IMAGINE IT

The Q3 2023 State of Cybersecurity

imagineiti.com

What happens when your business pays a ransom

When a business pays a ransom, it typically means they have fallen victim to a ransomware attack, where hackers have gained unauthorized access to their systems, exfiltrated and encrypted data, and demanded a ransom in exchange for the decryption key and a promise not to publicly expose the data. However, paying a ransom can have serious immediate and long-term consequences. Here are some possible outcomes:

- **Data decryption:** Paying the ransom may result in obtaining the decryption key, allowing the business to regain access to its encrypted data. This can be crucial if the data is essential for the organization's operations. However...
- **No guarantee of data recovery:** There is no guarantee that paying the ransom will result in the complete recovery of all data. Attackers may provide faulty decryption keys or fail to honor their promises, leaving the business with encrypted or partially corrupted data even after payment. Some estimates place the average amount of data actually recoverable by decryption keys at 65%, meaning that 35% of the data is lost even when paying a ransom.
- **Financial impact:** Ransom demands can be substantial, and paying the ransom can impose a significant financial burden on the affected business if the incident is not covered by Cyber Insurance. The payment may include the requested ransom amount as well as additional fees associated with the transaction, such as those charged by cryptocurrency exchanges.
- **Cyber Insurance Premiums:** When insurance carriers are forced to pay a ransom, insurance premiums increase globally. And if your business is forced to pay a ransom, you can expect your insurance premium to increase significantly.
- **Reinforces cybercriminal activities:** Paying the ransom encourages cybercriminals to continue their activities and may embolden them to target the same organization or others in the future. And it can create a vicious cycle where attackers perceive the targeted business as a lucrative target for future attacks.
- **Legal and regulatory implications:** Depending on the jurisdiction and the nature of the breach, paying a ransom may violate legal or regulatory requirements. Some countries and industries have specific regulations prohibiting or discouraging ransom payments.
- **Reputation damage:** Public knowledge of a breach and subsequent ransom payment can erode customer trust and damage the business's reputation. Stakeholders may view the organization as having weak security measures or being unable to protect sensitive information adequately. Also, once known on the Dark Web as a “payer”, the business risks attacks from other organized hacking groups.

Given the potential negative consequences, many cybersecurity experts and law enforcement agencies advise against paying ransoms. Instead, they recommend...

How to avoid paying a ransom

To safeguard your digital assets, it is crucial to take proactive measures that can help your business avoid falling victim to ransomware and the difficult decision of paying a ransom. By implementing the following prevention strategies, you can significantly reduce the risk of encountering ransomware attacks and paying a ransom.

- **Deploy "Immutable" Backups:** Hackers know how to destroy backups but can't if the backups are "immutable". In other words, the recovery data is stored in such a way that even a network admin cannot destroy them. This way, if your files are encrypted by ransomware, you can restore them from a backup without having to pay a ransom. Make sure your business also has immutable backups for Microsoft 365, Azure, and Google Workspace (might require a 3rd party solution). Ask your MSP to provide evidence that your backups are immutable.
- **Setup a Vulnerability Management Program:** Regularly updating your operating system, applications and verifying configurations are critical steps in preventing ransomware attacks. Software updates often include patches that address security vulnerabilities exploited by hackers. Enable automatic updates whenever possible and regularly check for and apply updates manually. Beyond that, there needs to be regular vulnerability scanning and remediation for external facing AND internal systems. Also, enrolling in an annual 3rd party Penetration Testing program is advisable to uncover additional gaps.
- **Enroll in a 24/7 Managed Detection & Response Program:** Basic business antivirus (AV) software is not robust enough to detect modern threats as it cannot detect nor thwart PowerShell or fileless malware attacks. Upgrading to Next-Gen AV and EDR will detect more threats. However, it is critical to take action against alerts 24/7 via "human-led" threat hunting and remediation.
- **Exercise Caution with Email Attachments and Links:** Ransomware often spreads through phishing emails containing malicious attachments or links. Be cautious when opening email attachments or clicking on links, especially if the email is unexpected, comes from an unknown sender, or looks suspicious. Verify the legitimacy of the email and its attachments before taking any action. Additional subscriptions, like Microsoft Defender for Office 365 or similar, can pre-scan this type of content.
- **Use Strong and Unique Passwords:** Creating long, complex passwords for all your accounts is vital. Use a combination of uppercase and lowercase letters, numbers, and special characters. Additionally, ensure that you use unique passwords for each of your accounts to prevent attackers from gaining access to multiple accounts if one is compromised. Utilizing a Password Manager application makes this process seamless.

