Course: CYB301 Security Defense and Response (Canadian Context)

Lab 8: Identity and Access Management Security

Coordinator and Instructor: Muhammad Siddiqui

Student: Saiprasad Raman (23074624)

IAM Security

Activity 1: Federated Security Scenario

In this activity, you will be provided with two different federated identity scenarios. For each, you should research the technology or situation described and then write a written recommendation to handle the issue described.

Part 1: Google OAuth integration

Example Corp.'s development team has implemented an OAuth integration with Google. The internal development team has written their own libraries for the company's OAuth endpoint and has implemented their server using HTTP between Example Corp.'s servers.

Q1: What security issues would you identify with this design, and what fixes would you recommend?

Ans.

Problems:

1. Having an HTTP server can be vulnerable to password attacks via sniffing packets or any other vulnerability scanners.
2. Tokens could be stolen.
3. Usage of old libraries that doesn't align with OAuth's standards.

Solutions:

1. Use an HTTPS-based server to avoid attacks on credentials.
2. Preserving tokens or using OAuth 2.0 which utilizes PCKE (Proof Key for Code Exchange).
3. Make sure the libraries are constantly updated according to OAuth's standards.

Part 2: High security federation incident response

Example Corp. is considering using Facebook Login to allow users to bring their own identity for its customer support website. This would remove the need for Example Corp. to handle its own identity management in most cases and is seen as an attractive option to remove expensive user support for this type of account.

Answer the following questions:

Q2: What recommendations and advice would you provide to the implementation team?

Ans.

1. Make sure all the communication between Example Corp. and Facebook are via HTTPS.
2. Evaluate risks associated with the implementation of Facebook login.
3. Ensure token are stored securely while implementing expiration of tokens.
4. Ask users to accept GDPR or GAPP regulations on data usage before continuing to access the website.

5. Educate users on utilizing proper login mechanisms while managing permissions.
6. Monitor and record logs on the user's attempts and patterns of using Facebook Login.

Q3: What should Example Corp.'s incident response plan include to handle issues involving Facebook Login?

Ans.

1. Create a team to respond to incidents depending on the risk factor. The team can be employees with different qualifications while utilizing other businesses to support the incident.
2. Identify the incidents based on what it is affecting currently whether it's the number of attempts to login, user unable to login or any other alerts from the monitoring systems in place.
3. Implement limits on number of login attempts to avoid Brute force Attacks.
4. Have a communication strategy in place to notify employees and stakeholders of any occurrence of the incident.
5. Record incidents and create a detailed report to educate employees and stakeholders on having proper precautions in place.
6. Review and update incident response plans every year.

Q4: Does using Facebook Login create more or less risk for Example Corp.? Why?

Ans.

1. Utilizing Facebook login to manage passwords would reduce the risk for Example Corp. with managing sensitive information.
2. This would be a better option for the users considering the hassle of creating and remembering new accounts in every domain they are connected to.
3. It could be high risk situation, if the login credentials are hacked and now could be utilized to login to other websites.
4. Users would be vulnerable to XSS attacks having a phishing attack in place of the original Facebook login page.
5. Compliance must be in line with Example Corp.'s requirements in terms of usage of data which could be a high-risk situation if not addressed with Facebook.

Part 3: Analyze your responses

To analyze your response to Part 1, use the OWASP Authentication cheat sheet found at https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html You will find tips on OAuth and application communications.

To analyze your response to Part 2, review federation-aware incident response policies like https://spaces.at.internet2.edu/display/TI/TI.100.1 and www.btaa.org/docs/defaultsource/technology/federated_security_incident_response.pdf

References:

Parecki, A. (2022, January 22). OAuth: When things go wrong. *Okta, Inc.* https://www.okta.com/blog/2019/04/oauth-when-things-go-wrong/

Kelly, M. (2024, October 2). *How to Create a Cybersecurity Incident Response Plan*. Hyperproof. https://hyperproof.io/resource/cybersecurity-incident-response-plan/

j.leroy@systancia.com j.leroy@systancia.com. (2020, September 3). *Social Login - The risks of Social Login | Blog - Systancia*. SEP - Systancia Experience Portal. https://www.systancia.com/en/social-login/

Activity 2: On-Site Identity Issues Scenario

In this activity, you will be provided with two different local identity scenarios. For each, you should research the technology or situation described, and then write a written recommendation to handle the issue described. In Part 3, you will review your answers and look for potential flaws that remain.

Part 1: Emergency privilege escalation

At Example Corp., administrative accounts are created and managed using a central identity and access management suite. This suite, as well as the company's central AAA servers, are hosted in redundant datacentres, and site-to-site VPNs normally connect those datacentres to multiple locations around the country.

