Bringing Enterprise Security Home

The May 2021 Colonial Pipeline ransomware attack that crippled fuel delivery for several days in the southeast region of the United States was not the first time US enterprises have been held hostage by criminal hackers—and it will not be the last.[1] A single compromised user opens the door for hackers to wreak havoc on an organization and, in this case, the organization's infrastructure. The assault on the vital Colonial Pipeline operation serves as a reminder that the new era of large-scale home-based employees that began with the onset of the COVID-19 pandemic requires additional strategies to shore up potential security breaches.

A standardized framework to protect nonenterprise home users who work and play in proximity to home-based employees is in its infancy, but secure solutions are available with some planning and forethought. After the pandemic is managed well enough for the economy to fully reopen, what will endure in enterprises across the world is the flexibility to work from home (WFH). Security measures must evolve to meet the demands of this cultural shift.

What Has Changed?

Worldwide, organizations of all sizes face a greater risk of cyberthreats, data theft, and complete operational shutdowns that can result in multimillion-US dollar ransom demands that may or may not restore vital, sensitive enterprise data. Some may say that it is precisely because enterprises pay handsome ransoms to recover their intellectual property or to stop data breaches that cyberattacks are on the rise. If the monetary reward for bad actors who throw wrenches into complex business operations is astronomical, and the risk of being caught and prosecuted is minuscule, cybercrime will undoubtedly continue to rise.

But there are plenty of other reasons cybercrime is on the rise. One facet of these crime sprees that is gaining traction is the ability of hackers to lure unsuspecting family members of enterprise employees working at home into opening fraudulent emails or clicking on dangerous links. All it takes is a spouse or child to pass along infected information to mom or dad, and then what seemed like an airtight computer security system established at the enterprise level flies out the window when family laptops or computers are not fortified with security measures.

Enterprises spend millions of dollars to protect their equipment and employees from sinister ploys. Office software protects computers that employees take home, but the same tools are not being offered to family members. Criminals can easily identify personal information of employees and family members through social media accounts and an array of easily accessible online searches.

An unsuspecting family member whose own computer has not been secured may open a link and innocently send it to the employee who is the real target of the hacker. The circuitous route to a hacker's true target may override otherwise solid protections installed on enterprise computers. Once the scheme is launched on unprotected devices, hijacking computer data poses myriad elements of risk and potential enterprise financial ruin.

Complex Solutions

It is difficult to determine details of specific hacks because corporate administrators are reluctant to reveal any information publicly.[2] Enterprises do not want to give hackers any ideas that might help them stage similar attacks. Resolving cyberattacks is difficult, and solutions depend on the nature of the attack.

Smaller-scale attacks against single users typically are not as attractive to cybercriminals because individuals do not usually have vital data stored locally on their machines, especially with the advent of protective technology. While restoring data after a computer hack of a single user can be a somewhat easy fix mitigated by resetting the user's machine, a laterally moving attack—that is, one that infects one machine and then uses that machine to infect other parts of the enterprise's infrastructure in the same network—is far more damaging.

Recovery from attacks on critical infrastructure systems or data storage systems can take weeks or

PRANAV KUMAR

Is a senior technical account manager with Zscaler. He has 16 years of experience in security with expertise in pre- and post-sales, designing, transition and transformation of security projects. He can be reached at pranav33@gmail.com

months, making this type of thievery profitable for the hacker. Because enterprises cannot afford to be shut down for long periods of time, they tend to pay ransoms just to get back to operational states. The Colonial Pipeline hack is an example of an attack that necessitated payment of a ransom.[3] Hackers were able to break into Colonial Pipeline's system by stealing just one password. Had the enterprise had a zero trust policy in place, any threat or attack would have been substantially reduced, since only a small subset of resources would have been accessible rather than the entire network.

Do Not Click the Link

Phishing schemes are common ploys of the hacker or cybercriminal. A person or entity masquerading as a legitimate organization or source tricks people into opening emails that require personal information. Even technologically savvy people sometimes fall prey to sophisticated phishing schemes because phishing emails often appear legitimate.

Continuing education and reminders of what to do and what not to do with regard to technology safety are a given for employees, but what about family members working alongside employees in a home office? Should the same training not apply to them, considering the risk is so high?

"The same effort that enterprises make to protect technology from cybercrime within brick-and-mortar office buildings should be extended to the home office."

The new WFH world should require enterprises to invest in educating family members about the dangers of fake emails, phishing ploys, scams and other threats posed by hackers intent on finding a roundabout way to infiltrate the computers of enterprise employees working from home. The same effort that enterprises make to protect technology from cybercrime within brick-and-mortar office buildings should be extended to the home office and to all the people living and using technology in that home.

Several strategies for home users can be employed. Organizations can hold educational seminars for entire families, fund online cybersecurity classes or fund classes at local schools or colleges.

Simple rule-of-thumb protocols could also be hammered home on a periodic basis, including using password managers, using two-factor authentication (2FA), avoiding phishing, avoiding insecure websites and avoiding posting personally identifiable information (PII) over social media.

Technology to the Rescue

Virtual private networks (VPNs) offer protected connections for use of public networks, but they are not foolproof. Cloud-based security solutions are another common method to safeguard data. Securing stored data in an Internet cloud is a safety measure that could easily be extended to all home users. Therefore, expanding security policies from the enterprise laptop to the home network is essential. In addition to providing easy-to-understand directions for cloud storage and security best practices, organizations should require employees working at home to double check safety measures installed on all computer systems being used at home by their family members. URL, or content-filtering solutions, allow enterprise administrators to restrict users from accessing websites that have not been approved. These filters also extend to certain web applications. Organizations can deploy security solutions to entire families to protect their networks and safeguard sensitive data.

