**Week7 Reflection on Cybersecurity**

Hang Yang

IS 5403: Cybersecurity

Prof. Jaime Martinez

April 27, 2024

**Week7 Reflection on Cybersecurity**

In the week7’s course, the videos introduce several core concepts of cybersecurity architecture. They are Roles and Tools, IAM, Endpoint Management. In the course of roles and tools, it focuses on what the role of cybersecurity architect is, as well as different mindset they should have from traditional IT architect. For example, a cybersecurity architect should consider how the system would fail instead of how the system is built up to work. Then a cybersecurity architect should further have a checklist to the question what I need to do to prevent the system from attacking. The checklist could be like: would the pass phase be stolen or broken? Would a single type of monitoring be enough for potential multiple types of devices? A cybersecurity architect should have some prepared solutions to this question checklist when occurs. When talking about security tools, it highlights the usage of cybersecurity frameworks besides principles and CIA triad. The NIST CSF is cited in the course as a good practice in the industry. It emphasizes the importance of taking the security concerns into architecture design from the very beginning of the business implementation lifecycle, not only in the risk analysis stage.

My main takeaway is from IAM, which stands for identity access management, an approach aimed at managing user profiles and access permissions. It comprises two main components: identity management and access management. Identity refers to a unique identifier used to recognize an object, such as a driver's license or SSN. In a system, user identity could be represented by user ID, username, or user signature. Access pertains to the ability to perform operations (retrieve, update, create, delete) on specific resources within the system. SSO (Single Sign-On) consolidates multiple applications under a single login system, often enhanced by Multi-factor Authentication (MFA) to bolster access controls. Compared to using the same passwords repeatedly, SSO + MFA offers enhanced security. The 4As serve as the foundation of IAM: admin, authentication, authorization, and audit. Admin, also known as identity management or identity governance, involves creating, updating, deleting, and reading user profiles. AuthN involves verifying a user's identity based on provided data points, such as passwords, facial prints, or else. AuthZ focuses on access management, employing approaches like risk-based access or adaptive access to control resource access. Audit ensures that IAM policies and procedures align with security standards and business goals.

The Coursera course introduced different type of data breaches, like phishing, PoS malware, ransomware. It explains the definitions of different data breaches, as well as illustrating some up-to-date data breach cases with a formatted template. Among the case studies, phishing stands out to my attention because I personally am also victim to the phishing scams. The case study helps me to better understand how to recognize the phishing email for some characteristics, like unknown senders, generic greetings, spelling and malicious link. This is not an online course, but also save me in my daily life. Regarding the final project, it requires us to present an individual study on a recent data breach case. As far as I could remember, I’ve been quite interested into ransomware at a time. So, I did some research on ransomware cases, and it really shocked me that ransomware breaches in 2023 got almost double the total cost of $567 million in 2022. 2023 became the largest amount of ransomware payment in the past five years. But you could take some steps to protect yourself or your organization from ransomware attack. The very first and most important one is to back up your data in a secure place. Then you could schedule regularly scan of systems and software updates to ensure that your organization is free from hardware/software vulnerabilities. Another effective approach is to enable holistic endpoint security management. This could largely mitigate the challenges of growing usage of private end-user devices, like mobile phones, tablets, smart wearing and more into private/public network. Network segmentation could also play an important role into depth of defense considering data breaches beyond ransomware. It’s still recommended to put critical data storage or some other critical platform into dedicated network zone under budget.

**References**

Sabin, S. (Feb 10, 2024). Ransomware gangs collected record $1.1 billion from attacks in 2023. Axios. Retrieved from

https://www.axios.com/2024/02/09/ransomware-earnings-2023-chart