T2021_18 Ransomware Attacks Are Evolving & So Should Your Security Strategy (5th November 2021)

Ransomware is a growing problem for organizations around the world and it's likely to get even worse. What started as a floppy disk-centered attack with a $189 ransom required has grown from a minor inconvenience for companies into a multi-billion greenback cyber crime business.

The organizational threat of ransom attacks goes well beyond encryption of sensitive or mission-critical data. For many organizations the thought of a breach and data becoming publicly available on the internet makes a high ransom seem worth it. No wonder ransomware is on the rise.

Staying One step ahead of Bad Actors

Modern ransomware attacks include various tactics like social engineering, email phishing, malicious email links and exploiting vulnerabilities in unpatched software to infiltrate environments and deploy malware. Which means that there are no days off from maintaining good cyber-security.

Another challenge which can be considered is when an organization's cyber threat defence strategies against common attack methods improve, malicious actors will adjust their methods so as to find new vulnerability points. This only means that threat detection requires real-time monitoring of channels and networks.

This poses a question about how can organizations ensure they stay one step ahead if they don't know what is the target of the next attack? The practical approach is for organizations to implement a layered security strategy that includes a balance between prevention, threat detection and remediation which starts with a zero-trust security framework.

By implementing a zero-trust security framework, organizations are better positioned to keep track of all connected devices and networks, detect and respond to threats in real-time, and stop potential attacks before damaging the organization's overall function and reputation.

What is Zero Trust?

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust

assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats.

Zero-Trust Security for Ransomware Protection

Establishing zero-trust security have quite a few requirements which are an operational framework and a set of key technologies designed for modern organizations to better secure digital assets. It also requires organizations to continuously verify each asset and transaction before permitting any access to the network.

Verification can be done through various methods such as ensuring that systems are patched and up-to-date, putting into practice passwordless multi-factor authentication and deploying unified endpoint management. Ensuring device hygiene through patch and vulnerability management is a critical component of a zero-trust strategy. What's more, utilizing key hyper-automation technologies such as deep learning capabilities can help security teams ensure that all endpoints, edge devices, and data are discoverable, managed and secured in real-time.

Organizations should also consider going one step further by taking part in drills to test their responses to ransomware attacks. Having a recovery plan in place can play a vital role in minimizing the time it takes to assess the threat at hand. Practice makes perfect, and this is no different for an organization's security strategy.

References

- Spicer, Daniel. (October 27, 2021). Ransomware Attacks Are Evolving. Your Security Strategy Should, Too. Retrieved from Threat Post: https://threatpost.com/ransomware-attacks-evolving-security-strategy/ 175835/

- Raina, Kapil. (May 6, 2021). Zero Trust Security. Retrieved from Crowdstrike:

https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/