SoftwareTrends

Securing the Remote Workforce of 2020

Organizations are increasingly embracing the flexibility and cost savings of employing a remote workforce, but IT teams must prepare to provide support and secure networks.

The ability of the worker to be able to work wherever and whenever they have an internet connection and a connected device has been an innovation that has introduced flexibility and mobility that allows business to be conducted in ways never thought of before.

But that disconnection from the four walls of the workplace has created challenges for the IT team tasked with ensuring the electronic security of the remote worker. Without the security ensured by an onsite, hardwired connection to an organization's servers, it becomes much more difficult to control who has access to the remote connection. Sensitive information can be compromised without the worker knowing, and it's imperative that controls and protections exist to help protect the corporate network from the outside.

The biggest threats to a remote workforce by far come in the form of phishing attacks and malware, both of which take advantage of a combination of insecure networks and unsuspecting human behavior to cause trouble.

"An attacker's primary goal is to gain entry and expand across domains so they can persist in an organization and lie in wait to steal or encrypt as much sensitive information as they can to reap the biggest payout," wrote Rob Lefferts, Corporate Vice President for Microsoft 365 Security, in a blog chronicling the problem.

"This is where intelligent solutions that can monitor for malicious activity across—that's the key word—emails, identities, endpoints, and applications with built-in automation proactively protect, detect, respond to, and prevent these types of attacks from being successful."

The Remote Worker is Here to Stay

As mobile technology has improved in recent years, so has the popularity of the gig economy and the worker with a remote workstation.

But it was the COVID-19 pandemic of 2020, which forced millions of Americans to shelter in place in their homes as well as work remotely from whatever spaces they could call a home office, that tested the ability of organizations to support and secure a mostly-remote workforce.

By 2028, almost three-quarters (73%) of all companies will employ remote workers.

As a result, employers were also forced to change their practices, shuttering offices and making contingency plans to support their workers who were still expected to do their jobs while staying healthy and taking care of their families under unprecedented levels of stress.

Remote working is a trend that’s long been poised to become prevalent. Even before the COVID-19 crisis, the gig economy and a general trend toward more flexible work environments has led to a dramatic increase in the number of remote workers. Consider the following statistics which show how fast the remote working trend has grown and how fast IT has had to catch up with protecting the networks that support those workers:

- As of February 2020, about 4.7 million, or just under 3.5% of the U.S. population were working remotely, according to a report from FlexJobs.
- Even before that, about 43% of the U.S. workforce did their job from home at least some of the time, according to a report from Harvard Business School.
- In the last five years, the remote workforce has grown by 44% comparing that with the last 10 years where it has grown about 91%, according to FlexJobs report.

The number of full-time remote workers will likely continue to rise, as employers begin to realize they can reduce office costs while giving workers the flexibility of working remotely—after all, happier employees make for more productivity.

During the pandemic, an estimated half of American workers were working from home, according to numbers from the Brookings Institute, and employers saw benefits from keeping them out of the office. In fact, one in five chief financial officers said the cost savings had inspired them to keep at least 20% of their workforce working remotely in the future. Furthermore, a 2019 report from Upwork projects that by 2028, almost three-quarters (73%) of all companies will employ remote workers.

Protecting the Basic Needs of a Remote Workforce

In order to work efficiently in a remote environment, workers need to have access to all of the tools they would be used to employing in the office. At a minimum, remote workers require a laptop or similar connected device and access to the internet, along with communications tools such as email, teleconferencing capabilities, access to file sharing networks, and function-specific capabilities for their particular position—many of which live in the cloud.

One of the biggest challenges for IT managers when dealing with a remote workforce is security—of the devices they are working on and the networks they will be connecting to, and from the inevitable online phishing and malware attacks to which they will be subjected. IT teams enjoy the ability to control things from within the "fortress" of their own domain, where they know the devices that are connected on the network, and can control the quality of antivirus software and access points; in the remote world there is very little way to control these factors and therefore endpoint security must be employed strategically.

Laptops and devices must be protected.

In a perfect world, employees are issued a laptop that doesn't leave the building and is only connected to the corporate internet network, therefore making them somewhat impenetrable to malicious activity. While it should be mandated that employees use company-issued devices when working remotely, the reality is that we are living in a world where BYOD (Bring Your Own Device) and the security challenges it presents to a network is more often the way people do work.

Think about it: how many remote employees have checked their work email on their smartphone or tablet? Are clients ever contacted via text message on a personal phone? Do remote workers use USB sticks to store sensitive information or documents with financial or other proprietary information? Chances are, yes, and these practices leave your organization vulnerable.

IT teams enjoy the ability to control things from within the "fortress" of their own domain, where they know the devices that are connected on the network, and can control the quality of antivirus software and access points; in the remote world there is very little way to control these factors and therefore endpoint security must be employed strategically.

Experts suggest that any connections made to the company from outside sources should be performed through a VPN (Virtual Private Network) which uses technology such as SSL (Secure Sockets Layer) or IPsec (Internet Protocol Security) to encrypt communications from the remote device.

Networks must be secured using multi-factor authentications.

The most secure way for remote workers to do business is to access the corporate network they are used to working on in the office, known in IT circles as the “headend.”

