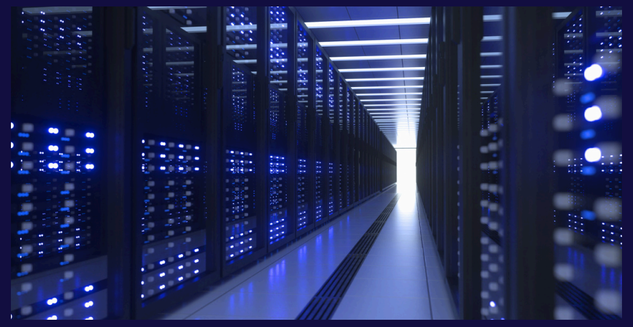
Emerging Threats and Countermeasures

Abdullah KARA
190254041

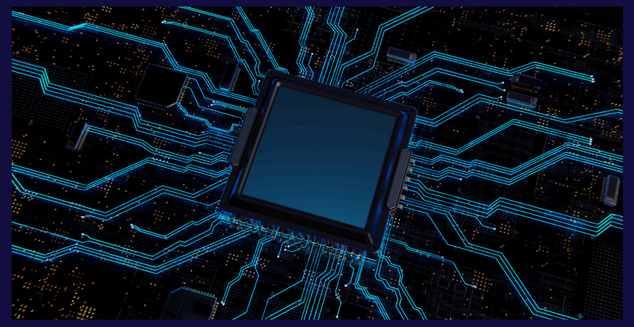
Introduction

Network security has become an increasingly complex and evolving field in today's digital age. Technological advancements and the process of digital transformation have led to networks becoming even more intricate, giving rise to new threats. In this presentation, we will examine three significant threats encountered in the field of network security and evaluate countermeasures for each one.

Emerging Threats



1.Artificial Intelligence (AI) Supported Attacks



2. Attacks via IoT Devices

3. Quantum Computing Security Vulnerabilities

Artificial Intelligence (AI) Supported Attacks

Artificial intelligence (AI) is utilized in both defensive and offensive methods in the field of network security. AI-supported attacks can be executed in a more unpredictable manner compared to traditional attack methods. For instance, AI-based malware can rapidly and automatically alter attack vectors and bypass defense systems. In addition to this, malicious software attacks, phishing attacks, etc.

Countermeasures for AI-supported Attacks

- Development of attack detection systems using machine learning and AI.
- Utilization of automated systems for continuous monitoring of network traffic and rapid anomaly detection.
- Implementation of AI-based defense systems.

Malicious Software Detection

Artificial intelligence can be trained to detect and analyze malicious software based on its code or behavior. Machine learning algorithms can identify patterns and signatures of known malware and then apply this knowledge to detect and prevent future attacks.

Phishing Detection

AI can be utilized to detect and prevent phishing attacks by analyzing email and social media messages. Machine learning algorithms can identify and flag suspicious messages based on characteristics such as the sender's domain, message content, and user behavior. This can help prevent users from inadvertently clicking on malicious links or providing sensitive information to attackers.

AI-supported antivirus software can provide faster and more accurate protection than traditional antivirus software by learning new types of malicious software and adapting to them.

Attacks via IoT Devices

Internet of Things (IoT) devices are becoming increasingly prevalent among connected devices in networks. However, these devices often have weak security measures and can be easy targets for attackers. The misuse of IoT devices can lead to network infiltration, data theft, and even physical harm.

IoT devices appear highly vulnerable due to several reasons:

Lack of security software on devices: Unlike regular computers, IoT devices typically lack security firewalls or virus scanners.

Less experienced device manufacturers: Businesses often lack the IT security expertise of server/computer manufacturers.

Multiple devices with the same security mechanisms: An attack that works on one device will work on thousands of devices.

Inaccessibility of IoT devices: Device owners deploy their machines remotely. Often, the device owner doesn't realize their devices have been compromised until it's too late. Once an attacker gains control over a device, they can operate all day until physically shut down by the device owner.

Countermeasures Against Attacks via IoT Devices

Development and enforcement of security standards and protocols. Strengthening IoT devices with security software and ensuring regular updates. Implementing network segmentation and tightening access control to critical systems.

Quantum Computing Security Vulnerabilities

Quantum computers pose a potential threat to traditional encryption methods. Security vulnerabilities in quantum computing could lead to the breaking of current encryption algorithms and put sensitive data at risk. Quantum computers can solve a code that a classical computer would take years to crack in a matter of hours.

Conclusion

In this presentation, we addressed three significant emerging threats such as AI-supported attacks, attacks via IoT devices, and quantum computing security vulnerabilities, and examined countermeasures for each. Organizations need to continuously update and improve security measures to effectively protect against these threats. Implementing the proposed measures will strengthen organizations' network security and better prepare them for future threats. My view is that anyone who is unsure about their security should quickly seek support from cybersecurity experts.

References:

https://en.wikipedia.org/wiki/Post-quantum_cryptography

https://www.wallarm.com/what/iot-attack#:~:text=An%20IoT%20attack%20is%20a,cause%20damage%20to%20the%20devices.

https://zayifakim.com/iot-guvenlik-tehditleri-ve-onlemleri.html

https://rfidhaber.com/kuantum-hesaplama/

https://mixmode.ai/what-is/ai-generated-attacks/

https://www.infosec.com.tr/yapay-zeka-siber-saldirilar-nasil-onlenebilir/

https://www.infosec.com.tr/2022-siber-guvenlik-gundemini-belirleyecek-5-tehdit/

https://nordvpn.com/tr/blog/iot-attacks/

https://ioturkiye.com/2020/09/iot-saldirilari-ve-onerilen-onlemler/

https://identitymanagementinstitute.org/cybersecurity-quantum-attack/

Thank you for watching