YORK UNIVERSITY

ITEC 3210 C – Fall 2023
Assignment 2
Professor: Andriy Pavlovych

Prepared by:
Muskanmeet Kaur (219633361)
Sahib Deep Singh (219170646)

PART 1. Designing networks: Key technical goals and best practices.

1) **Briefly define the 3 key technical goals in network design.**

- **Technical goal 1: Performance**
  Performance is a measure of a system's efficiency and effectiveness in carrying out tasks, which is frequently expressed in terms of speed, accuracy, or resource consumption. Making it a technical aim means enhancing these aspects to improve overall functionality.
- **Technical goal 2: Scalability**
  Scalability is critical to prepare for future development and demands while designing a scalable network. This might include the use of modular components, like as switches and routers, which can be readily upgraded or replaced.
- **Technical goal 3: Availability**
  Redundancy is essential for network availability. This may entail employing numerous network routes, installing backup power sources, and setting failover procedures. Regular maintenance and upgrades are also required to keep the network running smoothly.

2) **For each technical goal above, discuss four (4) best practices in network design one can use to reach that goal.**

- **Performance**
  BEST PRACTICE 1: Write clear, efficient code while eliminating infinite and unnecessary loops and resource-intensive processes.
  BEST PRACTICE 2: Implement effective caching systems to store and retrieve frequently used data, eliminating the need for repetitive calculations.
  BEST PRACTICE 3: Collect network data and the establish baselines. It provides a framework for better monitoring, problem resolution, and proactive management, resulting in a more dependable and efficient network infrastructure.
  BEST PRACTICE 4: Prioritize Asynchronous processes to improve performance by exploiting asynchronous programming whenever possible, allowing concurrent task execution, and decreasing wait times, particularly in I/O-bound processes.

- **Scalability**
  BEST PRACTICE 1: Load balancing can help prevent overload and enhance performance by distributing network traffic evenly across several components or connections. Load balancing is recommended for networks with several servers or high traffic volumes.
  BEST PRACTICE 2: Create systems that are modular and scalable, allowing components to be readily added or withdrawn. This encourages adaptation and flexibility in response to changing needs.

BEST PRACTICE 3: Adopt a microservices architecture, which divides the application into smaller, self-contained services. This allows teams to independently create, deploy, and grow individual components, improving agility and scalability.
BEST PRACTICE 4: Use auto-scaling technologies to alter resources dynamically based on demand. This means providing or de-provisioning resources automatically in response to changes in workload.

- **Availability**
  BEST PRACTICE 1: Using documentation to provide clear and well-structured information on the network's components, configurations, and processes simplifies network management and troubleshooting. It is suggested that all network designs be documented.
  BEST PRACTICE 2: Create robust redundancy methods to lessen the effect of hardware failures or system outages. This entails duplicating important components and services to enable continuous functioning even when there are interruptions.
  BEST PRACTICE 3: Implement automatic monitoring tools to continually track the system's health and performance. Set up alerts to warn administrators of any abnormalities or possible concerns as soon as they occur, allowing for proactive response.
  BEST PRACTICE 4: Set up frequent backup methods to protect crucial data and configurations. Create a thorough disaster recovery strategy to recover quickly from unforeseen catastrophes while reducing downtime and data loss.

PART 2. Case: Marriott Security Incident.

Question 1: Briefly discuss the immediate actions Marriott should take after discovering the attack. Include in your discussion why such actions are required.

To avoid additional unauthorized access, Marriott should promptly isolate and confine the impacted systems. They should also alert law enforcement and work with them to investigate the breach. It is critical to implement a communication plan to educate impacted guests about the occurrence and provide instructions on how to protect their personal information to preserve confidence.

Question 2: Briefly discuss FIVE (5) security controls covered in the ITEC 3210 mandatory text that would have helped prevent or detect this security incident earlier.

- **Antivirus Software:** Antivirus software aids in the prevention and detection of dangerous software such as malware and Trojans. During frequent scans, a strong antivirus solution might have spotted and removed the Remote Access Trojan (RAT) and other infections, preventing illegal access and data exfiltration.

- **Firewalls:** Firewalls serve as a barrier between a secure internal network and a potentially dangerous external network. Strong firewall rules would have prevented unwanted access to the Starwood Guest Reservation System, preventing the initial breach and restricting the attackers' lateral movement inside the network.
- **Backups:** In the case of a security breach, regular backups are critical for data recovery. If Marriott had kept current and secure backups, they might have restored the damaged systems to a known good condition following the attack, limiting data loss and disruption.
- **Encryption (data transmission and data storage):** Encryption protects sensitive data during transmission and storage. If Marriott had used encryption for guest data, attackers would have found it far more difficult to extract and abuse the data even if they acquired illegal access.
- **IPS and two-factor authentication:** Intrusion Prevention Systems monitor network and/or system activity for malicious exploits or breaches of security policies. IPS may have identified and prevented the attacks in real time. By forcing users to give two forms of identity before accessing systems, two-factor authentication (2FA) offers an extra layer of protection, defeating the assault.

Question 3: Discuss THREE (3) security controls covered in the ITEC 3210 mandatory text that would not have helped prevent or detect this security incident earlier.

- **Physical Security:** Because Marriot operates at the digital level, physical security safeguards would not have identified or blocked the remote access Trojan (RAT), or malware employed in the assault. The hack happened by cyber methods, utilizing malware and illegal network access.
- **DDoS Prevention:** To obtain illegal access and breach the Starwood Guest Reservation System, the attackers utilized sophisticated tactics such as deploying a Remote Access Trojan (RAT) and other malware. DDoS mitigation strategies would have been ineffective in preventing or detecting this sort of targeted strike. DDoS protection techniques are intended to lessen the impact of large-scale, malicious traffic flooding on a network.
- **Security Policies:** The incident involves a breach via a third-party vendor (Accenture), making internal security procedures difficult to anticipate and avoid similar external attacks. Also, having security policies does not mean all employees follow them.

Question 4: Should Mariott implement any recovery control? Justify your answer.

Yes, as part of their cybersecurity strategy, Marriott should include recovery controls. Recovery measures are critical for limiting the effect of a security event and resuming regular activities as soon as possible. Implementing recovery controls in the context of the mentioned event involving the breach of visitor data would entail activities such as: Data Restoration, Incident Response, Post-Incident Learning, etc.