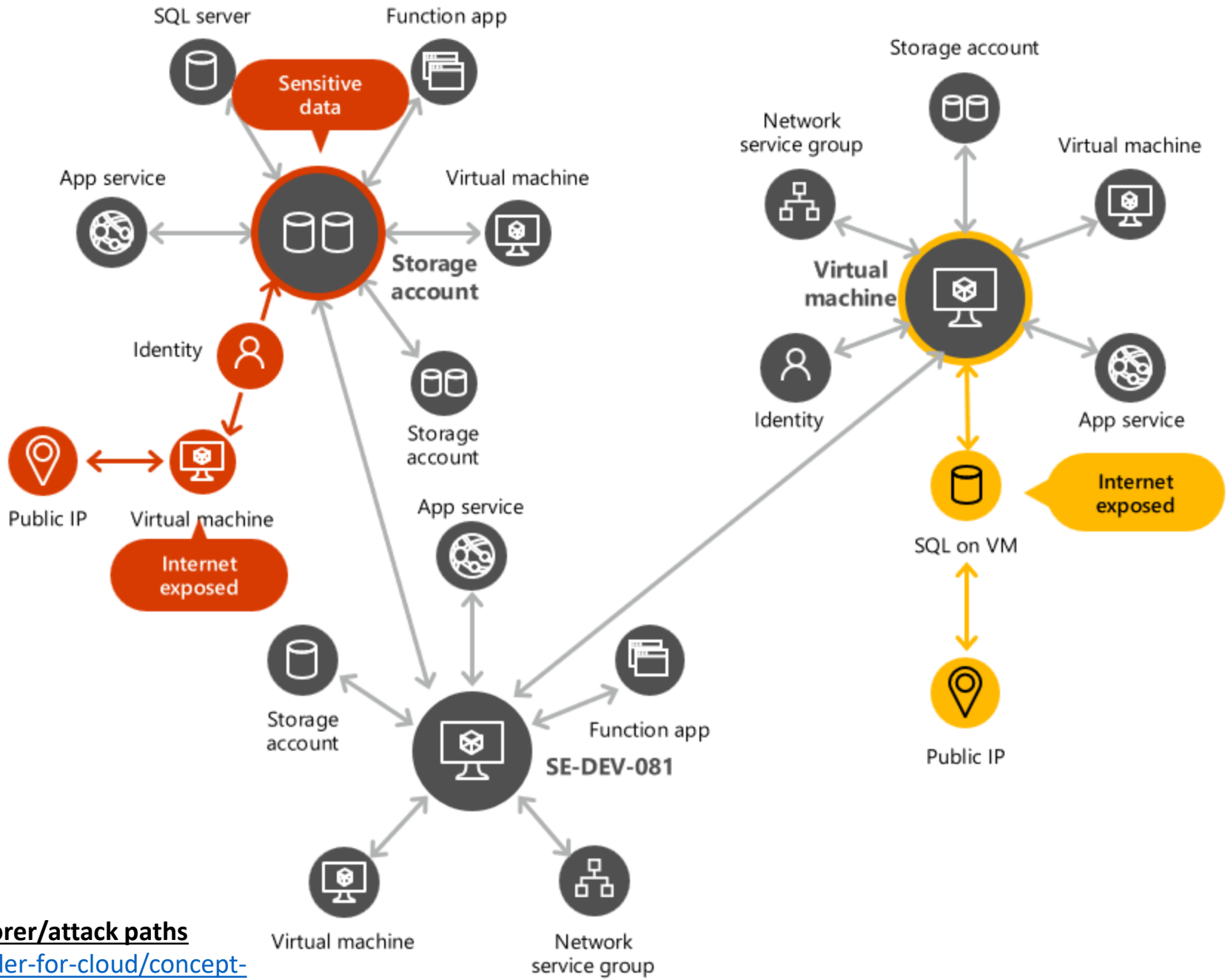
COMP3052 Computer Security

Session 01: Introduction to COMP3052.SEC



Reference: Investigating risk with security explorer/attack paths
https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-attack-path

Assets:

The assets could include customer data (e.g., personal information, account details), financial transactions, reputation and trust of the company. Let's say the total value of the assets is ***$10 million***.

Vulnerabilities:

Let's assume the following probabilities for the 3 identified vulnerabilities:

(1) Unpatched software on the web server: Probability = 0.6

(2) Weak password policy for employee accounts: Probability = 0.4

(3) Lack of encryption for stored customer data: Probability = 0.3

The combine vulnerabilities = (0.6+0.4+0.3)/3 = 1.3/3 = ***probability of 0.433***.

Threat:

Likelihood of a cyberattack by hackers targeting the system is moderate, with a ***probability of 0.3***.

Now, let's calculate the risk:

Risk = Assets * Vulnerabilities * Threat

Substituting the values:

Risk = $10,000,000 * 0.433 * 0.3

Risk = $1,299,000

(A) Hacker (B) Attacker

1. _____ refers to someone who proactively explores, identifies and alerts organizations to vulnerabilities that an attacker could use for malicious purposes. They seek to disclose in good faith by alerting organizations that may or may not have vulnerability disclosure policies.

2. _____ refers to someone who gains unauthorized access to someone else's network and computers for malicious purposes without permission or without warning the organization. This can be for monetary gain such as in ransomware attacks.

Reference: Hacker vs Attacker

https://www.tripwire.com/state-of-security/hackers-vs-attackers-different-animals

(A) Accidental Failures (B) Operating Failures (C) Intentional Failures

1. Security measures are primarily focused on protecting the computer system from _____, such as malicious attacks or unauthorized access.

2. Usability contributes to the prevention of _____ by making the computer system more user-friendly and intuitive, thus reducing the likelihood of errors made by users.

3. Reliability addresses _____ by ensuring the consistent and dependable performance of the computer system under normal operating conditions. This includes minimizing downtime, preventing crashes or system freezes, and maintaining data integrity.

(A) Reliability (B) Usability (C) Security

1. _____ measures include redundant power supplies and backup systems that can prevent system downtime due to hardware failures, while error-checking and error-correction codes help detect and correct data corruption or transmission errors.

2. _____ measures include antivirus software to protect against malicious software that can compromise system integrity, while strong authentication mechanisms like biometrics or two-factor authentication prevent unauthorized users from gaining access to sensitive information.

3. _____ measures include error messages that provide clear explanations and suggested actions help users troubleshoot issues effectively, reducing the risk of data loss or system misconfiguration.