Discussion-7 Network Security

Discussion Topic:

There are both internal and external threats that companies face in securing their networks. Describe what you believe are some of the highest risks to security in organizations? List at least three risks.

What might be a mitigating solution to each risk that you have listed?

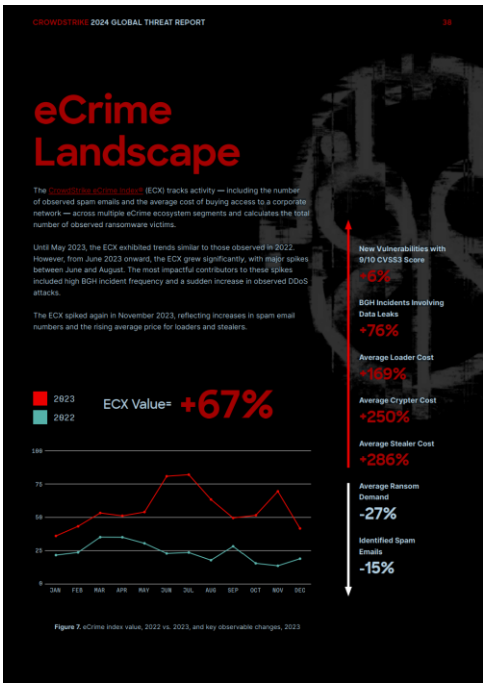
My Post:

Hello Class,

In today's technological landscape, where everything runs on computers and data is a valuable asset, companies are faced with significant challenges to secure their network and protect their data. Those threats are both internal and external and pose substantial risks that can not be ignored. CrowdStrike (2024), a leader cybersecurity technology company, “2024 Global Threat Report” shows that attacks are becoming increasingly sophisticated, using techniques like social engineering, exploitation of unpatched vulnerabilities, and insider threats to compromise networks and steal sensitive information. The figure below illustrates page 39 of the CrowdStrike report. Page depicts the EXC Value for 2023 which is a metric developed by CrowdStrike to quantify the level of eCrime activity over a period of time. The metric depicts a value of %67, meaning that crime activity in 2023 increased by %63 from 2022.

Figure 1

2023 eCrime Landscape



Note: the figure depicts page 39 from the "2024 Global Threat Report" by CrowdStrike (2024). The page shows the eCrime Landscape for 2023 and the EXC Value. A metric that measures the quantity of eCrime activity over a period of time.

Some of the highest risks faced by companies are:

- Social engineering attacks, especially phishing.
These attacks involve tricking individuals into providing sensitive information or performing actions that compromise security. Usually by sending emails to a potential victim that appears to be legitimate (uCertify, 2018). These attacks bypass most security measures put in place by the network administrators. A successful attack can lead to data breaches, financial loss, and reputational damage. To mitigate the risks of social engineering attacks, it is important to implement measures such as user training, email filtering, and Multi-Factor Authentication (MFA).

- Insider threats or insider attacks.
These threats originate from within the organization itself, from employees, contractors, or compromised accounts. Note that employees and contractors may be malicious or just careless. Insiders such as employees have often access to sensitive systems and data, making it easier for them to steal data, cause harm, or inadvertently compromise the organization's network security. To mitigate these risks of insider attacks, it is important to implement measures such as the principle of least privilege (granting users only the minimum access necessary for their job duties), network activity monitoring and auditing, and data loss prevention (DLP) solutions to prevent sensitive data from leaving the organization.

-Unpatched vulnerabilities or unknown and known unaddressed vulnerabilities.
Software and systems such as Operating Software (OS) may have novel or known vulnerabilities that can be exploited by attackers. Attackers are constantly scanning systems for known and unknown vulnerabilities, thus, failing to prepare for the possibility of unknown vulnerabilities or failing to patch known ones would leave them exposed to potential harm. To mitigate these risks of unpatched vulnerabilities, it is important to implement measures such as vulnerability Scanning and patch management, as well as, automated patching and penetration testing.

These are just a few of the many securities risks and with the emergence of AI, especially with Agentic AI predicted to become a reality this year, these risks are only expected to grow in intensity. Therefore, it is crucial for companies to invest in robust cybersecurity systems to protect their organization's network system and data by implementing all the mitigating solutions discussed in this post, along with solutions that can adapt to a fast-evolving threat landscapes fueled by eCrime and rogue actors/nation-states that are probably planning to fully leverage AI for malicious purposes.

-Alex

References:

CrowdStrike (2024). 2024 Global threat report [PDF]. CrowdStrike. Retrieve from: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

uCertify. (2019). Lesson 12: Network Security. *CompTIA Network+ Pearson N10-007 (Course & Labs)* [Computer software]. uCertify LLC. ISBN: 9781616910327