TECH LOCK®
A RevSpring Company

Ramsomware Realities and What to Do Next

Ransomware is the Top Security Concern

Ransomware and the notable ransomware families with their growing number of variants continue to evolve. Hackers no longer have to specifically target an organization and invest hours of reconnaissance to determine how to infiltrate, laterally move to high-value data, and then execute the exfiltration of data. They have found an easier and faster way to their desired monetary gains aided by the growth in digital currencies, such as Bitcoin. Ransomware-as-a-Service is accelerating this trend, and disrupting business.

Ensure your corporate cyber defenses are a match for blocking ransomware threats

How Ransomware Attacks

Website drive-by download

From a website that has been hacked, replicated, or contains malicious advertisement links which inject code into your computer – leveraging vulnerabilities, or capturing credentials and other information for later use.

Phishing

From email and attached content, malicious links, or files allowing code to be unsuspectingly launched.

Vulnerability weaknesses

Specific types of vulnerabilities with Remote Control Execution (RCE) capabilities and protocols, like Remote Desktop Protocol (RDP), can be leveraged to take direction within the organization and set up control points for the hacker.

continued on next page

"The private sector has a critical responsibility to protect against ransomware threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location."
- Anne Neuberger, Deputy National Security Advisor for Cyber (June, 2021)

Hard Truths About Business Disruption

"I have backups and can restore my business without paying the ransom"

If the hackers got in once, does your backup have the same configuration weakness or vulnerability that got you in this situation in the first place? Is your backup online and also susceptible to a breach?

"I have cyber insurance to help me offset a cost of disruption"

Cyber insurance is a growing business. But, many policies hide the fact that if phishing played a part in this event, they can consider this an employee-initiated situation, not a direct a cyber threat and may deny your claim.

"I might just pay the ransom"

Many ransomware families are shifting tactics from business disruption to full-on business reputational damage.

Past trend: Leverage gateway vulnerabilities that open the door for the ransomware malware and disrupt organizations by encrypting their data and holding it hostage for ransom payment.

New trend: Leverage gateway vulnerabilities, steal valuable data, and hold it for ransom with the additional threat of public disclosure.

Beyond the ransom payment, organizations need to factor in compliance fines, breach notification costs and the potential for lawsuits when sensitive data goes public.

Attackers know organizations have more at stake and have elevated their extortion tactics.

- **Six out of 10 companies say they were disrupted by ransomware in the past year**
- **On average companies hit by ransomware experienced six days of downtime**
- **A third of companies that paid ransom didn't get their data back**

TECH LOCK enables organizations to navigate, detect, and respond to today's modern cybersecurity and compliance challenges.

Take action today to look at your companys resiliency against ransomware:

- Perform a tabletop review of your Incident Response Plan
- Test backups of critical systems and restore time objectives
- Review segmentation of networks and access privileges
- Patch critical and high vulnerabilities and those listed in US CISA/DHS alerts
- Keep vigilant with 24/7/365 SOC monitoring with quick responses

We can help you assess your ransomware suseptibility and provide immediate assistance to enhance your ability to detect and respond to ransomware threats.

Our portolio of cybersecurity services and best-in-breed technologies allow small to medium sized enterprises achieve enhance security protection that is proven to be cost effective.

About TECH LOCK Inc.

TECH LOCK enables organizations to navigate, detect, and respond to today's modern cybersecurity and compliance challenges. Our full spectrum security-centric approach delivers value to our clients through defined and measurable outcomes combined with independent cyber research, specialized skills, and premium customer support and service.

Contact TECH LOCK today

320 E. Big Beaver Rd, Suite 145 • Troy, MI 48083

info@techlockinc.com

847.245.3727

www.techlockinc.com