Guidepost

CHANGE HEALTHCARE RANSOMWARE ATTACK: 10 LESSONS LEARNED

Why does it matter to you?

In February of 2024, Change Healthcare, a prominent player in the healthcare industry, fell victim to a ransomware attack that sent shockwaves through its systems and networks. The incident highlights the critical need for robust cybersecurity measures and vigilance across all organizations, no matter of their size.

How they did it – Anatomy of the Attack

Exploiting Weaknesses – The attackers meticulously identified vulnerabilities within Change Healthcare's infrastructure. The weaknesses ranged from outdated software to misconfigured settings and unpatched systems. With this information, the cybercriminals launched their attack, seeking to exploit any weaknesses in the company's defense.

Malware Deployment – The attackers didn't rely on brute force alone. Instead, they employed sophisticated malware to infiltrate the company's networks. This malicious software allowed the cybercriminals to gain unauthorized access, bypassing security measures that were meant to safeguard sensitive data.

Data Breach – Once the cybercriminals were inside the network, they targeted sensitive information. Patient records, financial data, and administrative details were all fair game. The breach exposed confidential data, putting individuals' privacy at risk. The result could be far-reaching, affecting patients, healthcare providers, and the end company itself.

The Aftermath and Lessons Learned

The Change Healthcare incident serves as a stark reminder for organizations and companies worldwide. What can we all learn from this incident:

1. **Never Click on Unverified Links** – Stay vigilant when it comes to emails and websites. Avoid clicking on suspicious links, especially those received via email that create a sense of urgency. Cybercriminals often use phishing emails to deliver ransomware. Hover over the links to verify their legitimacy before

clicking. Read the URL closely!

2. **Regularly Back Up Your Data** – Backup, backup, backup! Regularly back up your critical data using multiple methods. Consider cloud storage, external drives, or network-attached storage (NAS). Having clean backups ensures you can restore your data without paying the ransom.
3. **Keep Software Updated** – Cybercriminals exploit vulnerabilities in outdated software. Regularly update your operating system, applications, and security software. Enable automatic updates whenever possible.
4. **Use strong and Unique Passwords** – Password hygiene matters! Create strong, unique passwords for each account. Avoid reusing passwords across services. Consider using a password manager to securely store and manage credentials.
5. **Enable Spam Filters** – Filter out the noise. Turn on Spam filters for your email. These filters catch phishing emails and reduce the risk of accidental clicks on malicious links.
6. **Educate Employees and Users** – Knowledge is power. Train your team to recognize phishing attempts and suspicious behavior. Make sure your team knows how to report suspicious links! Regular security awareness training helps prevent successful ransomware attacks.
7. **Segment Your Network** – Isolate critical systems. Use firewall and virtual private networks (VPNs) to segment your network. If one segment is compromised, it won't affect the entire network.
8. **Assess and Improve Security** – Stay proactive. Regularly evaluate your network's security posture. Use vulnerability scanning tools to identify weaknesses. Stay informed about the latest threats and best practices.
9. **Avoid Paying Ransoms** – Think twice before paying. Explore alternative options, such as restoring from backups or seeking professional assistance. The money used to pay a ransom can go a long way to secure your systems in advance.
10. **Stay Informed** – Knowledge is your shield. Keep up with cybersecurity news, trends, and emerging threats. Awareness empowers you to take preventative measures.

Remember, prevention is the best defense against ransomware. Implement these tips, stay informed and protect your digital world from malicious attacks. It is also advisable to consult a third-party cybersecurity consultant to assess your vulnerabilities and provide guidance to prevent incidents and fortify your organization's security posture. Investing in those services not only shields your critical data, but can fortify your reputation and operational continuity.

C. TODD DOSS

Senior Managing Director

Christopher “Todd” Doss has a diverse background in managing and coordinating responses to complex security incidents, including but not limited to cyber-attacks, data breaches, and insider threats. Having led more than 4,000 cyber incident responses and investigations, he has gained an in-depth knowledge of designing and executing response plans and leading cybersecurity risk management projects.