Morgan Hodge

1 – cyber attack

Introduction

In today's digital age, the retail industry has undergone a significant transformation, due to the rise of e-commerce, as demonstrated by smartinsight's *Forecast Economic Growth in Online Retail Sales 2017-2023* (November 2021) and the increase in use of technology to streamline operations. With the increase of use of technology in businesses the risks of cyber-attacks also increase due to the many vulnerabilities that come with each new piece of technology. In this cyber report we will discuss the critical issue of human error in cybersecurity and exploring the potential impact of such errors and the steps we can take to help mitigate the risks.

Background

In this cyberattack it is apparent that an employee at the retail company "Brown-Rath" has been a victim of a social engineering attack, more specifically a spear phishing attack. It was reported that the employee received an email offering a prize draw, the prize included tickets to a game played by his favourite sports team as well as a gift certificate to his favourite food spot. Once opened, the pdf email installed a shell into the computer.

The evidence of the report shows that the employee was a clear victim of a spear phishing attack as the attacker must have carried out extensive research to find the victims interests and likes, as detailed in *Counter Intelligence: Spear Phishing and Cyber Attacks* (2016). They knew his favourite sports team as well as his preferred restaurant locations. The attacker would have done their research on the victim by looking at his social media sites and any other online sources they could find that is relevant to the victim.

The attacker used the victim's interests as bait to manipulate the victim into believing the email was legitimate and with the offer of free trips/items the victim must have believed the authenticity of the email and as a result, opened the malicious pdf file.

Critical analysis

The cyber-attack that took place on the Brown-Rath company could have been drastically worse if the incident had not gotten spotted so early on. When referring to the "cyber kill chain" model, as illustrated in *What is the cyber kill chain? A model for tracing cyberattacks (31.05.2020),* it would appear that the attacker reached stage 5, "installation" as the shell was installed onto the computer but the attack was resolved before stage 6 "command and control" could take place. This shows how close the attacker was to causing serious damage. It is not clear in the report what the attacker's intent was but as this was a company, there is guaranteed to be customer and employee data on the computers. If this data was leaked to the public, it would cause some serious reputational and financial issues for the company as this would be a breach of the General Data Protection Regulations (GDPR) as enshrined in the Data Protection Act 2018 and the company would be liable to prosecution.

To prevent social engineering attacks

To help mitigate the chances of a social engineering attack I recommend the company books a week of work for a cyber security professional to come and educate the employees on computer safety. This is because humans are the weakest link in a computer network as humans can create human errors, such as being manipulated. I believe this will be beneficial for the company as it will teach them what to look for in a malicious email, what files are safe to open and what aren't, etc. Phishing was the number one complaint for individuals and business in 20202 leading to $1.8 billion in business losses, as shown by *The ultimate list of stats Data, & trends for 2023,* so it is crucial that the employees know how to spot a threat.

To prevent malware

The pdf file acted as a "trojan horse" this is essentially a type of malicious software that appears to be legitimate but actually contains hidden malicious information code designed to steal or damage information on a computer system, as explained by *What is a trojan horse (June 2022).* This is just one form of malware that can be used to attack a system, to protect a system from malware I recommend installing Antivirus software on all the company computers as this will act as an extra layer of security before the malware can access the systems. I recommend "*Malwarebytes for business*" as this is an affordable and reliable antivirus that has hundreds of positive reviews.

Conclusion and references

In conclusion the attack could have been easily prevented with the correct security measures in place, fortunately this attack did not prove to be successful on the business as the attackers gained nothing. I recommend the company take my advice and hire a Cyber professional to teach the employees on how to be safe online as hopefully this will mitigate the chances of an attack repeating.

References:

Forecast Economic Growth in Online Retail Sales 2017-2023 Available at: https://www.smartinsights.com/digital-marketing-strategy/online-retail-sales-growth/ (Accessed 12th April 2023)

Counter Intelligence: Spear Phishing and Cyber Attacks (2016) Available at: https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Spearphishing.pdf

(Accessed 15th April 2023)

What is the cyber kill chain? A model for tracing cyberattacks (31.05.2020), https://search.brave.com/images?q=cyber+kill+chain&source=web&img=1
(Accessed 17th April 2023)

Morgan Hodge

The Data Protection Act 2018
Data protection: The Data Protection Act - GOV.UK (www.gov.uk)
(Accessed 18th April 2023)

