Courtesy of
Medical Society of Virginia Insurance Agency

Double Extortion Ransomware Attacks

In recent years, ransomware attacks have steadily been on the rise. These incidents—which entail cybercriminals compromising a device or server and demanding a large payment be made before restoring the technology (as well as any data stored on it) for the victim—are one of the most damaging cyberattack methods, incurring an average of $1 million in total losses per incident.

As these attacks become increasingly common, numerous ransomware techniques have also emerged. Specifically, double extortion ransomware attacks are now a potential cybersecurity concern for organizations across industry lines. This technique follows a similar protocol to that of a typical ransomware attack, but comes with an extra threat—the victim must pay a ransom not only to regain access to their technology and data, but also to keep that data from being uploaded publicly online.

Double extortion ransomware attacks are particularly concerning, seeing as these incidents can further pressure organizations to comply with ransom demands in order to keep their data private. Review the following guidance to learn more about how double extortion ransomware attacks work and what your organization can do to prevent such an attack.

How Double Extortion Ransomware Attacks Work

To outline the general framework of a double extortion ransomware attack, this technique starts out like most other ransomware incidents, in which a cybercriminal first gains access to their target's device or server—often via phishing scams, nonsecure websites or malicious attachments. From there, the cybercriminal is able to compromise the victim's technology and encrypt data stored on it. Then, the cybercriminal delivers their ransom demand and accompanying consequences for noncompliance.

Contrary to a typical ransomware incident, however, these consequences are twofold. That is, failing to pay the ransom could result in the cybercriminal both permanently restricting the victim's access to their technology and sensitive data, as well as sharing this data publicly on the internet. Although double extortion ransomware attacks can occur at any organization, these incidents are most common within establishments that store a considerable amount of sensitive data. This includes health care facilities, financial institutions, government organizations and large retail businesses.

Double extortion ransomware attacks can be significantly more damaging for affected organizations than typical ransomware incidents. This is because even if organizations have protocols in place (e.g., storing data in multiple secure locations) that allow them to recover their compromised information without paying a ransom, they may still be pressured to do so in order to keep their data from going public. After all, a data breach can lead to further ramifications—including reputational damages, regulatory fines and class action lawsuits.

What's more, cybercriminals who conduct double extortion ransomware attacks are known to demand higher ransom payments, sell or trade stolen data to other attackers for future extortion attempts and still move forward with sharing data publicly even after the ransom is paid (whether on purpose or by accident)—making these attacks all the more damaging.

Preventing Double Extortion Ransomware Attacks

When it comes to combatting double extortion ransomware attacks, it's important to prioritize standard ransomware prevention measures. This includes conducting routine employee training on how to detect potential ransomware risks (e.g., suspicious emails or attachments), implementing policies that prohibit

MSV℠ INSURANCE AGENCY

browsing nonsecure websites on organizational servers or devices, and installing adequate security features on all workplace technology (e.g., a virtual private network, antivirus programs, data encryption software, email spam filters, an internet firewall and a patch management system).

In addition to these key prevention measures, the best course of action for reducing double extortion ransomware attack risks is to establish an effective cyber incident response plan for your organization. This plan should explicitly address double extortion ransomware attack scenarios and outline steps that employees should take to limit the damages during such an event.

Lastly, it's vital to secure appropriate insurance coverage for ultimate peace of mind in the event of a ransomware attack. A dedicated cyber insurance policy can offer much-needed support and resources when an attack occurs, minimizing the potential damages and financial impact on your organization.

For additional risk management guidance and insurance solutions, contact us today.