Why Enhanced Cyber Security Is Required for Remote/Hybrid Workforces

OneConnect

7 Southside Drive, Suite 210,
Clifton Park, NY 12065
(518) 371-2295

www.oneconnectinc.com

The COVID-19 pandemic forced businesses to move to remote work to keep their operations running. Now, experts like McKinsey are convinced that remote/hybrid workforce models are here to stay. While businesses are struggling to support the remote/hybrid environment, the cyber security landscape is heating up as well.

HP Inc. announced the launch of HP Wolf Security and published a new report, Blurred Lines & Blindspots. The report combines findings from several global surveys by distinguished cyber security analysts like KuppingerCole. Here are some of the key conclusions from that report.

There has been a 238% jump in global cyber attacks during the pandemic.

Just over half, or 54%, of IT decision makers reported increases in phishing attacks, 56% reported an increase in internet browser infections, 44% reported that compromised devices were being used to spread infections throughout their organization, and 45% reported attacks using compromised printers.

In addition, a recent Tenable study offered more insight on the problem. The vast majority of participants in this study (80%) reported that they have more cyber risk as a result of remote work.

It's obvious that businesses of every size and in every industry must increase cyber security protections to survive the remote/hybrid workforce of the future. To accomplish this, you'll need to understand what the threats are, the essential areas you need to address, and the specific technologies and solutions you need to invest in.

CRITICAL CYBER SECURITY ISSUES RELATED TO REMOTE AND HYBRID WORKFORCES

The question of why remote and hybrid work causes so many cyber security issues has been on the minds of virtually all IT and business leaders. Based on the research, these are the key issues IT professionals encounter:

THE LINE BETWEEN WORK AND HOME HAS BLURRED

Today's workers are frequently working from home and admit to using personal devices for work and work devices for personal tasks. It's much more difficult and sometimes impossible for IT teams to keep track of and protect the devices and networks that are accessing business systems. Cyber criminals are happy to take advantage of these facts and attack remote workers. The result is that 67% of cyber attacks that impact businesses use remote employees as their initial targets.

Since remote employees aren't in a structured business environment, they exhibit a range of behaviors that make them a threat. For example, they often use their home WiFi networks that aren't secure enough to keep out hackers, don't worry about assigning secure passwords to the systems they access, use public WiFi networks at coffee shops, and they may even leave their devices unattended while they refill their coffee cups.

THIRD-PARTY SOFTWARE USAGE IS INCREASING

Employees are using business related third-party software more frequently, and many have third-party software on their personal devices that they use for work. As a result, IT leaders are seeing more attacks targeting vulnerabilities in third-party software that spill over into their business systems.

PHISHING AND MALWARE ARE SIGNIFICANT THREAT VECTORS

Phishing and malware are the most serious threats related to remote workers according to IT leaders in the U.S. When remote workers are at home, they're not as careful to watch for phishing emails. All it takes is opening an attachment or clicking on a link without questioning the source, and the phishing email has achieved its goal.

In addition, given the lack of tight security for many networks and devices used by remote workers, it makes sense that planting malware like ransomware is much easier in remote environments. Ransomware is reported as a top concern for IT teams because the effects can be devastating, often costing the business money, and causing loss of data, business interruption, decreased profits, loss of reputation, and more.

OneConnect

7 Southside Drive, Suite 210, Clifton Park, NY 12065
(518) 371-2295 | www.oneconnectinc.com

6 CYBER SECURITY ESSENTIALS FOR REMOTE AND HYBRID WORK

Microsoft recently published its 2021 Digital Defense Report which was created with contributions from security professionals in 77 countries. One of the key findings in that report is that businesses need to adopt a zero trust (never trust, always verify) security strategy for remote and hybrid workforces.

Because of remote work, there are many more cloud applications in use and remote workers are using their own devices. Therefore, cyber security that relies on firewalls and virtual private networks (VPNs) is ineffective in today's environment. Zero trust principles must be applied in these six areas to protect a business supporting remote and hybrid workers.

1. USER AUTHENTICATION

Whether a user is a person, service, or IoT device, the zero trust principles need to apply to authentication. Traditional protocols such as IMAP, SMTP, POP, and MAPI don't support a robust form of authentication like multi-factor authentication (MFA). New protocols need to be implemented that can support MFA at a minimum, and authentications that aren't based on passwords are even more desirable.

2. ENDPOINTS

Endpoints such as desktops, laptops, smartphones, servers, workstations, and IoT devices are prime targets for cyber criminals. Once a user or identity has gained access, data can flow to other endpoints, which creates a large attack surface for criminals to exploit. A zero trust model applied to endpoints will ensure that only verified devices can access business systems.

3. APPLICATIONS

While many cloud-native and modern applications require authentication, many others that were designed for direct connections rely on firewalls and VPNs to control access. These legacy applications don't use a least-privilege access protocol and can give users access with much higher permissions than are required or desirable.

4. NETWORK

Network attacks can be mounted using malware, phishing emails, and web applications – among other vectors. Protocols that are open to the internet are most vulnerable to these types of attacks. Protecting against distributed denial of service (DDoS) attacks is another aspect of the zero trust approach.

5. INFRASTRUCTURE

Most IT infrastructure has been changing as a result of remote work. In many businesses, applications were moved to the cloud almost overnight to support remote work when the pandemic first hit. It didn't leave time to carefully plan how to protect infrastructure whether it was on-premise, cloud-based, in containers, or provided by microservices. Applying zero trust principles to a businesses' infrastructure is critical.

6. DATA

Protecting data became much more difficult as remote workers took data away from the infrastructure that businesses control. Things such as encryption and data loss prevention are still core requirements for data security, but every organization also needs to manage sensitive data to make protection as effective as possible. Reducing risk requires that organizations put controls in place to make sure sensitive data is identified and properly controlled. Other controls on storage, access, flow, and determining when data should be eliminated are also critical.

CYBER SECURITY TRAINING FOR REMOTE AND HYBRID WORKFORCES

There are a variety of ways for businesses to bring their cyber security up to a level that will make remote and hybrid workplaces safe, but of particular importance is training employees on cyber security practices. Research has shown that a large percentage of cyber attacks involve some type of human error. An IT employee could misconfigure the security features of an application, for example. However, frequently

the error could be a line-of-business employee falling prey to a phishing email, which is becoming more common in remote workplaces.

Establishing a cyber security culture needs to start at the top and be supported throughout the business. Remote work is very common in today's workforce, but employees also need to realize that it comes with additional responsibility for cyber security. Investing in periodic training on cyber security will help keep the issue top of mind and remind employees of good cyber security practices.

CONCLUSION

The remote and hybrid workplace was thrust on businesses with little warning at the onset of the pandemic. However, as we move toward the hybrid workforce becoming a standard, business leaders need to take the opportunity to carefully evaluate the cyber security risk they face and determine the steps they need to take to mitigate that risk.

Developing the most effective cyber security strategy requires high level expertise. Many organizations can't afford and/or don't need those types of experts as full-time employees. For that reason, business and IT leaders are reaching out to technology experts who can work with them to choose the right cyber security technologies and solutions that will keep their organizations protected in this hybrid workforce business environment.

7 Southside Drive, Suite 210, Clifton Park, NY 12065
(518) 371-2295
www.oneconnectinc.com

OneConnect