- **Enable Multi-Factor Authentication (MFA):** Multi-factor Authentication provides an additional layer of security by requiring more than just a password to access an account. Enable MFA whenever possible, as it can prevent unauthorized access even if your password is compromised. Common forms of MFA include verification codes sent to your mobile device or biometric authentication.
- **Educate Yourself and Your Employees:** Education and awareness are crucial in preventing ransomware attacks. Regularly train yourself and your employees on best practices for online security, how to identify and report suspicious emails or activities, and how to respond in case of a potential attack. Utilizing an automated, recurring online Security Awareness Training and Phishing Campaign system makes this process significantly more effective.
- **Develop and Rehearse an Incident Response Plan (IRP):** Prepare an incident response plan that outlines the steps to take in case of a security breach or ransomware attack. This plan should include procedures for isolating affected systems, reporting the incident to insurance and the appropriate authorities, and engaging with cybersecurity professionals to mitigate the damage. Having a well-defined and rehearsed plan in place can help minimize the impact of an attack and ensure a swift recovery. Ask your MSP to review (and optionally rehearse) their IRP with you.

Pete's Insight

Does your business have the cybersecurity expertise to implement these ransomware circumventions? Does it have the thought leadership to stay ahead of the attackers? Very few small to medium businesses do. And very few MSP's have this skillset. I strongly encourage your business to investigate enrollment in a comprehensive Modern Managed Security Program built upon the NIST Cyber Security Framework.

Security pro-tip of the quarter

Protecting Against Malicious Ads

In today's digital landscape, online advertisements play a significant role in driving revenue for businesses and providing users with relevant content. However, the rise of malware and malicious ads has become a growing concern for internet users. Malicious advertisements can infect your devices with malware, compromise your privacy, and lead to various cybersecurity risks. To help you stay safe while browsing the web, I have compiled a list of essential tips to avoid malware in online advertisements.

- **Use an Ad Blocker:** Ad blockers are browser extensions or plugins that filter out unwanted advertisements. They enhance your browsing experience by removing annoying ads and act as a defense against malicious ads. A reliable ad blocker can significantly reduce the risk of encountering harmful content while surfing the internet. However, be cautious when selecting an ad blocker and choose one from a reputable source to ensure its legitimacy. Utilizing your browser's built-in ad blocker is advisable.
- **Beware of Clickbait and Suspicious Ads:** Malicious ads often employ clickbait techniques to entice users into clicking on them. Be cautious of ads promising unbelievable deals, quick riches, or free downloads. If an ad seems too good to be true, it probably is. Additionally, be wary of ads that mimic system messages or display alarming warnings, as these are commonly used to deceive users into downloading malware. Exercise caution and refrain from clicking on suspicious ads.
- **Exercise Caution with Social Media Ads:** Malicious ads on social media often redirect users to external websites that host malware or phishing. Avoid clicking on external links within ads. Look for indications of legitimacy, such as verified website domains, secure connections (HTTPS), and professional design. If in doubt, avoid clicking on the link or search the website separately to ensure its credibility.
- **Stay Away from Shady Websites:** Avoiding websites with a reputation for hosting questionable or pirated content can significantly reduce your exposure to malicious ads. These websites often lack proper security measures, making them prime targets for cybercriminals. Stick to reputable websites that you trust and that have a good track record for delivering safe and secure content.

Conclusion

Ransomware attacks pose a significant threat to individuals and organizations, but implementing the above prevention strategies can greatly reduce your risk of becoming a victim. Remember, prevention is key in the fight against ransomware payments.