McGowanPRO

Professional Liability Insurance

Virtual Private Networks (VPNs): Inherent Security Risks and How to Overcome Them

Each technological advancement brings with it new opportunities for cybercriminals. Cyber breaches increased by 20% in the U.S. in the first nine months of 2023 alone compared to the previous year,1 highlighting how cyberattack tactics are constantly evolving and progressing over time. Now more than ever, companies need strategies to combat cybercrime.

One often advertised way to combat hackers is a Virtual Private Network (VPN). VPNs connect essential functions and personnel securely to a company's central network. The best VPNs have further capabilities, such as data encryption, making them increasingly essential business connectivity tools.

However, despite their usefulness, VPNs also became frequent targets for hackers. This ebook will examine what a VPN is, why they have become an essential tool for businesses across the globe, and how best to protect VPNs against inherent security risks.

A Brief Introduction to VPNs

VPNs work through encryption. Data sent from a device to a VPN provider's server is encrypted along the way with a key only the device and VPN server have access to. This process is known as a "VPN tunnel". Other features are also layered on the data, working to:

- Mask IP addresses
- Encrypt personal data
- Sidestep website blocks or firewalls

Organizations use VPNs to make their online experiences more secure and private. They are attractive as they do not require cables and are entirely virtual, making setup easy. However, IT teams are required to manage VPNs and ensure they remain up to date, as well as encourage employees to use them effectively, especially when traveling.

VPNs are Essential for Businesses

Regarding online traffic, few features are as crucial for businesses as untraceable locations and anonymity. A VPN benefits a company by:

- **Securing data:** Work emails, locations, payment records, and other sensitive data sent across the internet on a public network can be accessed by bad actors, putting companies at risk. VPNs scramble data into code, encrypting it and making it harder for hackers to access it using the same network.
- **ISP and third-party tracking prevention:** Every device has a unique internet protocol (IP) address in the form of a number. Internet service providers (ISPs) use IP numbers to track a device's browsing history, effectively following an employee's activity across the internet. This trackability represents a significant security risk that VPNs overcome, as this data can be sold to third-party advertisers, given to government bodies, and even used by bad actors to break through security efforts. Instead, VPNs route browsing history through a VPN server instead of the ISP's servers, meaning the activity is masked and untraceable.
- **Working remotely:** With workers more on the move than ever, companies can rely on VPNs to protect data no matter where their employees are. With a suitable VPN, employees can access company data even on public networks without worrying about their devices being easily hacked.
- **Regional blocks:** Governments or corporations can place regional blocks on their content or internet access. VPNs allow users to bypass these blocks by spoofing the user's location. This means remote workers can have full access to the internet no matter where they are.

VPN Security Risks

While VPNs effectively improve an organization's digital security, cybercriminals frequently target VPNs. Because VPNs need to be accessible via the public internet, they can be visible to hackers and susceptible to attack.

A significant security weakness is a VPN's inherent complexity. Due to the advanced features a VPN provides, it also has multiple points along its functionality that can create a weakness. In 2022, cybersecurity firm Securin found that of the 71 VPNs they reviewed, there were nearly 1300 active vulnerabilities.2 These vulnerabilities are the result of security missteps such as:

- Ineffectual patch management
- Misconfigurations
- Missed software updates

New vulnerabilities are discovered yearly, and many are known but not yet patched, called zero-day vulnerabilities. If the VPN provider fails to update its services and shore up its defenses regularly, the result is risks that increase in severity over time.

Self-managed VPNs

VPNs managed by a company's IT team are known as self-managed VPNs. These types of VPNs are more vulnerable to cyberattacks than secure cloud-hosted VPNs or other remote access technology.

The reason that self-managed VPNs are so commonly attacked is that they are a worthwhile target. Their volume makes them worth the effort for cybercriminals. The cybersecurity industry is aware of these vulnerability issues, reporting that self-managed VPNs have noted 'high' or 'critical' vulnerabilities every year since 2021.

Companies that use a self-managed VPN experience an almost 4x higher likelihood of having a ransomware claim than those that do not

While higher rates of cyber attacks are present in companies that use self-managed VPNs, it does not strictly mean that there is a direct correlation. These companies could have vulnerabilities in other on-premises systems, or using a self-managed VPN is merely a signifier that the company is using outdated technology and makes them a target for cybercriminals.

In any instance, companies need to take steps to ensure their VPN is as secure as possible.

Making VPNs More Secure

With cyberattacks constantly changing, organizations should take all necessary steps to protect their data. The easiest action for companies is to implement automatic updates for their VPNs. This step allows the VPN to use the latest innovations in cybersecurity and ensures a breach that has been found can no longer be used following a patch.

Another way to protect a network is to limit the access of its users. Administrator accounts are especially vulnerable, as hackers can gain access to the complete network through one successful login. To combat this, organizations should reduce users' access to only the most relevant data so that even if a hacker gains access, they cannot see everything. Organizations can implement a zero-trust architecture in order to segment their networks and prevent wholesale access to anyone using a VPN key.

Implementing multi-factor authentication (MFA) also helps bolster security, preventing hackers from quickly accessing a network by asking for additional information. Users must provide more than just their password and username, with the MFA application requiring a code from an email address or another proof of identity.

The quality of a VPN also differs from provider to provider. Companies using free VPNs should research online whether the VPN has a strong reputation or consider using a paid VPN that can provide a more robust team dedicated to providing updates and patches quickly.

How to Choose the Right VPN

When reaching out to VPN vendors, organizations should evaluate a VPNs efficacy based on:

- **Reliability:** Request information on the VPN's safety features, such as MFA, IP address encryption, and more.
- **Speed:** VPNs unavoidably slow down internet speed as additional steps are added to the data that is being sent across the network. As a result, organizations that value speed and efficiency should look for a VPN that will meet their needs. The easiest way to check is to test the VPN before committing fully.
- **Reputation:** If a VPN is popular, well-recommended, and boasts excellent reviews or case studies, organizations can feel more secure in their choice. Research is vital, as only some companies that advertise a VPN service actually provide all of the features and encryption abilities VPNs should have. Taking the time to look at a VPN's online reputation will help weed out subpar offerings.

Take Security a Step Further

A final layer of protection companies should consider is insurance. The tactics hackers use are constantly evolving, with security breaches increasing yearly. This growing threat means cyberattacks will happen, and even the best security systems remain at risk.

One of the best ways to defend against cyberattacks is to prepare for the worst. Companies should rely on cyber insurance for protection, even when sophisticated cybercriminals breach defense measures. Organizations should rely on insurance from reliable providers, such as L Squared Insurance Agency LLC

L Squared provides a range of industry-leading coverages that protect against growing data security and privacy threats, including but not limited to:

- Legal liability coverage if sensitive data such as personally identifiable non-public information is stolen, lost, or disclosed without permission.
- Coverage for failing to comply with privacy policies.
- Legal cost coverage such as defending a regulatory proceeding if a privacy law was violated.

McGowanPRO
Professional Liability Insurance

Contact us:

L Squared Insurance Agency LLC
2430 Camelot Ct, Grand Rapids MI 49546
Phone: +1 800 940-1101 | Fax: +1 616 940 1196

Justin Norcross | President | L Squared Insurance Agency
Phone: 616 726 7081 | Mobile: 616 581 6072

Justin@L2Ins.com