CYBER SECURITY BEST PRACTICES FOR SMALL AND MEDIUM SIZED ENTERPRISES (SMEs)

Introduction

- **Name:** Emre OTU
- **Field of Study:** Computer Science (Artificial Intelligence), Year 1
- **Institution:** Brunel University London Pathway College
- **Duration:** 10 Minutes Presentation & 5 Minutes Q&A
- **Objective of Presentation:** In today's digital age, cybersecurity is of utmost importance for small and medium-sized businesses. This presentation focuses on various cyber threats such as phishing, ransomware, and DDoS attacks and suggests AI-based strategies to counter them. This presentation aims to assist SMEs in safeguarding their digital assets and ensuring business continuity.

Introduction

01

Introducing myself and the purpose of the slide.

What is cyber security?

02

The meaning of cyber security.

Importance of Cyber Security

03

Why cyber security is important?

Cyber threats to SMEs

04

- Phisings
- Ransomware
- DoS and DDoS Attacks

Conclusion

05

Overview of slides and the topic.

References

06

For further reading!

02 - 03

What is cyber security? And it's importance.

What is cyber security?

Cybersecurity's aim is to safeguard all our gadgets, ranging from smartphones and laptops to tablets and computers, along with the services we utilize, whether it be for personal or professional usage. Its key purpose is to prevent any attempts at stealing or causing harm to our devices and to impede unauthorized entry to the numerous personal data we have saved on these devices and the internet.

Why cyber security is important?

In the modern era, digital technologies like smartphones, computers, and the internet have seamlessly integrated into our everyday routines. These tools serve a variety of purposes, from online banking and shopping to communication via email and social media. It's difficult to envision a world without them. Yet, this reality underscores the critical nature of safeguarding our digital accounts, personal information, and devices from potential cyber threats.

04

Cyberthreats to SMEs

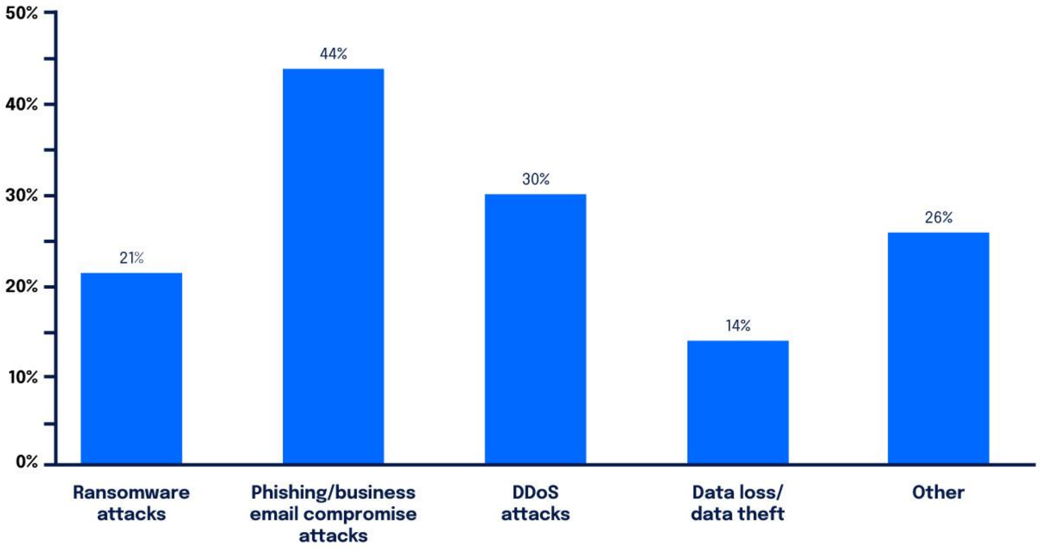
General Issues of SMEs
Problems, Solutions, Facts!

Why SMEs vulnerable to cyber threats?

Small and Medium Enterprises (SMEs) face a higher risk of cyber threats compared to larger businesses because of their limited financial resources. This makes it challenging for SMEs to establish strong security measures. The significance of cybersecurity may be underestimated by SMEs, as they might assume that they are not potential targets or that the risks are not significant. However, cyber attacks can result in severe consequences such as data breaches and financial losses, which can cause long-term harm to the business's reputation and customer trust. (OriginStamp, 2023)

Graph

What kind of security breach did you experience?



