EBOOK

4 TIPS FOR STRENGTHENING THE SECURITY OF YOUR VPN ACCESS

HOW SECURE IS YOUR VPN ACCESS?

Remote access gateways such as VPNs and firewalls provide critical anywhere-anytime connections to the networks and resources your remote users require in order to do their jobs. Today’s business environment is made up of a variety of users, including employees, contractors, vendors, customers, partners, and audit teams. Identity is the new perimeter – and a major attack vector. How can you strengthen the security of your VPN access?

FIND OUT INSIDE.

VPN SECURITY

TIP #1

ARE YOU STILL LEVERAGING USERNAMES AND PASSWORDS?

According to the 2016 Verizon Data Breach Investigations Report, 63% of confirmed data breaches leveraged weak, default, or stolen passwords. Usernames and passwords simply don’t provide enough protection, and expose your systems and data to cyber threats.

USE STRONG AUTHENTICATION

Two-factor authentication (2FA) methods require users to have two forms of identification in order to gain VPN access: something they know (e.g., username/password) and something they have (e.g., a hardware token).

Multi-factor authentication (MFA) tools extend this concept with a third identifier: something the users are (e.g., unique physical or behavioral characteristics). These tools provide convenience and security for your remote users with a variety of authentication options such as push notification and biometric (e.g., fingerprint).

VPN SECURITY

TIP #2

ARE YOUR USERS WHO THEY SAY THEY ARE?

Today’s rapidly growing mobile workforce and open business environment is expanding the requirement for remote access beyond employees to include contractors, vendors, customers, audit teams, and partners. In order to conduct business, stay competitive, and maintain agility, modern organizations are opening their networks to this broader user base. To minimize risk, it’s important to ensure that these users are who they say they are – and that they have the appropriate levels of access to your systems and applications.

BE SURE WITH IDENTITY AND ACCESS ASSURANCE

Depending on your industry, two-factor authentication or multi-factor authentication (2FA or MFA) for remote access may be a requirement. Even if it’s not, using these methods to secure your remote access gateways is an important step towards mitigating your risk from unauthorized users.

VPN SECURITY

TIP #3

ARE YOU FEELING POWERLESS?

The variety of external users introduces other variables too, including risk. A vendor's security standards, for instance, may not be the same as yours. In its March 2016 research report, the Ponemon Institute reported "a lack of confidence in third parties' data safeguards, security policies and procedures." It's true, you have no say in how other organizations handle their security. Ensuring the security of the remote user access to your systems, though, IS under your control.

TAKE CONTROL

The use of two-factor or multi-factor authentication (2FA or MFA) with context-based risk analysis allows you to enforce security standards, prompt users for step-up authentication if needed, and reduce risk by granting vital remote VPN access to your corporate systems and resources to authorized users only.

VPN SECURITY TIP #4

ARE YOU PUTTING YOUR BUSINESS AT RISK?

The high-profile 2013 Target data breach underscores the importance of securing your network access to third parties. Stolen credentials from the retailer's subcontracted HVAC vendor led to this devastating attack that resulted in the theft of the data of 70 million Target customers and 40 million credit and debit cards.

LOCK IT DOWN WHILE OPENING IT UP

The ability to collaborate and connect with geographically dispersed and external users is essential in our digital age. Their environments, behaviors, and devices, though, are variable that can introduce unnecessary risks to your business. Your best defense is a good offense. Start with a security solution that protects your VPN access against identity threats with convenient AND secure access.

AN EFFECTIVE IDENTITY & ACCESS ASSURANCE SOLUTION CAN:

- **Provide convenient and strong** authenticated access based on continuous risk-based analysis and contextual awareness
- **Automate processes** to manage which systems and resources users are authorized to access
- **Control what users can do** within those applications in order to meet your compliance and governance demands

SUMMING IT UP

STRENGTHEN THE SECURITY OF YOUR VPN ACCESS

VPNs and firewalls are effective remote access gateways. It takes a little more effort in the current business environment to ensure that users *really are* who they say they are.

Modern authentication and identity assurance solutions such as the RSA SecurID® Suite provide multiple convenient and secure ways to authenticate all of your users, analyze their behavior and context, and automate their levels of access – from anywhere and any device.

There's no better time to secure your VPN access than right now.

VISIT RSA.COM/TRYSECURID TO SIGN UP FOR A FREE TRIAL