**Security Recommendations For An IT company’s database to be prevented from ransomware attacks.**

**Introduction**

The recommendations to be implemented to protect the information security and networking company from being a victim of an attack is discussed in the report. Firstly, the possible cause of the attack is discussed. Then, the preventive measures to be taken to prevent the any kind of attack in the database is discussed. The report is divided into two sections that discusses the points of errors and the methods to prevent them. This report focuses on all the security design concepts is simple but effective and can be implanted by the IT staffs of the company easily.

**A. Possible causes of the ransomware attack:**

1. **Network Security**

The main point for network security comes from network management. The creation of new networks of an existing network is the everyday work of networking professionals. It is a term that has been gaining traction in recent years due to the increasing complexity and sophistication of cyber-attacks. It is essentially the implementation of security measures to protect networks, systems, and resources from malicious activity. These measures can include firewalls to control data flow, encryption techniques to safeguard confidential information, and authentication protocols to verify users who attempt to access sensitive data. Moreover, network security also consists of the prevention of malicious software from attacking or entering the computer system in the first place.

There can be many reasons that may have caused the attack that encrypted the entire backend database.

1. A human error is the foremost reason that causes a failure of the network security. A malicious email that reads log in and reboot stating a cause of “system maintenance” may have been sent from a hacker’s side to any one of the two IT staff working for the company.
2. Services that might not be necessary for the company could be one of the main reasons why the data was encrypted. These kinds of services are the main target for hackers to get into the system and take over the data.
3. The company may not have updated their system daily. Many computers/devices when not updated regularly can be attacked by hackers to steal information. It also gives them a chance to create a Denial of Server attacks.
4. The password that protects the company’s system may have been a weak one. This is one of the main reasons why hackers find it easy to break-into the system.
5. Given the internet used by the company (Bell) which allows both internet access to the internal users and provides access from outside from web server, it may enable the internal people working in the company to cause the ransomware.
6. **Application Security**

While coming into terms with the possible causes due to the compromise on the network security, there are threats that come with the application used by the company. Since the company uses two VMs for the web and a Database hosting application, the following vulnerabilities might also be the cause of the ransomware.

* 1. There may have been a breach on the database used by the company in terms of configuration, authentication, and communication.
  2. When a database is not developed properly, it leaves behind weak holes that can make it easier for the hacker to encrypt the database.
  3. SQL Injection in an application security makes a request to the application to give back the records from the account table and injections can change the data that results in the loss of the entire database application.
  4. Cross-site scripting uses data that is not fully validated and trusted. When not validated properly, the hacker can send the company’s ID to its own website that gives the hack a leverage to the company’s application.
  5. If there is a broken authentication, hackers can have full control over the company’s database system.
  6. Sometimes, discrete data of the company may also be exposed to a public platform which can cause a data compromise. These may include any credit/debit cards belonging to the company’s name, passwords of the system and other important credentials.

The database application of the company can also be encrypted if there is a server-side request forgery. It is also a type of application security vulnerability that gives the hacker permission to induce the server-side application to make a request to an anonymous location. It makes the connection to only an internal service that falls within the company’s structure.

**B. The recommendations to prevent any future attacks are given below:**

1. **Network Security Recommendations:**

The recommendations for the possible issues of network security are given as:

a. Implement a firewall to control access to the internal network and the web server. The firewall should be configured to limit access to only the services that are necessary for the business to run. This will prevent unauthorized access to the servers and the data stored on them.

b. Implement a secure network architecture with segmentation. Separate the web server from the application/DB server with two separate networks. This will limit the potential damage from an attack as only one network will be affected.

c. Implement a secure wireless network for guests. This will ensure that guests accessing the network have a secure connection and don't have access to the internal network.

1. **Application Security Recommendations:**

The recommendations for the possible issues of application security are given as:

a. Implement secure coding practices to ensure that the applications are secure and free from vulnerabilities.

b. Perform regular security testing of the applications to identify and fix any security issues before they can be exploited.

c. Implement an application whitelisting solution to limit the applications that can run on the system and prevent malicious applications from running.

1. **Endpoint Management Recommendations:**

End point management is the practice of managing devices, such as computers, mobile phones, and tablets, on a network. This includes ensuring that the devices meet security requirements, such as having the latest security patches installed, running up-to-date anti-malware software, and enforcing strong passwords. Additionally, regularly monitoring the devices and enforcing policies such as preventing users from accessing unauthorized websites can help ensure that the network remains secure.

The database can also be protected with the measures using the endpoint management methods. They are given as:

a. Implement a centralized endpoint management solution. This will allow IT staff to centrally manage and deploy security policies to all endpoints.

b. Implement a patch management solution to ensure that all endpoints are up to date with the latest security patches.

c. Implement endpoint anti-virus and anti-malware solutions to protect the endpoints from malicious software.

d. Implement endpoint security policies to ensure that all endpoints are configured securely.

1. **Access Management Recommendations:**

Access management is the practice of controlling who is authorized to access a system and what type of access they have. This can be done by implementing an identity and access management system that requires users to authenticate before accessing the system. Additionally, implementing role-based access control, such as limiting certain users to specific areas of a system, can help ensure that only authorized users have access to the system.

While pointing down the recommendations for the database to be free from any attacks, the access management for the database also should be considered. They are given as:

a. Implement access control policies to ensure that only authorized personnel have access to the system.

b. Implement multi-factor authentication for all access points. This will ensure that only authenticated users can access the system.

c. Implement a password policy to ensure that all passwords are secure and regularly changed.

1. **Defence in Depth Recommendations:**

Defence in depth is the practice of implementing several layers of security to protect a system. This can include implementing firewalls, intrusion detection systems, and segmenting the network into different zones. Additionally, regularly monitoring the system and ensuring that the appropriate security measures are in place can help ensure that the network remains secure.

Defence in depth is a solid security method that can be applied to protect the database.

It is composed of five layers. The attack preventive measures to protect the system is given as:

a. Implement a security incident and event management system to monitor the network for any suspicious activity.

b. Implement a log management solution to collect and monitor all logs from all systems.

c. Implement a backup and recovery solution to ensure that any data loss can be recovered quickly.

d. Implement an Intrusion Detection System (IDS) to monitor the network for any malicious activity.

e. Implement a Data Loss Prevention (DLP) solution to ensure that any sensitive data is not leaked outside the network.

Overall, these measures should be implemented to ensure that the company's networks and applications are secure. The IT staff should be properly trained to ensure that they understand the security measures that need to be implemented and how to properly configure them. Additionally, the company should regularly monitor their systems and enforce security policies to ensure that the network remains secure.

**Figure: Diagram showcasing the layers of security for the company’s database.**

**Diagram

Description automatically generated**

**Conclusion:**

In conclusion, it is essential to implement the appropriate security measures to ensure that the company's networks and applications are secure. The company ought to regularly monitor their systems and put their security policies into effect, in addition to providing the IT staff with the appropriate training. In addition, a comprehensive backup and recovery plan, an incident response plan, and regular security testing should be implemented to guarantee that the company will be able to defend itself against potential attackers and quickly recover from any security incidents that may occur.

**References:**

Complete Guide to Application Security*.* (n.d.). *Snyk.* <https://snyk.io/learn/application-security/>

Center for Internet Security. (n.d.). *Election Security Spotlight – Defense in Depth (DiD).* CIS.

<https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did>