The ultimate list of stats Data, & trends for 2023
https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering
(Accessed18th April 2023)

What is a trojan horse (June 17th 2022)
https://www.crowdstrike.com/cybersecurity-101/malware/trojans/
(Accessed 20th April 2023)

Malwarebytes for business
https://www.malwarebytes.com/business

(Accessed 21st April 2023)

Morgan Hodge

2 – Networking

Introduction

The choice of topology is a crucial decision when designing a computer network, The topology determines how the various devices in the network are connected to each other and how information flows between them. A well-designed network topology can provide efficient communication, high reliability, and scalability, as shown by *What is network topology?* However, a weak network topology can result in communication delays, network outages and bottlenecks.

Sometimes when accessing a web server over the internet the user may experience low download speeds, this is due to a variety of reasons ranging from the network being congested, having a data cap, weak WIFI signals and many more reasons as detailed in *7 Reasons why your internet is slow (and how to fix it) (Feb 14th, 2023).*

Background

The retail company "Brown-Rath" is looking for a network update due to the company expecting to double in size over the next few years. The current networking architecture is based on a flat design, as explained by *What is a flat Network? Definition, Benefits, and How It Works (21.2.2023).* This current design is working now but will not have the capabilities to support a network upgrade. Further into this report I will propose a new networking system that will have room for expansion.

An employee at the company may experience low download speeds when accessing a web server over the internet, we have assumed this problem is due to the network and not the web server. I have been asked to provide a networking tool that can be used to locate whether the network problem is within the company or outside of the company. The benefits of the business having this, is that they will be able to view all the nodes and devices attached to the internet, with this information it will help the business locate and resolve the issue.

Critical analysis

I believe to meet the company's needs, a hierarchical network architecture with three layers should be implemented (Core, Distribution and Access), as detailed by *What is hierarchical network design (July 20, 2021)*. The core layer would consist of high-performance switches with security features, the Distribution layer would enforce network policies, and the Access layer would provide connectivity to end-user devices.

The hierarchical network allows for size upgrades because it can easily accommodate the addition of new devices and users. As the company grows and expands, new switches or routers can be added to the access layer, and additional distribution layer switches or routers can be added to total the traffic. The core layer can also be upgraded to handle the increased traffic.

In order to enhance network security, network segmentation should be implemented, as well as VPN access and multi-factor authentication.

The networking tool I recommend is traceroute. This tool is typically used to diagnose hiccups or interruptions in the transfer of data and pinpoint where along the chain it occurred, as stated in *Traceroute Tool: How and what does it trace?*

I recommend this tool as it will show an exact path from the sender to the destination, this allows us to see exactly where the problem occurs. This will allow us to determine whether the problem is within the company or outside the company.

This tool will be beneficial for the business to have forever as this one tool can solve many problems, for example if there was a problem with one of the routers. This tool can be used to ping and locate the exact router that is causing issues, whereas without this tool it may have been unclear what router was causing issues.

Conclusion and references

The network will require an upgrade as the current structure will not satisfy the business's future needs. In conclusion I have decided the hierarchical network structure will be a suitable upgrade for the business as it allows for room to expand. The business may also consider network segmentation as this will make the network more secure as attackers will need to gain access to each segmentation.

In conclusion I believe this is the best networking tool for this business to use, it has many uses and does not take that long to understand and familiarise yourself with. I also recommend the business cyber team review the TTL configurations as the limit may be set too high, causing loops and data loss, this may be the outcome of a misconfigured network.

References:

What is Network Topology?

https://www.cisco.com/c/en/us/solutions/automation/network-topology.html

(Accessed 12th April 2023)

What is a flat Network? Definition, Benefits, and How It Works (21.2.2023)

Morgan Hodge

https://www.enterprisenetworkingplanet.com/management/the-risks-and-rewards-of-flat-networks/

(Accessed 16th April 2023)

What is hierarchical network design (July 20, 2021)

https://www.auvik.com/franklyit/blog/hierarchical-network-design/

(Accessed 17th April 2023)

7 Reasons why your internet is slow (and how to fix it) (Feb 14th 2023)

https://www.highspeedinternet.com/resources/why-is-my-internet-so-slow

(Accessed 11th April)

Traceroute Tool: How and what does it trace?

https://www.broadbandsearch.net/trace

(Accessed 14th April)