Example Corp.'s systems engineering department recently dealt with a major internet connectivity outage, which also resulted in engineers being unable to log in to the systems at the sites where they worked. This meant that they were unable to work to fix the issues.

The engineers have requested that you identify a secure way to provide emergency, on-demand privileged access to local servers when the central AAA services are unavailable. You have been asked to provide a solution to central IT management that is both secure and flexible enough to allow authentication for network devices, servers, and workstations.

Ans.

1. Have Role-Based Access Control (RBAC) in place allowing specific roles to access the systems for a certain period.
2. Create emergency accounts on the back-up systems that are used in case of failure of regular services which should only be used for administrative purposes.
3. Multifactor Authentication for all emergency accounts.
4. Implement IPMI to monitor hardware status which will allow access to the server if the Operating system is malfunctioning.
5. Utilize SSH keys to access servers while being constantly updated.
6. Maintain an emergency database access with encryption which will be backed up regularly.
7. Train engineers on the use of emergency solutions while creating proper documentation to follow the procedures.
8. Conduct drills or tests on the emergency mechanisms and improve on any findings in the report.

Part 2: Managing privilege creep

A recent audit of Example Corp.'s file shares shows that many long-term employees have significantly broader rights to files and folders than their current roles should allow. In fact, in some cases employees could see sensitive data that could result in negative audit findings in a pending external audit.

How would you recommend that Example Corp. handle both the current issue of privilege creep and the ongoing problem of ensuring that it does not occur in the future without seriously disrupting the company's operations?

Ans.

1. Conduct an Audit to give access rights to the users based on the requirements of the company.
2. Utilizing Role-Based Access Control (RBAC) to give employees access to resources on the least privilege principle.
3. Remove certain access rights from the users while notifying users about it. Grant temporary access which expires after a certain period.
4. Document the process of asking for access rights and have IAM solutions for automating systems to give access rights to the employees.
5. Create clear policies outlining the details of granting, reviewing and revoking access and communicating it to the users.
6. Training should be provided to the employees regarding risks associated with privilege creep and the importance of access controls.
7. DLP solutions will help in monitoring data from unauthorized access.

Part 3: Review

Review your recommendations to ensure that confidentiality, integrity, and availability are maintained. Did you provide a solution that covers each of these three areas?

Ans.

The above recommendations are being considered with confidentiality, integrity and availability as follows:

1. Confidentiality:
    - Having an access request policy in place will ensure that data is protected from being exposed to unauthorized individuals.
    - Educating users on protection of data helps maintain confidentiality.
    - Role Based Access Control (RBAC) systems will make it possible to limit data access to employees designated for that access.

2. Integrity:
    - Audits make sure that specific data is being shared with the people who are assigned specific duties and responsibilities.
    - RBAC ensures that data isn't modified by employees of different departments.
    - IAM solutions would be useful for automating access requests and approval processes.

3. Availability:
    - Temporary access to resources enables companies to maintain security by limiting its available time.
    - IAM solutions will help make the data available to users with the use of automated mechanisms

Does your solution cover each of these areas (if appropriate)?

- Personnel
- Endpoint devices
- Servers
- Services and applications
- Roles and groups

Ans.

Personal:
Providing training for employees ensures a personal understanding of policies and procedures.

Endpoint devices:
Usage of automated monitoring systems to avoid users from accessing unauthorized content.

Servers:
Proper policies make sure that servers are only accessed by authorized personnels.

Services and applications:
IAM solutions to automatically provide access to employees in need of resources.

Roles and Groups:
RBAC is used to assign access rights based on employee's role in a company.

If you were asked to conduct a penetration test of an organization that had implemented your recommendations, how would you approach attacking your solution?

Ans:

1. Planning:
   Define goals to clarify what needs to be achieved during the penetration testing process.
   Determining which applications are to be targeted, scope of testing and specific goals with the test.
   Implement monitoring mechanisms to track effectiveness of the penetration test while maintaining a record of activities.

2. Information Gathering:
   Contact users, managers and stakeholders to understand their roles and responsibilities.
   Understand the network infrastructure, key assets and how data flows within a network.

3. Access controls:
   Test RBAC and IAM systems to ensure whether only authorized users can access certain resources.

4. Exploiting Vulnerabilities:
   Use various techniques like social engineering, phishing and XSS attacks on users and endpoint systems to gain access to accounts.

5. Post Exploitation:
   Focus on maintaining access and escalating privileges and navigate through the system to find further vulnerabilities and potential attack vectors.

6. Reporting:
   Document the process while explaining the vulnerabilities in detail, their potential impact and recommendations for remediation.