tripwire

WHITE PAPER

Cybersecurity for Work From Home Tools

Challenges and Tips for Securing Remote Work Environments

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

A large segment of the global workforce has had to shift quite abruptly to working from home (WFH) in response to the COVID-19 pandemic. Results have varied widely in terms of the seamlessness of that transition. Ready or not, meetings and collaboration have become virtual by default for a lot of organizations. Cybersecurity and IT leaders the world over have been put in a difficult position akin to having to build a car that's already driving. This white paper covers the biggest challenges of that shift, and some actionable steps you can take to overcome them.

One of the most widespread effects of this sudden switch to remote work is the ubiquity of collaboration tools such as Microsoft Teams, Zoom and Webex. With these tools becoming the new default, it's a critical time to assess the common cybersecurity issues that arise in work from home environments. You can still maintain security and compliance amidst the increased use of these collaboration tools—if you know where to look.

Security Under the "New Normal"

Meetings, not only the individual one-on-ones but also mass gatherings of employees, have moved to the internet. The ability to video conference and feel some sort of human connection has become important for many employees. Collaboration is happening online with various tools that have been available for years, such as SharePoint and Confluence. Previously less-known offerings, for example whiteboard.microsoft.com to replace conference room whiteboards, are now being adopted at a quicker pace as well. Chat applications such as Teams and Slack are also relied on more heavily. These are just a few examples, but every aspect of business is becoming more virtual to minimize interruptions.

Shared Cloud Responsibility

First, it's important to understand that oftentimes products and services are shipped in an insecure state in order to make them more approachable by the general public. The reason for this is that the maker of these services wants to reduce the friction for customers to use what they've built. Implementing controls that increase friction can be a risk for losing users, but it's up to the customer to shift some of the usability over to security. However, having a secure ecosystem of tools for working from home doesn't mean that these tools are completely unusable.

The Amazon Web Services (AWS) security model brings up something to think about when adopting these types of technologies for working from home. There's a common misconception that cloud providers handle all security, possibly leftover from the era of hosting providers. While there are specific items that the provider is going to be responsible for, the truth is that there is a lot of security the customer is also responsible for. There are also shared controls and customer-specific controls that the customer must maintain in order to have a secure deployment of the service. So examining your cloud provider's exact security responsibilities versus your organization's is key.

Client-Side Vulnerabilities

WFH tools often include a client-side application running which connects the user to the service in question. This could be a VPN, a chat program, or even a browser extension to connect to a video conferencing service. Each of these are code running on endpoints, which can become an entry point for attackers. The purpose of these WFH tools is to enable business operations worldwide, which may have previously been conducted behind closed doors. Because of this, there are opportunities for private information to leak in ways previously not paid attention to.

It's important to understand how these are kept up-to-date and plan accordingly. Are these applications configured to automatically update, or are they going to alert the user that the update is available and that they, the user themselves, need to install? Or are you left on your own to manage how these updates are applied?

Widely-used programs such as Slack, Zoom, and Teams have all had client-side security issues. Slack had a recent vulnerability that allowed a malicious link to change where documents are saved, potentially leaking information to attackers. Zoom has also had various vulnerabilities reported recently, mainly due to the fact that more researchers are focussing on this suddenly-popular tool. Likewise, Teams is also facing issues with vulnerabilities, allowing attackers to control meetings and increase their permissions within the environment. All complex software is going to have bugs. The great news is that these vendors are taking security seriously and are regularly rolling out updates.

Password Security

It's also crucial to assess the password policies in play. This can include password complexity requirements or multifactor authentication, as well as just simply setting a password for some of these services. With the increased popularity of tools like Zoom comes increased focus from the hacker community. For example, a tool called zWarDial, available on GitHub, can scan hundreds of meeting IDs within seconds to automatically detect which ones it can enter without a passcode. So even if you're not publicly screenshotting your meeting IDs to the world, hackers can still quickly identify if you're vulnerable.

Meeting passwords certainly help. But only having a password is not enough. Credential stuffing is another common tactic from attackers using password dumps from other various breaches. They may take passwords from

something more benign like a forum and then reuse those credentials on other services such as banks, social media, or even these WFH tools. Risks like credential stuffing can be prevented by having some form of multifactor authentication—be it a one-time code, an SMS message, or app-based authentication.

Three Ways to Secure Remote Work Tools

There are steps for securing these types of WFH tools that are available to everybody. Here are a few options that you can start taking today to start securing these tools if you're using them within your own organization.

Use Industry Benchmarks

One of the better hardening tools that we've had available to as defenders these days are benchmarks from the Center for Internet Security (CIS) and technical implementation guides or STIGs from DISA (Defense Information Systems Agency). These provide prescriptive guidance on how to lock down operating systems, applications and various other services or devices. Unfortunately, these are hard to come by for tools that are enabling remote work. There are Citrix hardening guides from DISA available. You can also look to benchmarks from CIS for traditional VPNs and firewalls. It's worth looking on the CIS website to see if any of the tools that you're using have some of these hardening benchmarks available.

Follow Vendor Security Guidance

If a hardening benchmark is not available, the next best option is to look into the security guides and best practices published by your vendors. The downside to these guides is that vendors are oftentimes less prescriptive than CIS and DISA. Many of these are simply found by searching Google for the service provider name followed by a hardening guide or best practices—for example, "Zoom hardening guide" or "Cisco Webex practices." When in doubt, you can always reach out to the provider and see what they may have available for you.

When all else fails, you can fall back on the CIS Controls. While they may not match directly or explicitly call out the particular WFH solutions you're using, they should be broad enough to adapt. And remember that to apply the right security controls, you need to have a clear picture of how users are connecting. Understand how your organization's employees are using VPN services, for example.

Harden Home Hardware

By and large, organizations can't take full responsibility for the security of the home networks their employees use. But there are some things that you can encourage to help them secure their home networks. One of the biggest risks to any home user is their router or access point—that central termination point between their house and the public internet that must be kept up-to-date. That is going to be the easiest access point for any attacker to enter, so it should be a security priority all remote employees understand how to navigate. Help employees understand best practices like using guest networks and not letting their kids use work computers. Strong password-protected home networks and well-updated hardware can go a long way in keeping remote workers secure.

Summary

The onset of COVID-19 caused a rapid move toward WFH tools and remote work environments. The unexpected nature of this shift means security teams have had to quickly determine the best ways to secure those tools and home offices against new and expanding attack vectors. The challenges at the center of this shift include cloud account security, password management, and client-side vulnerabilities. Taking advantage of industry benchmarks and prioritizing the hardening of these remote work tools and environments will move your efforts in the right direction.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

WPCWFHT1a 2007