E-Guide

Maintain Security Policies with a Remote Workforce

ComputerWeekly.com

In this E-Guide:

Coronavirus: How to implement safe and secure remote working

The massive influx of remote workers has raised new challenges for security professionals – namely, how to maintain the same security posture that was in place when workers were predominantly office based.

Inside this E-Guide, learn about the considerations to take to ensure that remote work is being conducted safely and securely, including a look at new VPN and endpoint security factors.

Coronavirus: How to implement safe and secure remote working

Alex Scroxton, Security Editor

While much of the cyber security news agenda around the coronavirus outbreak has focused on the opportunistic, callous nature of cyber criminals, for whom this presents a golden opportunity to spread chaos and make a fast buck, for the average business cyber security is about more than keeping abreast of threat campaigns, bug disclosures and cyber attacks.

Currently, the biggest concern for chief information security officers (CISOs) and other security professionals is maintaining their organisation's cyber security posture during a period where the vast majority of office-based, IT-reliant workers are going to be working from home.

As Tal Zamir, founder of Hysolate, an Israel-based supplier of software-defined endpoint technology, explains, the transition to a temporary state of compulsory remote working surfaces challenges old and new.

"It is said that home is where the heart is, but with the coronavirus forcing a large part of the workforce to work from home to help contain its spread, home could be where the headache is," says Zamir.

Coronavirus: How to implement safe and secure remote working

If it’s not too late, lay the groundwork

Assuming it is not already too late to do so, IT and security teams should do their best to get out ahead of the transition to mass remote working by taking a few preparatory steps, says Liviu Arsene, a global cyber security researcher at BitDefender.

“Before deciding to enforce work-from-home policies, IT and security teams need to assess their current resources, project how much strain they need to support to enable remote employees to work in optimal conditions, and assess what risks need to be factored in and address,” says Arsene.

“For example … setting up and supporting conferencing software that ensures both a stable voice and video connection should be a priority, as most meetings will occur virtually and reliability is key.

“Making sure that all employees have valid credentials that don’t expire in less than 30 days is also mandatory, as changing expired Active Directory credentials can be difficult when remote.

“Even if a large number of employees need to change their passwords before leaving the office, it’s a hassle-free procedure that is best addressed proactively than reactively,” he says.

It goes without saying that whenever an employee is working remotely, they should be accessing your organisation’s network and any software-as-a-service (SaaS) resources they need via a virtual private network (VPN).

A VPN is a piece of software that creates a safe, encrypted “tunnel” from the user network, whether public or private Wi-Fi, across the public internet, and into the organisation’s network.

If preparing for a sudden increase in the volume of remote workers, it is absolutely critical to make sure that you have enough licences to accommodate simultaneous connections from all of them, says Arsene.

Phil Chapman, a senior cyber security instructor at Firebrand Training, says there are several steps security teams can take to make sure their VPNs are as robust as possible.

“Make sure employees are using a VPN with appropriate encapsulation and authentication to the data they are accessing. If possible, use IPSEC or SSTP [Secure Socket Tunnelling Protocol] as a connection,” he says.

“You can suggest split tunnelling, which allows a user to establish a secure VPN for work-related connections but use their own internet connection to do non-work related activities.”

Are VPNs all they’re cracked up to be? The answer may surprise you

In reality, for all the industry talk of the VPN as a means to enhance security, the technology comes with its own set of problems, as Chapman points out.

For one thing, they are reliant on the security of the originating network, and if this isn’t up to scratch, it can be a potential source of trouble.

“Advise your employees to avoid using their Wi-Fi connection at home and rather connect their laptop or workstation to the router with a network cable. Not only does this provide a more secure connection, but also enhances speed as it will be quicker than wireless,” he says.

“There is a greater security risk of using potentially malicious Wi-Fi networks and infected personal devices to access corporate assets. Security teams want to ensure that access to corporate resources is always done from a safe, trusted, operating system – in some cases, this is a hard compliance requirement,” adds Hysolate’s Zamir.

“A work-from-home solution must protect against a variety of endpoint-related attack vectors, such as OS vulnerabilities, app vulnerabilities, network vulnerabilities, browser/mail vulnerabilities, USB/external device vulnerabilities, and insider threats. It should be hard for malware to simultaneously access corporate network resources and have direct unfiltered access to the internet.”

Endpoint security and the CISO’s dilemma

“The Achilles’ heel for many IT teams will be securing endpoints that remote workers use to connect to the corporate network, endpoints that now will be fair game for cyber criminals,” says Zamir at Hysolate.

“As we prevent viruses from infecting our bodies through isolation, so too do we look to prevent viruses from infecting our computers. Isolation is the key to prevention. It ensures separation between healthy and ill.

“For the health of our corporate infrastructure, we leverage isolation to separate sensitive data from anything that could potentially cause it harm, including the wild internet.”

Coronavirus: How to implement safe and secure remote working

For this reason, says Zamir, the most sensible thing to do is to lock down all employee devices. But in practice, he acknowledges, this is a terrible idea because the lock down model typically ends up being just another source of frustration for users, and one they will try to get around, putting the business at greater risk than it might otherwise have been at.

