Technische Hochschule Rosenheim

Fakultät Informatik

Prof. Dr. R. Hüttl

IT-Security

Exercise 7

In this exercise, we'll look at authentication and authorization.

Task 1: Awareness Training Part 2

https://training.is-fox.de/fh-rosenheim-informatik

We complete the awareness test of our first exercise.
We start with the moduls concerning authentication

- Secure passwords
- Password management
- Multifaktor authentication

Then we complete the test with the moduls

- E-mail & phishing
- Sensitive information
- Social engineering

Task 2: Risk management for an IAM in a cloud environment

Identity and Access Management (IAM) represents an umbrella term for all processes and applications that are responsible for the administration of identities and the management of access rights to various applications, systems and resources.

The following functions belong to an IAM:

- Centralized management of identities and access permissions
- Centralized access control
- User authentication and authorization
- Multi-factor authentication
- Single Sign On Services
- Identity Brokering und Social Login (OpenID, SAML 2.0, z.B. Google, facebook, GitHub)
- User Federation (connection to LDAP, ActiveDirectory)
- Mapping of complex rules for access permissions (policies, RBAC, ABAC, etc.)
- Monitoring, Auditing, Reporting

Widely used cloud IAM are e.g. Amazon, Keycloak, Google

- Amazon AWS IAM https://aws.amazon.com/de/iam/
- Keycloak (OpenSource IAM) https://www.keycloak.org
- Google IAM https://cloud.google.com/iam

Risk analysis and measures:

A cloud native environment provider has implemented a platform to design, develop and operate business applications based on AWS. To prove that it is compliant (legally compliant) for banking and insurance applications, it commissions a Seucrity Audit.

The first step was a risk analysis. The cloud provider has integrated an IAM in its platform. In our task, we focus on the risk analysis of the IAM.

You have given the list of identified risks.

For each risk, look for measures to mitigate the risk.