Subscriber requested story: Cybersecurity - What VPNs can and can't do for you

Published on: 6/4/2019 Content area: Investment Adviser Comments?

Your local coffee shop may produce a quality cup of joe and offer you free Wi-Fi but be cautious that the service doesn't come with a malicious slice of cyber nastiness.

"When you're on public Wi-Fi, everything you do can potentially be inspected" by cyber spies, notes **Ray Hillen**, managing director for cybersecurity at **Agio** in New York.

A favorite antidote is to deploy a virtual private network. A VPN "is like a pipe" that connects two ends, encrypts the communications and prevents intrusion by a third party, says **Jeffrey Ingalsbe**, chief information security officer at **Flexible Plan Investments** ($1.6B in AUM) in Bloomfield Hills, Mich.

"Chances are the software you're using, whether they say it or not, is creating a private network" for your office, says **Bruce Leibstone** of **Warren Systems Group** in New York. "Most people may be using a VPN without realizing it."

Ammo in your cyber arsenal

Consider a VPN to be an essential tool should you have staff remotely connecting to your network, especially if they're logging in using public Wi-Fi in hotels, airports or a local **Starbucks**. "Whenever we're in a public location, our VPN is engaged," says **Tim Villano**, president/CIO, **Artemis Global Security** in Lakeview, Conn. "That's the standard I think we should have."

Many of the IT experts **IA Watch** spoke with also encouraged the use of VPN services for your personal devices, including your cell phone. Leibstone recommends **NordVPN**. Here's another list of vendors.

"It's just one layer of security" and not the end-all, be-all of cybersecurity, Villano says of VPNs. Leibstone favors VPNs that come with dual-factor authentication, a second level of security. Villano says you also must run anti-virus software, regularly download security patches, instruct staff not to open suspicious e-mail attachments and maintain a firewall, among other cybersecurity best practices. Ingalsbe suggests the use of routers and packet filtering as well.

There are no industry standards for VPNs. Leibstone recommends you go with a well-known brand, like a **CISCO** firewall. Ingalsbe suggests you search **Gartner's Magic Quadrant** for any recommended VPNs.

Tips for selecting a VPN vendor

"Firewall vendors aren't all the same," notes Ingalsbe. Ask your vendor how its VPN traffic works and how often it monitors your network traffic for trouble. The vendor should be periodically revisiting its VPN security. Include this inquiry in your annual cybersecurity vulnerability assessment, he adds.

Tip: Ask your firewall vendor how best to log in remotely, suggests Leibstone.

Know that VPNs don't protect you against two vulnerabilities, Ingalsbe continues. One is a so-called "man in the middle on the other end" and the second is an employee who places the VPN's settings on his personal laptop and then visits risky online sites. This behavior can permit a cyber bad guy to get "dropped off in the corporate network. It's like an Uber," he says. The bad guy bypasses your security and could snoop until his evil heart is content unless you've deployed other cybersecurity measures.

Be aware of "split-tunneling" VPN, points out Ingalsbe. This requires all incoming internet travel to go through your VPN but outgoing traffic need not. Firms often will permit this technology because staffers don't want the network to restrict which internet sites they can visit.

Villano, whose firm builds VPNs for advisers, suggests you start by talking with your IT managed service provider. Ask if it should build you a VPN or if you're best to go with a commercial brand. Ask your VPN provider how long it maintains its logs, he adds.

Keep an eye on things

Logs will allow you to know “who connected when and for how long” and from where, counsels Hillen. Better still, limit the access to your network when someone logs in remotely. “They shouldn’t have access to everything,” states Hillen.

“We are beginning to migrate away from” VPNs, Hillen continues. Cloud services with encryption are gaining fashion. He favors virtualized desktops. Instead of connecting through a VPN, a virtual desktop “runs in the environment and doesn’t allow your workspace to be in the environment,” describes Hillen. This can keep malware out of the network. Add dual-factor authentication and “if you have something nasty on your device it doesn’t have the opportunity to get to your network,” he adds.

Villano notes OCIE examiners are focusing on cybersecurity and remote access (**IA Watch**, March 28, 2019). He predicts examiners will ask to see your P&Ps related to remote connectivity.

The information contained herein was current as of the publication date.

Indexed by: Compliance Best Practices | Cybersecurity |

Back to Search Results /