Information Technology

[Name of the Writer]

[Name of the Institution]

Information Technology

Organizations perform risk assessments to ensure that they are able to identify threats which include viruses, malware, and attackers to their information systems. Risk assessment addresses the potential inauspicious impacts to organizational operations and assets which are caused by the threats which the organization is facing. Risk assessment represents the risks level which organizations are facing so that it helps an organization to identify the different levels and create suitable risk mitigation plans according to threats.

Risk mitigation is one of the risk management activity in which only selected risks are being treated. There are many risk mitigation strategies which are used to deal with different types of risks. The strategies which are used for risk mitigation are risk acceptance, risk reduction, risk transfer and risk avoidance (Yoon, 2018). Risk acceptance is that in order to reduce the impact of risk there are no actions which are taken and accept the identified risk, risk reduction is that measures are taken at a certain level of acceptance to reduce the risks, risk transfer is the process of transferring the risks in other entities and risk avoidance is that the company don't take decisions which will cause risk in their operations. Risk reduction strategy always must be applied according to the situation.

**Different threats**

* IP address spoofing
* Denial of Service attacks (DoS)
* Distributed Denial of Service attacks (DDoS)
* Packet analysis/sniffing
* Session hijacking attacks
* SQL Injection Attack

These threats cause different vulnerabilities in the system. IP address spoofing is the act of making a fake source IP address to hide the identity of the attacker and launching a DoS attack. Attackers will use IP spoofing to get access to the sensitive data of the organization and not allow them to identify the identity of an attacker using spoofing (Various types of network attacks, 2019). Denial of service attacks causes vulnerabilities like disturbance or delay of services by swamping it with large quantities of useless traffic. When Denial of service attacks are launched server will not be able to answerable to the requests from the users. These types of threats are very common as many organizations have to face daily problems of slow network performance, a slow response time of the server, unavailability of the web page and most importantly they can't access to their data (Various types of network attacks, 2019). Distributed Denial of service attacks also causes such type of issues, but they occur differently where multiple infected systems swamp a particular host with traffic concurrently (Various types of network attacks, 2019).

Packet sniffing is the procedure of seizing data packets which are travelling in a network. It is mainly used by the organization to analyze the traffic of the network and finding any suspicious traffic in the network (Various types of network attacks, 2019). Session hijacking attacks are used to attempt unauthorized access to information or services in someone’s system. They allow hackers at one point of the network to take part in a conversation between others network and allow the IP data packets to pass through that point (Various types of network attacks, 2019). Similarly, SQL injection attacks are very common these days. Hackers use the current sensitivity in the database or systems to inject their code for execution that changes the data from the database and also allows hackers to become administrator of a database so that they can create changes in the existing database (Various types of network attacks, 2019).

|  |  |  |
| --- | --- | --- |
| **Threats Identification** | | |
| Threat attacks on Vulnerabilities | Potential Hacking actors | Types of remediation and mitigation techniques |
| IP address Spoofing | Attackers who engage in targeted attacks which are driven by profits | Packet filtering is the best technique to defend the IP address spoofing and design network protocols which don't allow unidentified IP address authentication |
| Denial of Service attack | Opportunistic who are usually amateur hackers and those attackers who want to damage the organization | The only way to detect these attacks is to block unusual traffic on the network |
| Distributed Denial of Service attack | Opportunistic who are usually amateur hackers and those attackers who want to damage an organization | The DDoS is also detected in the same way as DoS attack. There are different tools which can help in identifying such attacks |
| Packet analysis/sniffing | IT professionals in the company and Internal user error | The best method of countermeasure against packet sniffing is to use encrypted communication |
| Session hijacking attacks | Hackers who are having stolen session cookie to gain access usually these are inside the organization | Apply encryption to the traffic which is passed between networks |
| SQL injection attacks | These types of attacks are usually created by competitors in the market, and the attackers are usually government sponsored in this case | These types of attacks can be prevented by using only parameterized statements, limit the permission on the database and check the pattern of the query. |

Federal Information Security Modernization Act (FISMA) has implemented an information security plan to protect the confidentially, integrity and availability of its information resources. The risk management serves as a foundation on which the risks are controlled. The POAM is an action plan which helps the organization to identify and assess information security and privacy weaknesses. It is the requirement of every organization where a weakness of security and privacy has been found.

Risk management strategy is essential for every organization. Every organization is facing massive challenges in their business operations. Cyber-attacks are the biggest threat which organizations are facing, and they need to sort out how they can control this risk. Organizations need to build a strategy in which they define which products and services are required for their business operations and how they will impact the business. One of the most important sources which will guide an organization in implementing their security policies is the NIST Cybersecurity framework (Shen, 2013). This framework defines what core functions are required for an organization to implement in their security program. These functions are Identify, Protect, Detect, Respond and Recover. Similarly, there are other frameworks and standards which can help in guiding organizations in creating a strong security policy.

**References**

Shen, L. (2013). NIST Cybersecurity Framework: Overview and Potential Impacts, The. *SciTech Law.*, *10*, 16.

Yoon, J., Talluri, S., Yildiz, H., & Ho, W. (2018). Models for supplier selection and risk mitigation: a holistic approach. *International Journal of Production Research*, *56*(10), 3636-3661.

*Security 1:1 - Part 3 - Various types of network attacks | Symantec Connect*. (2019). *Symantec.com*. Retrieved 31 January 2019, from https://www.symantec.com/connect/articles/security-11-part-3-various-types-network-attacks