BTS SIO SLAM 1 CYBERSECURITY PRESS ARTICLE

CONTINUITE PEDAGOGIQUE AVRIL 2020

‘Click for urgent coronavirus update’: how working from home may be exposing us to cybercrime

24 mars 2020, 06:12 CET

Author : Craig Valli, Director of ECU Security Research Institute, Edith Cowan University

Apart from the obvious health and economic impacts, the coronavirus also presents a major opportunity for cybercriminals.

As staff across sectors and university students shift to working and studying from home, large organisations are at increased risk of being targeted. With defences down, companies should go the extra mile to protect their business networks and employees at such a precarious time.

Reports suggest hackers are already exploiting remote workers, luring them into online scams masquerading as important information related to the pandemic.

On Friday, the Australian Competition and Consumer Commission’s Scamwatch reported that since January 1 it had received 94 reports of coronavirus-related scams, and this figure could rise.

As COVID-19 causes a spike in telework, teleheath and online education, cybercriminals have fewer hurdles to jump in gaining access to networks.

High-speed access theft

The National Broadband Network’s infrastructure has afforded many Australians access to higher-speed internet, compared with DSL connections. Unfortunately this also gives cybercriminals high-speed access to Australian homes, letting them rapidly extract personal and financial details from victims.

The shift to working from home means many people are using home computers, instead of more secure corporate-supplied devices. This provides criminals relatively easy access to corporate documents, trade secrets and financial information.

Instead of attacking a corporation’s network, which would likely be secured with advanced cybersecurity countermeasures and tracking, they now simply have to locate and attack the employee’s home network. This means less chance of discovery.

Beware cryptolocker attacks

Cryptolocker-based attacks are an advanced cyberattack that can bypass many traditional countermeasures, including antivirus software. This is because they're designed and built by advanced cybercriminals.

Most infections from a cryptolocker virus happen when people open unknown attachments, sent in malicious emails.

In some cases, the attack can be traced to nation state actors. One example is the infamous WannaCry cyberattack, which deployed malware (software designed to cause harm) that encrypted computers in more than 150 countries. The hackers, supposedly from North Korea, demanded cryptocurrency in exchange for unlocking them.

If an employee working from home accidentally activates cryptolocker malware while browsing the internet or reading an email, this could first take out the home network, then spread to the corporate network, and to other attached home networks.

This can happen if their device is connected to the workplace network via a Virtual Private Network (VPN). This makes the home device an extension of the corporate network, and the virus can bypass any advanced barriers the corporate network may have.

If devices are attached to a network that has been infected and not completely cleaned, the contaminant can rapidly spread again and again. In fact, a single device that isn't cleaned properly can cause millions of dollars in damage. This happened during the 2016 Petya and NotPetya malware attack.

Encryption: not a cryptic concept

On the bright side, there are some steps organisations and employees can take to protect their digital assets from opportunistic criminal activity.

Encryption is a key weapon in this fight. This security method protects files and network communications by methodically "scrambling" the contents using an algorithm. The receiving party is given a key to unscramble, or "decrypt", the information.

With remote work booming, encryption should be enabled for files on hard drives and USB sticks that contain sensitive information.

Enabling encryption on a Windows or Apple device is also simple. And don't forget to backup your encryption keys when prompted onto a USB drive, and store them in a safe place such as a locked cabinet, or off site.

VPNs help close the loop

A VPN should be used at all times when connected to WiFi, even at home. This tool helps mask your online activity and location, by routing outgoing and incoming data through a secure "virtual tunnel" between your computer and the VPN server.

Existing WiFi access protocols (WEP, WPA, WPA2) are insecure when being used to transmit sensitive data. Without a VPN, cybercriminals can more easily intercept and retrieve data.

VPN is already functional in Windows and Apple devices. Most reputable antivirus internet protection suites incorporate them.

It's also important that businesses and organisations encourage remote employees to use the best malware and antiviral protections on their home systems, even if this comes at the organisation's expense.

Backup, backup, backup

People often backup their files on a home computer, personal phone or tablet. There is significant risk in doing this with corporate documents and sensitive digital files.

When working from home, sensitive material can be stored in a location unknown to the organisation. This could be a cloud location (such as iCloud, Google Cloud, or Dropbox), or via backup software the user owns or uses. Files stored in these locations may not be protected under Australian laws.

Businesses choosing to save files on the cloud, on an external hard drive or on a home computer need to identify backup regimes that fit the risk profile of their business. Essentially, if you don't allow files to be saved on a computer's hard drive at work, and use the cloud exclusively, the same level of protection should apply when working from home.

Appropriate backups must be observed by all remote workers, along with standard cybersecurity measures such as firewall, encryption, VPN and antivirus software. Only then can we rely on some level of protection at a time when cybercriminals are desperate to profit.

https://theconversation.com/click-for-urgent-coronavirus-update-how-working-from-home-may-be-exposing-us-to-cybercrime-133778

A lire aussi :

https://us.norton.com/internetsecurity-emerging-threats-working-from-home-due-to-coronavirus.html

https://theconversation.com/phishing-scams-are-becoming-ever-more-sophisticated-and-firms-are-struggling-to-keep-up-73934

https://theconversation.com/how-to-avoid-getting-hooked-by-a-festive-season-phishing-scam-52159

https://theconversation.com/working-from-home-risks-online-security-and-privacy-how-to-stay-protected-13459

https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing