Ransomware in 2020

NGU
RISK MANAGEMENT

August, 2020

Kyle Greenup
kgreenup@ngutn.com
615.822.5454

Cyber threats continue in 2020 and there are many threats to be aware of moving forward. In this article, we'll address the Ransomware threat in the United States (definition: Ransomware), what you need to know, and how you can protect your network, data, customers, vendors, and employees.

First, let us consider SonicWall's Mid-Year Update on Cyber Threats (link to report). According to the report (dated July 2020), there has been a significant uptick of 109% in Ransomware attacks in the United States compared to this time in 2019. That translates to just under 80 million Ransomware attacks in the US alone in 2020. What may be worse for TNRMT Members is that Tennessee is #4 in terms of Ransomware Volume by State (6.8 million attacks), and public entities remain a hot target.

From an attacker's perspective, Ransomware is a very enticing form of malware. The relative ease of use coupled with anonymous payouts are the main drivers that give Ransomware a highly attractive quality in the eyes of an attacker. And unfortunately, attackers are becoming greedier and bolder. The ransom payouts are growing in value and the consequences of failures to pay the ransoms are growing as well. Consequences include not only the inability to access company data, but network downtime and the significant effort to restore critical systems and/or data. The worst consequences of all could be that the attacker decides to release or sell your private data and the fallout associated with communicating that fact to customers, employees, vendors, and the public in general.

Ever increasing threats compel us to consider a network protection practice that utilizes a multi-faceted, encompassing approach. Securing a network properly takes training, effort, and expense. Consider this list:

- End-User Cyber Security Awareness Training (offered by TNRMT and SEC). We believe that this is essential. When users cannot identify threats, those threats become much more difficult to mitigate. Employees are often a threat not due to their nature, but due to their inherit clearance on your network and their relative lack of Cyber Security training.
- Patch All Systems. Many systems are compromised using known vulnerabilities. Keeping systems and software patched on a regular schedule should always be part of your network security practice.
- Secure Your Data Backups. If your organization is not using a secure, off-site backup solution with a daily backup frequency, consider re-assessing your backup strategy.
- Security Software. All production systems should have advanced security software. This software is often the first line of defense between your organization and a breach. Security software must be updated with new definitions, ideally multiple times per day.
- Avoid Common Ports. According to SonicWall's Mid-Year Update on Cyber Threats, 75%-90% of attacks target systems using 'Common Ports', also known as 'Well Known

Ports' (more information: Well Known Ports). If you can avoid using common ports, do so. If you cannot avoid using common ports which is often the case, then ensure you have a strong security solution in front of those exposed systems.

- Secure Your Perimeter Network. Mostly, this means using a Next Generation Firewall (definition: Next Generation Firewall) on incoming connections. Next Generation Firewalls (NGFWs) are offered by a variety of vendors and can offer a variety of services to better secure your perimeter.
- Secure Your Network Infrastructure. If there is a single word that describes a secure network infrastructure, it's probably 'Hardened'. Hardening your network is critical to eliminate exposures and the practice will drastically reduce successful attacks. Different devices are hardened by using a variety of techniques, and often you can find device hardening guidance from the vendor.
- Use the eRisk Hub, powered by NetDiligence®. TNRMT Members have access to the eRisk Hub at no additional cost. Use this information sign up, learn about your exposures, establish a response plan, and more.

We welcome any questions, comments, thoughts, and sharing of your own experiences within the topic of Cyber Security. Please contact any of us listed below at any time.

Tom Montgomery
tmontgomery@sectn.com
615.826.4274

Chris Stites
cstites@ngutn.com
615.289.4101

Mark Bilyeu
mbilyeu@sectn.com
615.210.7827

Jason Baggett
jbaggett@tnrmt.com
865.228.8835

Kyle Greenup
kgreenup@ngutn.com
615.822.5454