HORST INSURANCE

Protecting What Matters To You®

Report Reveals Rising Ransomware Risks From VPN Vulnerabilities

The latest Coalition Cyber Threat Index Report found that 60% of cyber insurance claims stemming from ransomware attacks in 2024 involved the exploitation of perimeter security devices, namely virtual private networks (VPNs). The report compiled claims data spanning between Jan. 1, 2024, and Oct. 31, 2024. Over 40,000 VPN-related vulnerabilities were identified, representing a 38% increase from the previous year's data. Looking ahead, the report projected that these vulnerabilities will only continue to rise, potentially reaching 45,000 by the end of 2025. Although VPNs are intended to benefit businesses by providing secure gateways to internal networks and simplifying remote access capabilities for employees, they have to be launched correctly and updated on a regular basis to remain effective. Otherwise, they can end up becoming attack avenues for cybercriminals rather than protective barriers. With this in mind, it's imperative for businesses to uphold the following VPN security measures:

- **Select a trusted service provider.** First and foremost, businesses should carefully research different VPN service providers and choose one that fits their needs. Specifically, the provider should have a solid reputation and display a commitment to cybersecurity. The best VPN service providers typically provide built-in encryption features and have no-logs policies, meaning they won't store any data regarding users' online activities. Some providers may even offer extra security features, such as kill switches for compromised programs or devices.
- **Enable security features.** Businesses should be sure to enable any available security features to strengthen their VPNs, including antimalware programs, adblockers, multifactor authentication protocols and data leak prevention tools. In addition to the VPN software itself, these security features should be updated regularly. If possible, businesses should consider enabling automatic software and security updates or deploying patch management solutions to stay on track with such updates.
- **Watch for suspicious activity.** There are various threat detection tools (e.g., endpoint detection and response solutions) that can help businesses closely monitor their VPN connections and identify any unusual network activity in real time. These tools can allow businesses to address connection issues as swiftly as possible and respond to potential threats before they escalate to large-scale attacks.

By implementing these measures, businesses can uphold VPN security and minimize potential cyberattack avenues, thus preventing costly losses and related insurance claims. Contact us today for additional cybersecurity developments.

Cybersecurity Exposures Stemming From QR Codes

Quick response (QR) codes are a series of pixels arranged to form a large square that contains a long string of data. They function similarly to a barcode. They can be scanned by code readers or smartphones and often contain URLs so individuals can access websites without having to type in a specific web address. Once scanned, QR codes allow a quick and convenient way for clients to access a business's information or leave a review. They can also be used to prompt users to take certain actions, such as making a payment or downloading an app. Although they can be a useful tool, the nature of QR codes allows them to be exploited by cybercriminals. Since legitimate QR codes appear as a random scramble of pixels within a larger square, it can be difficult for users to differentiate between the safe and malicious ones. Additionally, QR codes may be standalone images, so they may not be accompanied by telltale signs of malicious activity, as is often the case with fraudulent emails (e.g., misspellings, suspicious links). Businesses encounter risks from QR codes in a couple of ways. For instance, they could be exposed to cybersecurity threats if employees scan malicious QR codes on company devices and end up compromising their login credentials, confidential business servers and data. Alternatively, if companies utilize QR codes for business purposes, their legitimate codes can be manipulated by cybercriminals, potentially impacting their customers and causing lasting reputational damage. As cybercriminals increase their use of QR codes, it's essential for businesses to mitigate the risks associated with them. In particular, businesses should:

- Provide continuous education to employees on the latest cyberthreats and dangers connected to QR codes.
- Be cautious when scanning QR codes and double-check the web addresses of the sites these codes direct users to.
- Install security software across workplace technology with content filtering that inspects links and attachments and blocks access to suspicious items.
- Maintain strict access controls for business servers to limit damage from malicious actors if they obtain employees' login credentials from QR code scams.
- Disable automatic QR code scanning on devices.
- Reduce the use of QR codes in electronic business communications to disincentivize cybercriminals from using them to target customers.

Contact us today for further risk management guidance.

Benefits of Cybersecurity Awareness Programs

Cybersecurity awareness programs provide informative training sessions on cyberthreats and cybersecurity best practices. These programs aim to educate employees and organizations about the importance of maintaining a secure online environment and the potential risks associated with cyberattacks.

Implementing a comprehensive cybersecurity awareness program is one of the most important strategies for recognizing and preventing cyberattacks. Establishing such a program can create a stronger cybersecurity culture and provide employees with essential training to prevent breaches.

These programs can offer several benefits to businesses, such as:

- **Improved employee understanding of cybersecurity risks and best practices**—Extensive training provides employees with vital information about data breaches and how to prevent them. This can lead to a reduced likelihood of successful phishing attacks, social engineering tactics and other cybersecurity incidents.
- **Faster incident response and mitigation due to employee preparedness**—Once employees are equipped with the knowledge on how to respond to cyberattacks, they can act more swiftly if one occurs. This may reduce an incident's spread and impact, which, in turn, can lessen needed response times and lower associated costs.
- **Enhanced customer trust**—Compliance with industry regulations and standards may instill trust in clients. Having a cybersecurity awareness program in place demonstrates a business's commitment to data protection.
- **Potential insurance cost savings**—Insurance providers may offer more favorable premiums to businesses with cybersecurity awareness programs because such training may reduce the likelihood of breaches, resulting in a lower chance of needing to file an insurance claim related to the losses.

Contact us today for additional cybersecurity resources.