Design Document:

Risk Assessment Tool That Calculates the Type, Cost And Likelihood of Breaches.

Institute of Technology Carlow

Department of Computing & Networking

Student Name: Eimhin Lane
Student Number: C00240680

Table of Contents

Introduction:

We look at the various questions that can be asked in a risk assessment system, alongside the effects of how you handle these questions. These can be better used to develop our tool and help count the different types of threats when using the tool.

Types of Questions:

The questions are formed from the knowledge gained over the course, with the necessity to learn how to identify threats and what leaves you open to attack. The questions as seen are also added to by various sources such as documentation from the University of North Dakota[1], Tetra Defence[2] and IT Governance[3].

The variety of questions asked by the questionnaire can be varied with a myriad of options available to choose from. Each of these questions need to peer deeply into the technical aspects of a company and workplace vigilance for updates and keeping hardware secure and monitored. Some examples of the type of questions asked to monitor the security of a company are such;

How frequently do you experience loss events in a year?

What is the type of data you store?

How much is stored on site?

How routinely do you perform backups?

Where are your backups stored?

Number of phishing emails received in a year?

Is your software up to date?

Are you using older hardware?

Do you store all information in a single location?

How much is stored on cloud?

How many employees do you have?

How many end user devices?

Mobile laptop desktop(company devices) How many end points are on your network?

What protections are on your network?(firewalls, proxies, intrusion detection)

What operating systems are you running?

What versions of operating systems?

Whats the applications used(Microsoft offices apps, etc…)?

What browser do you use? What anti-virus software do you use?

Which anti-virus, on what devices?

How many clients do you service?

Attacks:

List of all methods of attacks, listing how each attack is perpetrated. If a user's answer implies any of the list points it will add a point to a count for that attack. When finished points are tallied and whichever has the most is the attack you are most likely to experience in the timeframe of a year.

Virus –

•Primarily Targets Windows Devices.

•Higher employee count increases odds of poor passwords.

•Lack of Anti-virus

•Lack of daily system scans

•Not regularly updating

•Lack of backups

Trojan –

•Generally received from scam emails/phishing emails.

•Not regularly updating

•Lack of Anti-virus

•Lack of site restrictions

•Lack of daily system scans

•Lack of backups

Worms –

•Generally received from scam emails/phishing emails.

•Unrestricted email/website downloads.

•Lack of Anti-virus

•Higher employee count will allow the worm to spread more.

•Lack of daily system scans

•Lack of backups

Ransomware Attack –

•No monitoring of background tasks

•No regular backups

•Targets medium sized businesses

•High Income

•Unrestricted email/website downloads

•Not up to date equipment

Man in the Middle –

•Unsecured internet

•Generally received from phishing emails.

•No monitoring of background tasks

•No VPN employed

•Servers up to date

•Deny non-https websites

SQL Injection –

• No input White list

•No parametered statements

•Not utilising character escaping

•No web application firewall

•No sanitisation of user inputs

•Lack of proper database error messages

Zero Day Exploit –

•Not enforcing restrictions for websites and emails

•Up to date software and hardware

•Not monitoring background activities

•No proper firewall

•Lack of backups

•Lack of daily system scans

Questions List:

Question: How many users do you have?

Effects(High): Virus, Worms

Effects(Medium): Ransomware

Question: Do you use windows?

Effects: Virus

Question: Do you use Anti-virus?

Effects: Virus, Trojan, Worms

Question: Do you perform daily or near daily scans?

Effects: Virus, Trojan, Worm, Zero Day Exploit

Question: Are your hardware and software up to date?

Effects(No): Virus, Trojan, Ransomware, Man in The Middle

Effects(Yes): Zero Day Exploit

Question: Do you backup regularly?

Effects: Virus, Trojan, Worm, Ransomware, Zero Day Exploit

Question: Do you receive many scam emails?

Effects: Trojan, Worms, Man in The Middle

Question: Do you implement website/email access and download restrictions?

Effects: Trojan, Worm, Ransomware, Man in the Middle, Zero Day Exploit

Question: Do you monitor background tasks consistently?

