**COMP718**

**Tutorial 2 - Governance and strategic planning for security**

**This tutorial comprises a problem-oriented exercise (Task 1) and one review task (Task 2).**

**Task 1. Controls, threats, vulnerabilities**

You are a security consultant. You have been commissioned by a university that offers most of its programmes online, to help them develop their InfoSec programme. As part of your work, you are using the article below. You have found table 14, 15 and 16, and Figure3 very helpful in understanding the risk environment in a typical higher education (HE) institution. You are of the view that the findings summarised in **Table 16 apply to the university you are working for.** Your next step is to suggest appropriate security controls that could become part of your university’s InfoSec programme

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39.  [https://www.mdpi.com/1999-5903/13/2/39](https://www.mdpi.com/1999-5903/13/2/39 )

1. **Suggest operational, technical and managerial security controls that would be appropriate for handling DoS/DDoS attacks.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident | Vulnerability | Threat | Asset under threat | Incidents consequences |



***Handling DoS/DDoS Attacks***

* **Incident:** Denial of Service (DoS) / Distributed Denial of Service (DDoS) attacks
* **Vulnerability:** Insufficient network defense mechanisms
* **Threat:** Attackers using network flooding techniques
* **Asset under Threat:** Online services and network infrastructure
* **Incident Consequences:** Service outages, degraded performance, loss of availability

1. **Managerial Controls:**
2. Develop and enforce an incident response plan specifically for DoS/DDoS scenarios.
3. Conduct regular training for staff to recognize and respond to DoS/DDoS attacks.
4. Establish a communication plan for informing stakeholders during and after an attack.
5. **Operational Controls:**
6. Implement network monitoring to detect unusual traffic patterns.
7. Perform regular vulnerability assessments and penetration testing on the network infrastructure.
8. Collaborate with ISPs and use services that provide DDoS mitigation.
9. **Technical Controls:**
10. Deploy firewalls and intrusion prevention systems (IPS) with anti-DDoS capabilities.
11. Use rate limiting and traffic shaping to manage incoming traffic loads.
12. Implement redundant systems and failover mechanisms to maintain service availability.

b**) Suggest operational, technical and managerial security controls that would be appropriate for handling abuse and misuse incidents.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Incident | Vulnerability | Threat | Asset under threat | Incidents consequences |



***Handling Abuse and Misuse Incidents***

* **Incident:** Abuse and misuse of university IT resources
* **Vulnerability:** Inadequate access controls and monitoring
* **Threat:** Internal or external users exploiting IT resourc es for unauthorized purposes
* **Asset under Threat:** IT infrastructure, sensitive data
* **Incident Consequences:** Data breaches, legal implications, reputational damage

1. **Managerial Controls:**
2. Establish clear usage policies outlining acceptable and unacceptable behaviors.
3. Provide regular training and awareness programs for all users.
4. Develop a reporting mechanism for abuse and misuse incidents.
5. **Operational Controls:**
6. Monitor user activities and implement logging to track access and usage patterns.
7. Conduct periodic reviews and audits of user permissions and access rights.
8. Establish disciplinary procedures for policy violations.
9. **Technical Controls:**
10. Use access control systems to enforce user authentication and authorization.
11. Implement data loss prevention (DLP) tools to monitor and control data transfers.
12. Deploy endpoint security solutions to detect and prevent misuse of IT resources.

**Task 2. Review the concept of planning and answer the following questions**

|  |  |
| --- | --- |
| What are the three common levels of planning? |  |
| What is strategy? |  |
| What is InfoSec governance? |  |