● Ransomware

● Phising

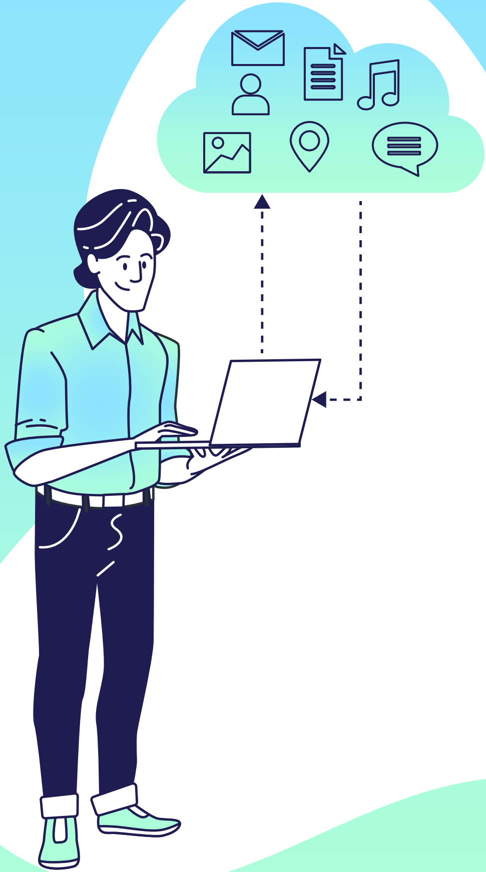
● DoS & DDoS

Security Breaches

What are the most critical cyber threats that small and medium-sized enterprises (SMEs) are facing? (DigitalOcean, 2023)

04.1

Phising



PROBLEM VS. SOLUTION

Problem

- Scammers often pretend to be trustworthy entities to deceive individuals.
- Potential victims are contacted through emails, text messages, or phone calls.
- Personal information such as passwords and credit card numbers.
- The ultimate objective of phishing attacks is to steal sensitive information for malicious purposes, such as identity theft or unauthorized financial transactions. (Microsoft, n.d.)

Solution

- Consider utilizing AI-powered solutions to safeguard your business against phishing and business email compromise attacks. (Expert Insights, n.d.)
- To improve cybersecurity, it's important to train employees on best practices. Focus on enhancing employee awareness by providing proper cybersecurity training. (ENISA, 2021)

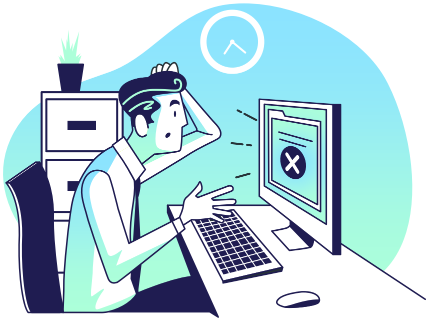
Fact

A significant finding from the Cyber Security Breaches Survey 2022 is that phishing attempts were identified as the most common cyber threat to UK businesses, with **83%** of businesses who experienced an attack reporting phishing attempts. (Department for Digital, Culture, Media & Sport, 2022)

04.2

Ransomware

PROBLEM VS. SOLUTION



Problem

Ransomware is a form of malicious software that effectively restricts access to a device or data by encrypting it and demanding a ransom for its release. The severity of its impact can vary from merely locking a computer to outright theft or deletion of data. (NCSC, n.d.)

Solutions

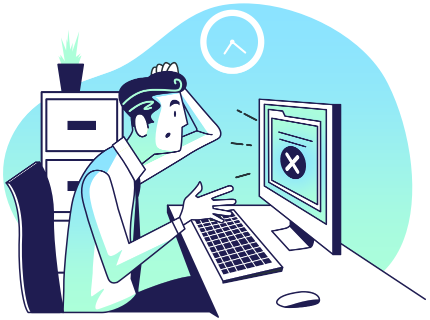
- Regularly updating and patching computer systems is crucial to prevent ransomware attacks and ensure the safety of our data and network.
- Regularly backing up data and storing it separately from the main network is crucial in preventing any possible encryption by ransomware. (NCSC, n.d.)

