Cyber Security

2024

Zero Trust in Action

Vathna.lay@cadt.edu.kh

Scenarios

- Scenario 1: A user's account shows unusual activity: emails they didn't send, files they didn't access, and a login from an unfamiliar location.
- Scenario2: The marketing department is using an unapproved cloud storage service to share sensitive campaign materials.
- Scenario 3: A ransomware attack has encrypted files on a cloud-hosted server, demanding payment for decryption.
- Scenario 4: A former employee who was laid off still has access to sensitive financial data.

Scenarios

- Scenario 5: An employee's account shows a login attempt from a foreign country they've never visited.
- Scenario 6: An employee downloads a large amount of sensitive customer data to their personal device.
- Scenario 7: An employee receives a seemingly legitimate email from their "manager" asking them to click a link and enter their credentials.

Scenarios

- Scenario 8: A cloud server's security settings are misconfigured, allowing unauthorized access from the internet.
- Scenario 9: A cloud-hosted application becomes unresponsive due to a sudden surge in traffic, potentially indicating a DoS attack.
- Scenario 10: A disgruntled employee intentionally deletes critical data from a cloud databas

Tasks

- Based on experience in Practice 6, prepare for this practice
- Everyone needs to prepare their research about all scenarios.
  - Individual preparation will be checked and scored during the lab session
  - The same preparation notes will be punished
- The group will be randomly grouped during the lab session
- After matching the group with the topic, you have 15 minutes to prepare for the
- After the presentation, the slide has to be submitted in moodle.

Scenario 1: The Compromised Credentials

- Confirmation: How would you verify if the account is indeed compromised?
- Damage Mitigation: What immediate steps should be taken to minimize potential damage?
- Prevention: what measures could have been in place to prevent this breach?

Scenario 2: The Shadow IT Application

- Discovery: How might this unauthorized use be discovered?
- Risk Assessment: What are the primary risks associated with using an unapproved cloud service?
- Mitigation: What steps should be taken to address the situation?

Scenario 3: The Ransomware Attack

- Zero Trust Advantage: How would a zero trust framework have potentially mitigated this attack?
- Recovery: What are the options for recovering the encrypted files?
- Prevention: How can you prevent similar ransomware attacks in the future?

Scenario 4: The Over-Privileged User

- Least Privilege: How should this employee's access have been managed initially?
- Remediation: What steps should be taken now to revoke their access?
- Prevention: What processes should be implemented to prevent similar incidents?

Scenario 5: The Suspicious Login Attempt

- Investigation: How would you investigate this login attempt?
- MFA & Honeypots: How could these tools have helped?
- Response: What actions should be taken if the login is confirmed as unauthorized?

Scenario 6: The Unauthorized Data Download

- Detection: How might this unauthorized download be detected?
- Motivation: What could be the motivations behind this action?
- Response: What immediate actions should be taken?

Scenario 7: The Phishing Attack

- Identification: How can you identify this as a phishing attempt?
- Impact: What could be the consequences if the employee falls for the phishing attack?
- Education: How can you train employees to spot and avoid phishing attacks?

Scenario 8: The Cloud Misconfiguration

- Detection: How might this misconfiguration be discovered?
- Impact: What are the potential consequences of this misconfiguration?
- Remediation: What steps should be taken to address the misconfiguration?

Scenario 9: The Denial-of-Service (DoS) Attack

- Identification: How can you determine if this is a DoS attack?
- Impact: What are the consequences of a successful DoS attack?
- Mitigation: What steps can you take to mitigate a DoS attack?

Scenario 10: The Insider Threat

- Prevention: What measures could have been in place to prevent this insider attack?
- Detection: How might this incident be detected?
- Response: What actions should be taken after discovering the data deletion?