BIZCOMMUNITY

6 ½ considerations for securing the home office

By Perry Hutton

23 Jun 2015

As increasing numbers of employees work from home, organisations often overlook the security needs of remote workers.

Telework predates the BYOD phenomenon by decades. Despite Yahoo!'s move to the contrary, many organisations are shrinking their office spaces and expanding their employees' ability to work from home. Employees value the flexibility and the lack of a commute while employers value lower operating costs and workers working extended hours. Even companies that don't encourage telework specifically frequently have employees working remotely, whether for travel, to accommodate a sick child or simply to save some extra hours of productivity.

Modern home office

Market research firm, Gartner, even confirmed in a June 2014 study that the desktop computer is, in fact, not dead. Of the 40% of respondents who reported using personal devices for work, the most common device was a desktop PC, presumably in a home office. The bottom line for all of this, though, is that organisations need to take the security of their employees' home offices seriously.

goodluz via 123RF

Let's take a step back and think about what actually constitutes a modern home office. For some, it's clearly a space in the home, quite possibly occupied by a desktop computer discarded by the kids in favour of a shiny new i-Device. For others, it might be a desk in the local library or a comfy wing chair at their local coffee house and be accessible to all family. In our exceptionally mobile world, our "home offices" can literally be anywhere that isn't company property.

What this means is that "securing the home office" is really about taking a holistic approach to endpoint security and remote access rather than making sure that employees have something more than WEP securing their wireless routers at home.

Here are some critical best practices for creating secure remote work environments, wherever they might be:

1. Use a VPN

This is a big one. No matter how an employee accesses corporate resources, if done with a correctly implemented VPN tunnel, content moving to and from employee resources is secure. There are even VPNs offered as a service to secure mobile sessions over public WiFi, but building VPNs under corporate control is easy, cost-effective, and ultimately safer than relying on VPNs in the public cloud.

2. Enforce client antivirus installation and updates

Multi-layered approaches to security are critical to ensuring their effectiveness, both within corporate networks and outside of them. At the same time, it can be difficult to ask users to protect themselves or their employers' networks. Running antivirus updates and OS patches tends to fall fairly low on their list of priorities so implementing services that enforce automatic updates on clients outside of corporate networks is a must for remote workers.

3. Prevent the use of consumer cloud storage products

As consumer cloud storage products like Dropbox and Google Drive have become more full-featured and easy to use, it becomes very tempting for users to simply upload work files to the cloud, alongside Grandma's pumpkin pie recipe and pictures from last summer's vacation. Unfortunately, when employees leave a company, there is no way for employers to ensure that corporate assets don't stay on that desktop computer in the ex-employee's home office. Preventing access to these services while employees are on the network provides a layer of protection and control, not to mention regulatory compliance for many industries.

4. Provide platforms that avoid the use of removable media and facilitate secure collaboration

Of course, if users can't upload their files to their personal cloud-based storage account, they'll be tempted to load them onto flash drives or other removable media to access them at home. Well-publicised vulnerabilities on these types of media, though, make this a dangerous prospect. The solution? Provide business-grade tools for secure file sync and share and enterprise collaboration so the temptation of thumb drives and cloud storage are easy to resist.

5. Wherever possible, secure the environment

While it isn't possible to go to every users' home to deploy an access point, and centrally manage them as one can do in a corporate network with optimised security settings, it is possible to require home office users to implement strong encryption on their home routers. Even if that means stepping a user through the setup or offering 4G hotspots at a discount to employees (that use encryption by default), it makes sense to take steps to ensure a relative degree of security on home networks.

6. Security begins with education

Security pros and hackers aren't born with deep security and networking expertise - why should we expect employees to be automatically savvy enough to avoid the latest phishing scheme or a bit of malware?

Unfortunately, that's all too often the mindset for many organisations, the majority of which rely on firewalls, intrusion prevention systems, and antimalware software to protect their networks but ignore the real weak link in the security chain: users. Even large organisations with strong security measures have been brought down by unwitting users who fell for sophisticated social engineering and disclosed login credentials or introduced malware onto the network.

6 ½. Have a policy

This is the "½ a consideration" because it seems as if it should go without saying. But recent research suggests that a lot of organisations have no written policy on personal devices, home offices, or remote access to company networks and assets. Perhaps this should have been #1 - good, well-thought-out policies that both IT and employees can live with is a cornerstone of good security. To implement policy with technology, companies need the underlying policy.

ABOUT PERRY HUTTON

Perry Hutton, regional director of Fortinet for Africa, comes from an accounting background and has spent the last 22 years in IT, the last 10 of which have been in IT security specifically. Contact him at phutton@fortinet.com.

- Security threats of the smart city - 7 Apr 2016
- Security rules for first time cloud users - 15 Feb 2016
- 6 ½ considerations for securing the home office - 23 Jun 2015
- Health-care industry - the next cybercrime target? - 9 Mar 2015
- Securing the new era of big data - 22 Jan 2015

View my profile and articles...