**THREATS, VULNERABILITIES AND MITIGATION TECHNIQUES**

**RECOMMENDED READING- Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015)**[**Compromising a Medical Mannequin.**](https://aisel.aisnet.org/amcis2015/HealthIS/GeneralPresentations/5/)**Healthcare Information Systems and Technology (Sighealth).**

**SUMARY POST 1**

Kumar (2017) has noted that data accessed illegally can be used as ransom, to commit tax frauds, to provide supporting disability documentation, to send fake bills to insurance providers, to obtain healthcare, prescription drugs, medical treatment, and to obtain government benefits like Medicare and Medicaid (Kumar, 2017)

The evolution of  Internet of Things, (IoT) comes with significant challenges  such as hijacking of IoT devices, financial crime, home invasion etc as seen in the article on mannequins, therefore, it is important cyber security measures are put in place wherever there is sensitive data.

 I like the point raised by David on the  NHS Digital (2020) recommendations  for fewer routes to unpatched software. A lot of smart devices were developed without security in mind probably due to limited resources, therefore, these devices don’t  support the processing power needed for secure communication like encryption and  are not designed to accommodate software or firmware which makes vulnerability patching difficult. In addition to software patching and encryption etc Security by Design (SBD) will  ensure devices connected to the internet are secure (Cybersecurity in the Internet of Things: Legal aspects | Elsevier Enhanced Reader)

REFERENCES

Kumar, Caleb (2017). New Dangers in the New World: Cyber Attacks in the Healthcare Industry. Available from <https://ojs.stanford.edu/ojs/index.php/intersect/search/authors/view?firstName=Caleb&middleName=&lastName=Kumar&affiliation=Stanford%20University&country=US>. Accessed 22 May 2021

Cybersecurity in the Internet of Things: Legal Aspects | Elsevier Enhanced Reader’. Available from [**https://doi.org/10.1016/j.clsr.2016.07.002.** Accessed 22 May 2021](https://doi.org/10.1016/j.clsr.2016.07.002.%20Accessed%2022%20May%202021)

**BASIC SCANS CARRIED OUT USING STANDARD TOOLS SUCH AS PING, TRACEROUTE, DIG, NSLOOKUP**

**SUMMARY POST 2**

In addition to David’s comment on Ping Transmission failure, failure to get a response from a remote host can be caused by a remote host being down, problem in some links/nodes in the forward path between the last successful hop and the remote host, or one in some links/nodes in the backward path. Also, some nodes may be programmed not to respond to such packets sent by traceroutes or ping. While pinging,  the first reply may take a long time to come in due to ARP lookups at each router After that, ARP results are cached.

Reference

Kobashi et al– A Tool For Diagnosing Internet Connectivity Problems [**https://courses.cs.washington.edu/courses/cse561/04au/projects/papers/Tungaraza-Kobashi.pdf**](https://courses.cs.washington.edu/courses/cse561/04au/projects/papers/Tungaraza-Kobashi.pdf). Accessed 14 June 2021.

**RECOMMENDED READING- DATA PROTECTION COMMISSION (2020) CASE STUDIES DATA PROTECTION COMMISSION** Available from: [**https://dataprotection.ie/en/pre-gdpr/case-studies**](https://dataprotection.ie/en/pre-gdpr/case-studies)

**SUMMARY POST 3**

AlKilani *et al* (2019) opines that conventional data loss solutions such as firewalls, Intrusion Detection and Prevention Systems aren’t faultless. They tend to suit only data with a predetermined structure. Such systems have weaknesses and can be circumvented. For instance, a data’s file structure can be modified using exfiltration techniques such as Command Prompt Application to affix a confidential test file into a non-confidential file using TYPE command which is available in most Windows operating systems in order to display the contents of the file into another file thus preventing such data from being detected by the conventional data loss solutions thus resulting in false negatives.(AlKilani *et al.*, 2019)

A self-learning Intelligent Information Leak Protection System may be a more reliable data loss solution. These mine and extract information, categorizes documented images and classify them as Sensitive or Non-Sensitive Data, (based on the presence of Non-Public Information and Personal Identifiable Information or semantic signatures) using state of the art classification algorithms to learn which data is sensitive.

According to Guha *et al.*,( 2021), Intelligent self-learning is typically implemented using various mechanisms, such as Described Content Matching (DCM), Exact Data Matching, Indexed Document Matching, Vector Machine Learning, Content Matching Classifiers, and File Type Detection to detect Data Loss Prevention (DLP) violations in a message or document (Guha *et al.*, 2021).

Reference

AlKilani, H. *et al.* (2019) ‘Data Exfiltration Techniques and Data Loss Prevention System’, in *2019 International Arab Conference on Information Technology (ACIT)*. *2019 International Arab Conference on Information Technology (ACIT)*, pp. 124–127. doi: 10.1109/ACIT47987.2019.8991131.

Guha, A. *et al.* (2021) ‘A Deep Learning Model for Information Loss Prevention From Multi-Page Digital Documents’, *IEEE Access*, 9, pp. 80451–80465. doi: 10.1109/ACCESS.2021.3084841.