CLOUD SECURITY CHECKLIST

Prepared by HANIM EKEN

https://ie.linkedin.com/in/hanimeken

Cloud security checklist:

1. **Identity and Access Management (IAM):**

- [ ] Implement strong authentication mechanisms such as multi-factor authentication (MFA).
- [ ] Use role-based access controls (RBAC) to limit permissions based on user roles and responsibilities.
- [ ] Regularly review and audit user permissions to ensure least privilege access.
- [ ] Enable logging and monitoring of user activities for accountability and security incident detection.

2. **Data Encryption:**

- [ ] Encrypt data at rest using encryption keys managed by the cloud provider or customer-managed keys.
- [ ] Encrypt data in transit using Transport Layer Security (TLS) or other secure communication protocols.
- [ ] Implement encryption for sensitive data stored in databases, storage buckets, and other repositories.

3. **Network Security:**

- [ ] Segregate network resources using virtual private clouds (VPCs) or network security groups (NSGs) to control traffic flow.
- [ ] Use firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and filter incoming and outgoing traffic.
- [ ] Implement network access controls, such as IP whitelisting and blacklisting, to restrict access to authorized users and applications.

4. **Data Protection:**

- [ ] Regularly back up data and ensure backups are stored securely and can be easily restored in case of data loss or corruption.
- [ ] Implement data loss prevention (DLP) measures to prevent unauthorized access, sharing, or leakage of sensitive data.
- [ ] Monitor data access and usage patterns for anomalies or unauthorized activities.

5. **Compliance and Governance:**

- [ ] Understand and comply with relevant regulatory requirements and industry standards applicable to your organization and data.
- [ ] Implement governance policies and procedures for cloud usage, including procurement, deployment, and decommissioning of resources.
- [ ] Conduct regular compliance audits and assessments to ensure adherence to security standards and regulations.

6. **Incident Response and Recovery:**

- [ ] Develop and maintain an incident response plan outlining roles, responsibilities, and procedures for responding to security incidents.
- [ ] Conduct regular security assessments and penetration tests to identify vulnerabilities and weaknesses in cloud infrastructure and applications.
- [ ] Establish communication channels and partnerships with cloud service providers and security vendors for incident reporting and collaboration.

Monitoring and Logging:

- [ ] Enable logging and monitoring of cloud infrastructure, applications, and user activities.
- [ ] Set up alerts and notifications for suspicious activities, security events, and resource utilization anomalies.
- [ ] Regularly review and analyze logs and monitoring data to detect and respond to security incidents promptly.

7. **Training and Awareness:**

- [ ] Provide security awareness training to employees, contractors, and partners on cloud security best practices, policies, and procedures.
- [ ] Conduct regular security drills and simulations to test incident response capabilities and employee readiness.

8. **Cloud Provider Security Assurance:**

- [ ] Understand the security measures and assurances provided by the cloud service provider (CSP) and ensure they align with your organization's security requirements.
- [ ] Review and assess the CSP's security certifications, compliance reports, and audit findings to evaluate their security posture.
- [ ] Establish clear roles and responsibilities for security management, including shared responsibility for security between the organization and the CSP.

9. **Continuous Improvement:**

- [ ] Regularly review and update cloud security policies, procedures, and controls to adapt to evolving threats and regulatory requirements.
- [ ] Conduct post-incident reviews and lessons learned sessions to identify areas for improvement and implement corrective actions.
- [ ] Stay informed about emerging cloud security trends, best practices, and technologies to enhance your organization's security posture over time.

HANIM EKEN

https://ie.linkedin.com/in/hanimeken