MedNetworx Cybersecurity Report

February 2024: Ransomware

According to a study by Sophos, the rate of ransomware attacks on healthcare related organizations was 60% last year. The root causes of these attacks were:

- *Compromised credentials (32%)*
- *Exposed vulnerabilities (29%)*
- *Email based attacks (36%)*

A ransomware attack can cripple company infrastructure and can potentially have steep costs to recover valuable data or rebuild IT infrastructure appropriately to prevent another attack.

How can you fight ransomware?

The main strategy for combating ransomware is deterrence, but even the best anti-ransomware strategies develop faults as actors become more elaborate. Continued refinement and cooperation is necessary to keep data secure, and CISA has introduced new joint-efforts as time has gone on.

- As of January 2023, the Ransom Vulnerability Warning Pilot (RVWP) contacts critical industries in case of a ransomware breach or major security vulnerability. Contact your regional officer to get more free resources from CISA.
- Report cyberattacks as they occur to CISA, the FBI, or U.S. Secret Service to help prevent future ransomware incidents.

While devloping a ransomware prevention strategy isn't as simple as instituing a few safeguards, the following should give you a firm foundation to start building a secure data sphere.

Vital Ransomware Prevention Measures

Offline Backups

Offline, encrypted backups can get systems back up and running quickly and potentially elimanate the need to pay ransomware hackers for integral data.

- Automated cloud backups are still prone to danger because hacked files can be synced to the cloud.
- "Golden images" or templates with preconfigured settings and operating systems can be used to quickly redeploy systems.

Phishing-Resistant Multifactor Authentication (MFA)

By requiring multiple forms of authentication (password, digital token, and biometric identification) MFA helps construct an environment resistant to multiple types of ransomware tactics such as:

- Push Bombing- User is flooded with push notifications until they accept,
- SS7- Ransomware actors exploit vulnerabilities in the SMS text system to intercept calls and messages
- Sim-Swap Attacks- Phone carriers are convinced to lend control of a device to a ransomware activated Simcard, compromising the device.

Need help or resources with ransomware safety for your organization? MedNetworx's total IT solutions can address any potential cybersecurity issues you have.

MedNetworx™ Practice Innovation.
12700 Park Central Dr. Suite 1050
Dallas, TX 75251
Phone: 469-854-8400
Fax: 972-387-4000