Unit 10: Analyzing and Mitigating Security Breaches

Objectives:

- Discuss a number of case studies related to the most famous breaches of the 21st century.
- Apply the breach checklist provided in the lecture cast.
- Analyze an assigned case study and post results.

Outcomes:

- Utilize the breach checklist to analyzes a breach.
- Recommend a number of actions and tools based on the analysis.
- Critically assess published responses.

Reflections:

Data breaches happen when a firm's database is hacked, allowing attackers to gain access to crucial data including credentials, account numbers, telephone numbers and payment details among other things.

Studies show that adversarial assaults are the most common cause of data breaches, second by human mistake, and then system failures. Cyber-attacks, spoofing, spyware and ransomware are all examples of malevolent assaults in this environment (McLeod and Dolezel, 2018).

Data breaches can be prevented by following these guidelines:

- Periodic examinations of security vulnerabilities in organizational systems to resolve high-priority security holes are ongoing.
- Virtual security breaches on IT networks to test for potential flaws are known as penetration tests.
- Accidental or negligent sharing of information or social engineering techniques like Phishing are often the cause of security breaches. The importance of promoting knowledge and understanding cannot be overstated. Precautions include training workers on security protocols, teaching them how to avoid social engineering assaults, and identifying sensitive data.
- Strategies for a response, containment, reduction, and restoration in the event of a security crisis must be documented by security personnel (Learning Center, 2017).

The network's perimeter must be protected using security technologies in order to prevent unauthorized access and a broad variety of attacks on information systems. Impervo’s Web Application Firewall prevents attacks like SQL injection and XSS (RFI). Most famous breaches of the 21st century:

- Yahoo (2013-2014) Impact: 3 billion user accounts.

- eBay (2014) Impact: 145 million users.
- Equifax (2017) Impact: Personal information of 143 million consumers and credit card data of 209 000 consumers.
- Target Stored (2013) Impact: 110 million customers.
- Uber (2016) Impact: The personal information of 57 million Uber users and 600,000 drivers.

References

Learning Center. (2017). *What is a Data Breach | Tips for Data Leak Prevention | Imperva*. [online] Available at: https://www.imperva.com/learn/data-security/data-breach/.

McLeod, A. and Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, 108, pp.57–68. doi: 10.1016/j.dss.2018.02.007.

Moghimi, D., Lipp, M., Sunar, B. and Schwarz, M. (2020). *Medusa: Micro architectural Data Leakage via Automated Attack Synthesis*. [online] www.usenix.org. Available at: https://www.usenix.org/conference/usenixsecurity20/presentation/moghimi-medusa [Accessed 10 May 2022].

Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*. doi:10.1007/s11227-020-03213-1.