“Users prefer to use a single device with a single set of peripherals, without switching between devices. They would like to have direct connectivity to their apps and data, without any added network latency, both in the corporate network, in the cloud, and in their personal home network,” says Zamir.

“They expect to always work natively and locally and have fast, responsive applications. They want to be able to print with their home printers and to be able to use their Wi-Fi networks at home or at the coffee shop.”

For this reason, CISOs must walk a fine line between overly restricting user behaviour and optimising cyber security hygiene. If the restrictions are too tight, you risk alienating your user base and choking their ability to work productively, but if the restrictions are too loose, you risk exposing your business to unacceptable levels of risk.

Sending out rules and guidelines regarding accepted applications and collaborative platforms is a must

Liviu Arsene, Bit Defender

“Sending out rules and guidelines regarding accepted applications and collaborative platforms is also a must, as employees need to be made aware of what is sanctioned and what is not,” says Arsene at BitDefender.

Coronavirus: How to implement safe and secure remote working

“Combined with the deployment of network security, monitoring, and logging tools, IT and security teams can be notified whenever untrusted connections or unauthorised applications are spotted to quickly and timely block them.”

CyberArk Europe, Middle East and Africa (EMEA) director David Higgins says that endpoint security for remote workers should be considered in the context of a zero-trust security policy.

“In the current environment, where endpoint devices such as smartphones and laptops have disparate levels of security, cyber security needs to match the flexibility of modern working,” he says.

“We can no longer ensure the security of these endpoints. We should assume endpoint devices are already compromised or soon will be. This position is important because it mandates that we adopt the critical premise of zero trust by enforcing isolation to prevent such devices ever directly accessing critical assets.

“Once combined with a just-in-time provisioning of access process, this can dramatically reduce the likelihood of an attacker using a remote worker’s identity to infiltrate a business,” he says.

Talk to your people, don’t let them be the weakest link

As has been demonstrated time and time again, one of the greatest risks to organisational security is humans themselves, who collectively display an ability to accidentally do the wrong thing in almost every situation – in this case, falling for a cyber security threat.

Coronavirus: How to implement safe and secure remote working

At a time of heightened stress and fear, this becomes even more crucial. What is more, the cumulative volume of phishing emails and other cyber threats that have coalesced around the coronavirus is enormous – it may even be the largest ever.

All this adds up to a real headache for CISOs, but fortunately, if your workforce is appropriately equipped and educated, it doesn't need to be, leaving you free to concentrate on the big issues.

Even though some of the risks associated with working in a public place – or even in an office – are minimised when isolated at home, Firebrand Training's Chapman says remote working staff can start by behaving as if they are in the office and apply the same mechanisms as they would in their usual workplace.

"Acceptable usage policies (for corporate and bring-your-own-device equipment) should be robust and apply at home equally as at work. This also includes in regards to telephone calls and online meetings," he says.

Oz Alashe, CEO at CybSafe, says there are several basic steps that remote workers can take to protect themselves. "All emails, text messages and phone calls can be faked or 'spoofed' to appear as if they're from colleagues or from other trusted parties," he says.

“These attacks are especially convincing for remote workers. For emails, check the sender details. If you receive a request you weren’t expecting, or one which has an undue sense of urgency, slow down. Stay in control of your actions.

If you receive a request you weren’t expecting, or one which has an undue sense of urgency, slow down. Stay in control of your actions

Oz Alashe, CybSafe

“Think about what protections you need to have in place at home. As a minimum, use an antivirus program, turn on your firewall and update when prompted.

“Use a favourites list or Google to navigate through the internet. Do not follow directions or links from emails or text messages you weren’t expecting. If you think you’ve identified a social engineering attempt, report it. If you’re unsure, ask. It’s good to talk about cyber security.

“Don’t leave yourself vulnerable to malware infection or data loss. Encrypt your data and keep backups on clouds and external hard drives just in case.

“A green padlock doesn’t necessarily mean a website is safe. Make sure you check the website’s URL. If you’re ever unsure about the legitimacy of a website, stop. Google it and follow the link provided to reach your destination,” he says.

Remote working doesn’t have to be risky

The volume of interest in coronavirus means that cyber criminals and threat actors will continue to heavily exploit it, and depending on how long the crisis stage of the pandemic

lasts, we could be looking at the emergence of a highly significant, long-term cyber security issue.

However, as is so often the case when it comes to cyber security, paying a little care and attention to basic security hygiene should be the first priority for both CISOs, security teams and users.

Just as going into self-isolation and quarantine will help us collectively flatten the curve and minimise the number of coronavirus infections and deaths, collective caution when it comes to remote working and cyber security will help organisations and individuals avoid falling victim to a needless and unnecessarily distracting incident.

Coronavirus: How to implement safe and secure remote working

Read more about remote working

- Staff are going to have to work from home, if they can, for the foreseeable future. We look at steps to ensure they remain fit and productive.
- With hundreds of thousands likely to be working remotely for some time, the UK's NCSC has issued best practice guidance to enable security teams to support them.