**Assignment Topic: Backup System Security Analysis and Baseline Assessment**

Introduction

This assessment assesses backup system security and suggests strategies to protect the backup infrastructure, ensuring data availability and integrity in the face of disasters, breaches, or attacks.

**Generic Challenges:**

* Unencrypted backup data
* Inadequate access controls
* Lack of backup restoration testing
* Vulnerability to ransomware attacks
* Compliance with industry regulations
* Archival requirements

**Business-Specific Challenges:**

* GDPR-compliant backups
* Data protection during audits
* Ransomware resilience
* Limited resources for backup integrity testing

**Brief Discussion of Standards Relevant to the Business**

* **GDPR (General Data Protection Regulation):** Backup systems must comply with GDPR by ensuring secure data handling and maintaining data integrity during storage and transmission.
* **"NIST SP 800-34" (National Institute of Standards and Technology (NIST), 2010):** This standard guides contingency planning, maintaining backup system integrity and availability during disruptions.
* **"ISO/IEC 27031" (ISO/IEC, 2011):** Emphasises ICT readiness for business continuity, highlighting security practices, encryption, and access control in backup systems for business resilience.

**Bulleted/Tabular List of Tools and Justifications**

|  |  |  |
| --- | --- | --- |
| **Tool** | **Justification** | **Challenges Addressed** |
| **Veeam Backup & Replication** | **Comprehensive backup and recovery with encryption and access control.** | **Unencrypted data, access controls, backup testing** |
| **Acronis Backup** | **Specialises in backup security with ransomware protection and encryption.** | **Ransomware attacks, data encryption** |
| **HashiCorp Vault** | **Securely manages backup encryption keys and secrets.** | **Secure storage of encryption keys, access control** |
| **Commvault** | **Scalable backup solutions with encryption, access control, and compliance features.** | **Compliance (GDPR), access control, scalability** |
| **Wireshark** | **Detects unsecured transmissions in network traffic during backups.** | **Detection of unsecured data transmission, monitoring** |
| **Splunk** | **Log management enables security incident detection in backup systems.** | **Security incident detection, log analysis** |

**Methodology**

* **Type:** Combination of remote and local assessments, based on the backup system setup and geographical location.
* **Automation:** Automated backup will use Veeam, Acronis, and Commvault for encryption and data backups.
* **Manual Tasks:** Manual inspection for encryption settings, access controls, and network traffic analysis will be performed with Wireshark.
* **Testing Environment:** Testing will be done in isolated environments to avoid production impact, with regular schedules to maintain backup integrity.

**Discussion on Available Models/Methodologies/Tools and Approaches**

* **Backup and Recovery Models:** Veeam and Acronis provide secure and efficient automated backups. Commvault supports scalable enterprise backup with compliance features.
* **Encryption and Secrets Management:** HashiCorp Vault ensures encryption key management for backup and recovery operations.
* **Network Traffic and Log Analysis:** Wireshark and Splunk analyse data transmissions and monitor logs for security threats, identifying unsecured transmissions and detecting incidents through log monitoring.

**Selection of Methods/Tools/Approaches**

* **Primary Tools Selected:** Veeam Backup & Replication, Acronis Backup, HashiCorp Vault, Commvault, Wireshark, Splunk.
* **Approach:** Automated and manual methods will cover security challenges with remote monitoring and localised testing.

**Business Impacts on Use of Tools and Methods**

* **Out-of-Hours Scanning:** Veeam and Acronis will back up during off-peak hours to minimise system disruption.
* **Network Traffic:** Wireshark's analysis may cause slowdowns, but scans will be scheduled during maintenance windows to reduce impact.
* **Processing Demand:** Splunk's log monitoring affects system processing demands. Thresholds balance performance and security monitoring.

**Timeline of the Completion of the Task**

|  |  |
| --- | --- |
| **Week** | **Task** |
| **Weeks 1-2** | **First evaluation of backup timing, encryption techniques, and access control setups.** |
| **Week 3** | **Utilise monitoring software (e.g., Splunk) and perform testing to verify the integrity of backup data.** |
| **Week 4** | **Evaluate resilience against ransomware using HashiCorp Vault for encryption management.** |
| **Week 5** | **Perform restoration testing and confirm adherence to GDPR and other applicable regulations (e.g., Commvault).** |
| **Week 6** | **Prepare the final report, including detailed recommendations and an executive summary.** |

**Summary of Limitations and Assumptions**

* **Limitations:**
  + Backup integrity testing may not cover all formats due to limited time and resources.
  + Automated tools may not detect specific misconfigurations or human errors.
  + Ongoing monitoring and verification are needed to prevent ransomware attacks on backups.
* **Assumptions:**
  + Backup systems are aligned with the organisation's security policies.
  + Data is compliant with GDPR and relevant regulations.
  + Testing is performed in non-production environments to prevent disruptions.

**Learning Outcomes Addressed**

1. **Identify and analyse security threats and vulnerabilities in network systems and determine appropriate methodologies, tools, and techniques to manage and/or solve them:**
   * Solutions selected to address encryption, access control, and network monitoring challenges. Veeam, Acronis, and Wireshark are chosen as appropriate tools.
2. **Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues:**
   * The careful evaluation of tools like Splunk, HashiCorp Vault, and Commvault demonstrates a thoughtful approach to risk mitigation and security maintenance.

**References**

National Institute of Standards and Technology (NIST), 2010. *Contingency Planning Guide for Federal Information Systems* (NIST Special Publication 800-34 Rev. 1). Gaithersburg, MD: NIST.

ISO/IEC, 2011. *ISO/IEC 27031:2011 - Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity*. Geneva: International Organization for Standardization.