Lodestone

JANUARY 2023

STATE OF CYBER

monthly newsletter

NETWORK SEGMENTATION AND HOW IT CAN PREVENT RANSOMWARE

Network segmentation is a critical security measure for any network because it works on multiple levels to protect data and devices, as well as reduce and remove attack vectors.

There are multiple levels to network segmentation, examples of which include:

- Segmentation by VLAN: this is a common practice for most organizations, which allows for networks to be broken down into subnets or smaller groups.
- Firewall Segmentation: firewalls can be configured to use predetermined rulesets to allow or deny certain traffic into and out of a network or between segments of a network.
- Least Privilege Segmentation: this is typically not seen as a type of segmentation, but Least Privilege is a methodology that restricts areas within the network to only qualified users. This can assist in preventing malicious users from accessing protected data or protected systems within the network, as they may not have the proper administrative privileges to do so.

Malicious users are looking to accomplish multiple items within your network. From data exfiltration to encrypting your most important data, without segmentation they are given free reign across the network to do as they please. Without those methodologies and segmentation of data, backups, specialized systems, Threat Actors are able to move more easily within the network unrestricted from system to system. Implementing subnets restricts the Threat Actors to a specific part of your environment, unable to move into your most important subnets where protected data is stored, where backups are placed in case of disasters, or any other types of specialized data that cannot be lost.

It's crucial for organizations to regularly review and update their security architecture to ensure readiness and a strong security posture. Consider Lodestone for help with a comprehensive cybersecurity assessment.

FIN7 HACKERS CREATE AUTO-ATTACK PLATFORM TO BREACH EXCHANGE SERVERS

A Russian cyber threat group has developed a new exploitation software called Checkmarks, which scans Microsoft Exchange servers for vulnerabilities and allows for SQL injection scanning on target websites. The group has already scanned 1.8 million targets.

MICROSOFT URGES ADMINS TO PATCH ON-PREMISES EXCHANGE SERVERS

The latest Exchange Cumulative Updates (CU) have been released by Microsoft. With the rampant rise of Exchange related attacks and vulnerabilities, the latest updates will further help protect the environment from exploitation.

DECRYPTED: BIANLIAN RANSOMWARE

Recently, Avast has released a decryptor for the BianLian Ransomware Group. This free-to-use decryptor will allow any previous victims to decrypt their data if they were effected by the BianLian group.

2022 DATA BREACH INVESTIGATIONS REPORT

Verizon has rounded up the most common breach methods, vulnerabilities and threat groups during the past year. This past year shows a 13% increase in ransomware, with 2022 being the largest rise seen in the last five years. The past year alone shows that 82% of breaches involved the use of stolen credentials, phishing, or configuration errors within networks.