Fact

In 2021, 37% of small and medium-sized enterprises (SMEs) encountered a ransomware attack, which is a noteworthy statistic. It is important to note that the average cost of recovering from such an attack is $1.85 million for businesses, according to Kochovski's research (2024). Additionally, it is worth noting that only 57% of affected SMEs were able to restore their data using backups. (Cybereason, 2021)

04.3 DoS and DDoS Attacks

PROBLEM VS. SOLUTION



Problem

A type of cyber attack called Denial-of-Service (DoS) can harm network resources and services, like email or websites, by overwhelming the target with traffic. This leads to legitimate users being unable to access the services. These attacks can cause significant financial damage to organizations that are affected, in addition to operational disruptions (CISA, 2021).

Solutions

- Detecting and redirecting abnormal traffic flows using a DoS protection service, which filters out malicious traffic.
- Creating a strategy to recover from disasters that includes effective communication and recovery during attacks.
- All internet-connected devices need to have their security enhanced to ensure they are not compromised. (CISA, 2021).

Fact

DDoS attacks have significantly increased, and there has been an 82% boost in application layer attacks in 2022 as compared to 2021. Year-over-year, financial services experienced a 121% surge in these attacks, underscoring the mounting cyber threat to businesses, including small and medium-sized enterprises. (Pixelprivacy.com, 2024)

Businesses can suffer significant financial losses due to DDoS attacks, with downtime and mitigation efforts potentially costing up to $50,000. According to reports, almost 70% of organizations experience between 20 to 50 DDoS attacks in a month, indicating that these cyber threats are frequent and expensive. (Comparitech.com, 2018-2024)

05

Conclusion

Overview of the presentation

CONCLUSION

Small and medium-sized enterprises (SMEs) live in a world where cybersecurity is a top priority to safeguard against threats such as phishing, ransomware, and DoS/DDoS attacks. To effectively defend their data and ensure business continuity, SMEs must invest in employee training, use AI for security, and regularly update their systems. It is important to note that maintaining trust and achieving success in the digital marketplace requires effective cybersecurity as a crucial component.

06

References

REFERENCES

- Microsoft. (n.d.). What is phishing? Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing [Accessed 24 March 2024].
- European Union Agency for Cybersecurity (ENISA). (2021). Phishing: most common cyber incident faced by SMEs. Available at: https://www.enisa.europa.eu [Accessed 22 March 2024].
- Expert Insights. (n.d.). The Top 11 Phishing Protection Solutions. Available at: https://www.expertinsights.com [Accessed 22 March 2024].
- Department for Digital, Culture, Media & Sport. (2022). Cyber Security Breaches Survey 2022. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022 [Accessed 22 March 2024].
- DigitalOcean. (2023). Cybersecurity for SMBs in 2023. Available at: https://www.digitalocean.com/reports/cybersecurity-smbs-2023 [Accessed 24 March 2024].
- National Cyber Security Centre (NCSC). (n.d.). A guide to ransomware. Available at: https://www.ncsc.gov.uk/ransomware/home [Accessed 24 March 2024].
- Cybereason. (2021). Ransomware Statistics, Data, Trends, and Facts [updated 2023]. Available at: https://www.varonis.com/blog/ransomware-statistics/
- Kochovski, A. (2024). Ransomware Statistics, Trends and Facts for 2024 and Beyond. Cloudwards. Available at: https://www.cloudwards.net/ransomware-statistics/
- Cybersecurity & Infrastructure Security Agency (CISA). (2021). Understanding Denial-of-Service Attacks. Available at: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks [Accessed 24 March 2024].
- Pixelprivacy.com. (2024). DDoS Attack Statistics, Facts & Figures for 2024 – Threat Report. Available at: https://pixelprivacy.com/resources/ddos-attacks-statistics/
- Comparitech.com. (2018-2024). 20+ DDoS attack statistics and facts for 2018-2024. Available at: https://www.comparitech.com/blog/information-security/ddos-attack-statistics-facts/ [Accessed 24 March 2024].
- OriginStamp. (2023). The impact of cyber attacks on SMEs. Available at: https://originstamp.com/blog/the-impact-of-cyber-attacks-on-smes/ [Accessed 24 March 2024].

THANKS!

Thank you for listening to me! If you have any questions related to my topic, I am happy to answer them.

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by Stories