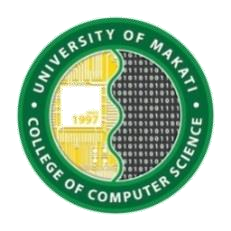
 **UNIVERSITY OF MAKATI**



J.P. RIZAL EXT. WEST REMBO MAKATI CITY

|  |  |  |  |
| --- | --- | --- | --- |
| **NAME** | **DELABAJAN, CALVIN P.** | **ESIGN** |  |
| **YR & SECTION** | **IV - BINS** | **DATE** | **09/04/2024** |

**INFORMATION ASSURANCE AND SECURITY 2 (IAS2)**

**ACTIVITY 1: SECURITY MEASURES**

1. **APPLICATION SECURITY**

* **Vulnerability Detection**
* Implementing a method that utilizes historical network logs to detect vulnerabilities in real-time can significantly improve protection efficiency. This involves analyzing network packets for harmful data and applying a vulnerability detection policy based on past logs.
* The integration of machine learning techniques can further enhance vulnerability detection by identifying patterns indicative of potential threats.
* **Network Filtering**
* Deploying a virtual machine set for security filtering can streamline the complexity of security equipment while ensuring robust protection for service systems. This method allows for tailored security measures based on specific service requirements.
* **Business Process Security**
* Establishing a security model that focuses on business process elements ensures that applications operate securely and logically. This model defines safe attributes and conducts consistency tests to maintain security throughout the application lifecycle.

1. **CLOUD SECURITY**

* **Encryption**
* Essential for safeguarding data both at rest and in transit, encryption techniques ensure confidentiality and integrity of sensitive information.
* **Identity and Access Management (IAM)**
* IAM systems, along with multi-factor authentication (MFA), bolster user verification processes, reducing the risk of unauthorized access.
* **Intrusion Detection Systems (IDS)**
* These systems monitor for suspicious activities, providing real-time alerts and enhancing threat detection capabilities.



1. **INFRASTRUCTURE SECURITY**

* **Network Segmentation**
* This is used to contain the spread of an attack within a company and differentiate critical systems from non-critical ones.
* **Firewalls and Intrusion Detection/Prevention Systems (IDPS)**
* Maintains network integrity by monitoring, detecting, and blocking unauthorized traffic.
* **Access Controls (RBAC)**
* Ensures that only appropriate personnel access sensitive systems via role-based àccess controls.
* **Regular Vulnerability Patches**
* All systems are patched and updated regularly for known vulnerabilities
* **Encryption**
* helps to keep sensitive data safe and encrypted in rest & transit.
* **Endpoint Protection**
* The idea is used to prevent malware and advanced threat defending for clients, including antivirus software.
* **Continuous Monitoring and Logging**
* can detect suspicious activities by continuously monitoring network events, later respond if any is found.

1. **ENDPOINT SECURITY**

* **Antivirus and Anti-Malware**
* Antiviruses / anti-malwares are deployed to safeguard endpoint.
* **EDR**
* utilized based on the use case with advanced threat detection and response
* **Data at rest encryption**
* Encryption data on the endpoint so that if a lost or stolen by device, contents cannot be deciphered.
* **Patch Management**
* Keep endpoint software current and patch vulnerabilities ·
* **User training**
* Further, users need to be trained in basic security practices like phishing and password management.

1. **EDGE SECURITY**

* **Risk Analysis and Standards**
* Multi-access edge computing (MEC) must address security risks associated with technologies like network slicing and virtualization. Implementing ISO/IEC 27001:2022 controls can help manage these risks effectively.
* **Data Protection Techniques**
* A novel edge data security schema utilizing spike modulation and backscatter communication has been proposed to safeguard RFID-based devices against common threats like denial of service attacks.
* Physical layer security mechanisms, such as friendly jamming, can protect data confidentiality during uploads in MEC by degrading attackers' capabilities.
* **Access Control Mechanisms**
* Efficient access control is crucial in information-centric edge networking. Confidentiality-enhanced network coding allows for secure data transmission while enabling user revocation without significant overhead(Wu et al. 2021).

1. **CRYPTOGRAPHY**

* **Encryption and Decryption**
* The primary function of cryptography is to convert readable data into an unreadable format (encryption) and back (decryption) using algorithms like RSA and elliptic curve cryptography (ECC).
* **Data Integrity**

- Techniques such as hashing and digital signatures ensure that data remains unaltered during transmission, thus maintaining its integrity.

* **Authentication and Non-repudiation**
* Asymmetric key algorithms and digital certificates are utilized to verify identities and ensure that actions cannot be denied later.

1. **INCIDENT RESPONSE**

* **Cybersecurity Management**
* A robust cybersecurity management framework should focus on integrity, authentication, and availability of information assets. This involves continuous monitoring and the use of advanced detection tools to identify potential threats.
* Systematic approaches to intrusion detection are necessary to manage and contain security breaches, thereby mitigating losses and maintaining operational integrity.
* **Data Protection Compliance**
* Incident response must also consider data protection regulations, such as GDPR, to avoid privacy risks associated with processing personal data during security incidents. This requires balancing IT security measures with legal obligations.