The problem is that workers will likely be connecting using a vulnerable public or home Wi-Fi connection, the “endpoints” which are most vulnerable to being compromised without the proper layers of encryption. Remote networks need to be able to meet sudden and large volumes of teleworkers needing access to networks. User and device authentication for sign-on and guest management is paramount, as is perimeter security. You simply must be able to detect and terminate suspicious activity and malware.

At the very least, passwords into corporate networks should be updated frequently to avoid the danger of hackers getting into your remote workers’ systems. As remote working becomes more ubiquitous, the use of teleconferencing apps such as Skype and Zoom has increased, and during the pandemic the use of these platforms for meetings, webinars, and as a general replacement for in-person communicating skyrocketed. Not surprisingly, hackers found a way to compromise the security of these technologies.

Hackers exploited weaknesses in the Zoom’s platform’s code, allowing access to login information, as well as the ability to install malware, take over the microphone and webcam on some machines, and join a meeting in progress without being invited.

Maintain firewalls with data loss prevention software.

Corporate networks need to be protected by ensuring that any remote attempts to get through are met with a robust defense strategy.
By employing an endpoint protection platform (EPP), which uses several technologies such as antivirus software, data encryption, intrusion prevention, and data loss prevention software, threats can be detected and stopped at the endpoints.

“When the EPP is set up, it can quickly detect malware and other threats, according to a blog from McAfee. “Some solutions also include an Endpoint Detection and Response (EDR) component. EDR capabilities allow for the detection of more advanced threats, such as polymorphic attacks, fileless malware, and zero-day attacks. By employing continuous monitoring, the EDR solution is able to offer better visibility and a variety of response options.”

Account for human error and “rogue” employees.

Not all security risks are electronic in nature. People generally have good intentions, and sometimes make mistakes. They are social beings, and may inadvertently give away important information or trade secrets while chatting with “vendors,” or give away a password to someone pretending to be an IT professional needing access to an account for updating. In addition, occasionally an employee will use a corporate network to transact their own “rogue” business activities.
A network with the proper monitoring software, as well as vigilant IT personnel, can detect telltale signs such as abnormally high traffic from a particular login late at night, for instance, or the transfer of large files overseas.

The IT Team as Educator

Employees working from home need to learn how to protect themselves and their home networks from malicious activity that could affect not only their own personal data, but also that of their employer.
For the most part, many IT professionals enjoy a certain level of autonomy because of their specialty. They usually have contact with workers on technical issues only when they need it, and most times the employee steps aside while IT takes care of tasks such as onboarding, network fixes, software updates, and other problems.

To help make remote working safer, the IT professional is increasingly being asked to step into the role of teacher, to help workers understand and identify online hazards such phishing and malware attacks, and the dangers of inadvertently revealing passwords or other sensitive information. Security experts recommend educating employees on some basic step to avoid compromising business networks.

Avoid public Wi-Fi networks whenever possible.

Companies set up secure VPN networks with several layers of encryptions and password logins for a reason. When accessing networks at a coffee shop or other public place, the same protections cannot be guaranteed. At the very least, employees should always be encouraged to log in to the corporate VPN network to take advantage of firewalls and data encryption.

Keep work data only on work devices.

When working from home, the temptation is to use one's personal home computer or tablet to do work. This can put data at risk, especially if other members of the household use the device. Website access cannot always be restricted, and all it takes is a click on the wrong email to compromise sensitive company data.

> The IT professional is increasingly being asked to step into the role of teacher, to help workers understand and identify online hazards such phishing and malware attacks, and the dangers of inadvertently revealing passwords or other sensitive information.

Remote control is essential.

Make sure that employees know that IT is monitoring data usage, and can take control of their computer at any time. This is essential for periodic software update pushes, as well as the ability to remotely track or delete a laptop should it be lost or stolen.

Be on the lookout for external threats.

Employees clicking on emails from sources they don't know remain one of the most common ways that phishing attackers gain entrance to a network, despite the best efforts to keep them out. Employees must be trained to never open emails from sources they are unfamiliar with. In addition, many more people are using social media, and employees need to be taught how to employ "social distancing" online. They need to be careful not to share corporate data on social media networks and also about the dangers of using unsecured, external storage devices such as USB sticks to store data as they can spread malware and are easily compromised.

Preparing for the Future of Remote Working

The need for a flexible remote workforce will not subside in the future, as employers choose to lower costs and keep their workforces limber and able to work anywhere. Employees will also appreciate the flexibility, and the ability to revolve their workday as much as possible around the rest of their lives.

As a result, IT teams will need to work double time to help their employees continue to stay productive while making sure client information and corporate networks stay operational and safe. In order to do so, it will take a concerted effort to make sure that networks are protected by robust technology while educating workers on how they can help keep information where it belongs.

Many companies embraced early on the digital transformation necessary to ensure a seamless transition to a remote workforce. Those that did not will need to quickly come up to speed in order to stay competitive, especially in a post-COVID world where entire companies may be periodically forced to work in the cloud in the name of public health.

The future of remote work is an exciting one that can offer mobility and flexibility, as well as cost savings and minimal disruption to business when employees cannot be onsite. In order to make that happen, companies must be on board now to adopt IT policies and procedures to manage that transition.