Effects: Ransomware, Man in The Middle, Zero Day Exploit

Question: What is your average income?

Effects: Ransomware

Question: Do you have a secure internet connection?

Effects: Man in The Middle

Question: Do you use a VPN?

Effects: Man in The Middle

Question: Do you implement White list for inputs?

Effects:6 SQL Injection

Question: Do you parameterise statements?

Effects: SQL Injection

Question: Do you utilise character escaping?

Effects: SQL Injection

Question: Do you utilise a firewall?

Effects: SQL Injection, Zero Day Exploit

Question: Do you sanitize user inputs?

Effects: SQL Injection

Question: Do you display database error messages on the front end?

Effects: SQL Injection

Prevention:

Virus:7

Viruses, often hidden as decoy .exe files, can be prevented through relatively straight forward means. Ensure your employees know the importance of password complexity. Utilise a good Antivirus to keep your system safe and automate more tedious tasks such as perform regular system scans. Keeping backups can be worthwhile as it will allow you to get back on your feet faster if you end up compromised.

Trojan:

Trojans establish a backdoor for hackers to enter your system. Prevention begins with caution, don't install any software from emails without confirming the sender is not malicious. If in a larger company, you may need to implement restrictions on various websites and sources. As it is with many cases of security keeping up to date and utilising an Anti-virus can vastly improve protection from a Trojan attack. If in the event these preventative measures are not enough you may need to rely on backups to restore systems to a safe state, as such regular backups are necessary.

Worms:

When suffering from a worm it can result in massive losses due to its highly infectious spreading methods. Preventing worms can be helped through limiting the reliance on the internet. Worms can easily spread through connections, the internet being no different as such limit website access and email downloads. Additionally keeping your system spread across various servers with few connections can help slow the spread of a worm. In the event of a worm attack limit employee connectivity to one another on the system as more employees means more targets and damages.

Ransomware:

Ransomware can be costly, so prevention is very important. The best method to avoid ransomware is to not click unsolicited download links in emails. Ensure you are up to date in both software and hardware terms. Tracking background tasks can ensure you know what is running on your system

and can help you understand if you're in the process of being compromised. Backups are entirely necessary to counter Ransomware, though the backup must be kept on another device from yours. Backups can completely bypass the threat ransomware can pose.

Man in The Middle:

A man in the middle attack is one that best succeeds under poor network security conditions. Improving your network security will prevent an intruder from intercepting. VPNs can help you avoid any malicious users who are attempting to intercept your packets. Avoid insecure sites, anything that isn't https should be considered a threat. Keep updated, avoid phishing emails and monitor background tasks to best counter these attacks.

SQL Injection:

The best way to avoid an SQL Injection is sanitisation of code. Implementing secure methods such as white lists, character escaping, parametered statements and utilising firewalls can help mitigate the threat. Don't leave database errors on the front end as it offers an "in" for attackers.

Zero Day Exploit:

Zero Day attacks are extremely difficult to predict and prevent due to the nature of new releases. Being up to date is important for security but a Zero Day attack can completely flip that safety on its head. More often than not it's safest to leave the most recent update alone for a month in order to test the security of it in the public eye. I'd under threat of another attack, however, you simply must update and take the risk for security purposes. If updated monitor systems as you would if under threat in order to prevent zero Day attacks from being catastrophic.

Sources:

1. University of North Dakota Online. *7 Types of Cyber Security Threats*. [online] Available at: <https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/> [Accessed 1 March 2022].

2. Jones, M., 2021. *Top 15 Cyber Security Questions to Ask if You're In the C-Suite*. [online] Tetra Defense. Available at: <https://tetradefense.com/cyber-risk-management/15-cybersecurity-questions-to-ask-for-c-suites/> [Accessed 7 March 2022].

3. Irwin, L., 2021. *Top 5 cyber threats and how you can tackle them - IT Governance Blog En*. [online] IT Governance Blog. Available at: <https://www.itgovernance.eu/blog/en/how-to-identify-and-respond-to-cyber-threats> [Accessed 7 March 2022].