1. **VULNERABILITY MANAGEMENT**

* **Vulnerability Scanning and Management**
* A robust vulnerability management system automates the scanning of network devices, generating reports that prioritize vulnerabilities based on severity.
* This system includes a notification mechanism to ensure timely remediation of identified vulnerabilities, enhancing overall security posture.
* **Risk Assessment and Prioritization**
* Effective risk management involves identifying and evaluating potential security risks, allowing organizations to prioritize vulnerabilities based on their impact and likelihood.
* Tools that digitize vulnerability reports can help in setting countermeasure priorities, ensuring that high-risk vulnerabilities are addressed first.
* **Coordinated Vulnerability Disclosure**
* Implementing a coordinated vulnerability disclosure (CVD) policy encourages collaboration with ethical hackers, facilitating the identification and reporting of vulnerabilities while minimizing legal risks.

1. **DISASTER RECOVERY**

* **Cybersecurity Integration**
* Incorporate strong cybersecurity measures into disaster recovery plans, focusing on backup and recovery protocols, data encryption, and access controls to mitigate risks during recovery phases.
* **Data Protection Techniques**
* Employ consistent data backup and recovery methods, utilizing cloud-based solutions and physical security measures to safeguard sensitive information from loss or unauthorized access during disasters.
* **Advanced Technologies**
* Leverage IoT technologies to enhance data verification and validation, ensuring reliable communication channels and minimizing information overload during disaster events.
* **Secure Transmission and Storage**
* Implement secure transmission protocols and storage encryption to protect backup data, ensuring that data remains secure throughout the recovery process.



1. **HEALTH DATA MANAGEMENT**

* **Temporal Hash Signature**
* This method enhances data integrity by linking records and verifying them through temporal signatures, addressing risks from cyber-attacks like ransomware.
* **Four-Layer Security Framework**
* Incorporating data encryption, granular access control, and activity monitoring, this framework optimizes storage while ensuring privacy in healthcare data management.
* **Vulnerability Assessment**
* Identifying and addressing vulnerabilities in big data management systems is crucial, as these systems are increasingly targeted by cyber threats.
* **IoT Security Protocols**
* With the rise of IoT in healthcare, implementing robust security measures to protect connected medical devices from external attacks is vital.

1. **DIGITAL FORENSICS**

* **Encryption and Access Controls**
* Implementing strong encryption protocols and strict access controls is essential to protect sensitive information from unauthorized access and breaches.
* **Network Security**
* Utilizing firewalls, intrusion detection systems, and regular security audits can help defend against cyber-attacks targeting digital assets.
* **Database Forensics**
* This involves identifying and analyzing cyber threats at the database level, which is crucial for investigating and mitigating attacks.
* **Incident Response**
* Establishing a robust incident response plan, including forensic investigations and recovery strategies, is vital for minimizing damage from security breaches.

**REFERENCES:**

1. Peng, Xu., Meirong, Chen., Lifang, Feng., Guanfeng, Wu., Fangli, Ma., Danchen, Wang. (2017). (4) An application security model based on business process in information system. doi: 10.1109/ISKE.2017.8258785
2. H, Lalchhanhima., Lalrintluanga, Sailo., ., Malsawmtluangi., N, Venkatesan., Lalhmingmawia, Kawlni., C, Lalramliana. (2024). (1) Security Systems in Cloud Computing. doi: 10.53555/kuey.v30i5.5858
3. Bernadette, Fleury., Philippe, Loudenot., M., Suszko., Sandrine, Fourel., X., Kapola., Julien, Langrand-Escure., Jean-Baptiste, Guy. (2022). (6) Sécurisation du système d’information des structures médicales. Cancer Radiotherapie, doi: 10.1016/j.canrad.2022.06.032
4. Quan, Shen., Yanming, Shen. (2023). (1) Endpoint Security Reinforcement via Integrated Zero-Trust Systems: A Collaborative Approach. doi: 10.1016/j.cose.2023.103537
5. Alina, Florina, Glavan., Daniel, Gheorghica., Victor, Croitoru. (2023). (1) Multi- access edge computing analysis of risks and security measures. Revue Roumaine Des Sciences Techniques-serie Electrotechnique Et Energetique, doi: 10.59277/rrst-ee.2023.68.2.15
6. Swati, Chaudhari., Archana, Thakur., Alpana, Rajan. (2023). (2) Securing Digital Information Using Cryptography Techniques to Enhance IT Security. doi: 10.37256/rrcs.2320232635
7. Alin, Zamfiroiu. (2022). (2) Cybersecurity Management for Incident Response. Romanian Cyber Security Journal, doi: 10.54851/v4i1y202208
8. Valéry, Vander, Geeten. (2024). (5) How can national policies support the development and implementation of coordinated vulnerability disclosure?. doi: 10.69554/woer4540
9. Sandeep, Reddy, Gudimetla. (2024). (1) Cybersecurity Considerations in Disaster Recovery Planning. International Journal for Research in Applied Science and Engineering Technology, doi: 10.22214/ijraset.2024.62253
10. (2023). (1) Information security protection for eHealth records using temporal hash signature. International Journal of Intelligent Enterprise, doi: 10.1504/ijie.2023.127233
11. Rexhep, Mustafovski. (2023). (1) Ensuring information security in the digital age. doi: 10.46763/etima2321119m