of the health care workers

Methodology

The assessment process that will be conducted is based on what is described by McNab (2016) with a combination of internal and external scans, in addition to social engineering, analysis, and risk assessment (Tunggal, 2021; Cyber Today Academy, 2021). The assessment will start with the identification of resources (reconnaissance) using Nmap and Nessus followed by vulnerability scanning and investigation. This will be facilitated by Nessus tools that search for common vulnerabilities and exposures.

Wireshark will be used to monitor network traffic and detect any evidence of malevolent activity as part of internal scanning.

In the analysis stage, the vulnerabilities will be sorted according to severity and impact on the business. At this stage, the decision to perform a penetration test will be discussed. The assessment process will involve more than one cycle that ultimately leads to the collection of the required information.

After gathering resultant data, a report will be generated with a remediation and mitigation plan. The input stakeholders and the IT department.

Summary of limitations and assumptions and business impacts

An electronic health records system is expected to be used heavily during working hours, and to a lesser extent at night. Thus, the scan time should be scheduled with the stakeholders to minimize service disruption. However, some internal scans including Wireshark will be necessary during normal traffic. Test scans will be performed as necessary to measure the effect of such scans on network performance.

Since a remote scan will be performed, firewalls and intrusion detection systems might interfere with successful scans. Arrangements should be done in advance with the IT personnel to seek the best time for shutting down protection systems to allow for the scanning process to be completed.

References

Limitation Act 1980, c.58.United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/1980/58/contents [Accessed 10 October 2022]

Consumer Protection Act 1987, c.85. United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/1987/43 [Accessed 10 October 2022]

Data Protection Act 2018, c.12. United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/2018/12/contents [Accessed 10 October 2022]

Health and Social Care Act 2008, c.14 United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/2008/14/contents [Accessed 10 October 2022]

Cyber Today Academy (2021) vulnerability assessment tutorial for beginners. Available from: https://www.youtube.com/watch?v=hIbkwnOteTc [Accessed 10 October 2022].

ICO.ORG.UK (2021) The UK GDPR. Available from: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/ [Accessed 10 October 2022].

Mcnab, C. (2016) *Network security assessment : know your network*. Third edition. ed. Sebastopol, CA: O'Reilly. Available via the Vitalsource Bookshelf. [Accessed 10 October 2022].

NHS (2021) Records Management Code of Practice. Available from: https://transform.england.nhs.uk/information-governance/guidance/records-management-code/ [Accessed 10 October 2022].

Tunggal, A. (2021) What Is a Vulnerability Assessment? And How to Conduct One. Available from: https://www.upguard.com/blog/vulnerability-assessment [Accessed 10 October 2022].