If an enterprise invested in securing every home device with a cloud-based security solution, it would safeguard noncorporate home users by providing URL filtering, content filtering, advance threat protection, email security and other security features.

Sophisticated enterprise-level security solutions can be installed on all home computers. Zero trust policies developed by IT professionals for enterprise use—designed to provide secure remote access to applications and services—could be extended to all devices used by family members.

Zero trust policies should be taken literally. No one should be trusted to protect an organization's sensitive material. Instead, users must be authenticated and placed within a security bubble or software-defined perimeter.[4] If a home user's computer is compromised, zero trust helps reduce the attack vector of that user. The compromised machine's ability to communicate with other resources on the network, including enterprise laptops, could also be restricted.

Smart home appliances, for instance, are no longer dependent on current or legacy VPNs. However, encouraging employees and family members to access such appliances over typical unencrypted Internet connections increases the risk of eavesdropping attacks. Zero trust policies are just one of many tools in an arsenal of options designed to safeguard vital enterprise information at home.

Technology offers enterprises a wide range of tools to ensure that sensitive data are never accessed by unauthorized users, but if a computer is, nevertheless, breached, the data are at least retrievable, and ransom demands can be ignored. Data loss prevention (DLP) strategies provide assurances that data are never lost or misused. Many enterprises believe home is a safe place, but printing sensitive enterprise data using a home computer is an unsafe practice. Common home computer antivirus programs are generally not powerful enough to block bad actors determined to steal information or hold an enterprise hostage for ransom. Plus, every Internet provider has its own set of security software (bloatware). That is the catch.

Home users, whether they work for the enterprise or not, generally would benefit from an enterprise-level security solution installed on their personal computers. Although organizations cannot enforce such high-level security measures, they can certainly drive home security recommendations on a regular basis.

Help for Family Members

Developing a cybersecurity framework for family members of employees may be a paradigm shift, but the benefits are well worth the cost and time involved to roll out a new policy or program. Secure business networks can circumvent the many tricks cybercriminals employ to infect computers.

> "Cyberattacks on home networks are also more likely to succeed, especially if an employee's family members do not have security software installed on their personal computers and other devices."

Even before any money is spent, there are simple solutions to help family members safeguard information. The importance of creating stronger passwords is a lesson that can be extended to families. Many people use easily breakable passwords and sometimes use the same password for multiple sites. Hackers know this and capitalize on it. Once they have cracked one password, they will use that same password or a variant to access multiple accounts. Organizations should develop policies and protocols for safe password creation, and this information should be shared with family members of employees working from home. It may not be a foolproof solution, but if all family members employ recommended protocols such as using passphrases instead of easily crackable passwords—and organizations implement zero trust policies—the chances of hackers infiltrating a system will be dramatically reduced.

What to Do and What Not to Do

It is a reality that home networks are not as secure as enterprise networks and, therefore, are more vulnerable to an array of cyberthreats. Cyberattacks on home networks are also more likely to succeed, especially if an employee's family members do not have security software installed on their personal computers and other devices.

Because of the easy entry points, educating household members about cybersecurity is paramount in the effort to protect online data. Communicating the following protocols to home-based employees and their families may be helpful:

LOOKING FOR MORE?

- Read *A Holistic Approach to Mitigating Harm From Insider Threats. www.isaca.org/insider-threats*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

"Enterprises have found that it is critical to stop providing unfettered access to the network using traditional VPNs."

- Do not click on any links within an email that look even slightly suspicious.
- Do not install any unknown applications (apps) from untrusted developers on phones or tablets.
- Use a basic (built-in) firewall on modems or routers to prevent any inbound access.
- Do not install any software from untrusted sources.
- Keep all applications on auto-update.
- Limit information-sharing on social media, especially PII. That information can be used to craft a highly specific attack to trick a household member into divulging sensitive information or clicking on a link that might enable the installation of malware.

Enterprises have found that it is critical to stop providing unfettered access to the network using traditional VPNs. Many recent large-scale attacks occurred because hackers were able to gain unauthorized access to an enterprise laptop and use a VPN to access other enterprise machines.

User traffic should be routed through a security stack so that even if a lateral attack stems from a home network, the downloading of malware is prevented by scanning the employee's traffic.[5]

Advanced security techniques such as cloud sandboxing of files can be highly effective defense mechanisms. Cloud sandboxing creates a safe and isolated environment that reproduces an end-user operating environment where code can be run, observed and rated based on activity rather than specific characteristics. By containing network traffic and other data, a sandbox can isolate and stop hidden malware.

Conclusion

The bottom line is that the enterprise landscape shifted globally in the wake of the COVID-19 pandemic, which required people to isolate and work at home to avoid spreading the virus. It turns out that working from home has been rewarding for both employers and employees. Employees are still productive, and commute times have either been reduced or eliminated altogether. Home is the new remote office for the employee.

However, the changes to work environments necessitated by the pandemic have also created some new challenges. The biggest hurdle that enterprises must contend with is providing better security for everyone using home computers and devices in the same workspace as employees. For employees who will continue to work from home after the pandemic, security issues can be addressed in advance to aid the transition to permanently working from home.

Enterprises can capitalize on the emerging market of home-based security for families of employees, but with the paradigm shifts, there will be a learning curve. There will be a trade-off between security and information sharing, but if cybersecurity measures are implemented at the home base, vital information will be safeguarded.

Education, technology and communication with employees and family members working from home may seem like simple strategies to reduce threats and attacks from hackers, but these strategies need to be reenforced as often as possible from all enterprise security teams.

Endnotes

1 Sanger, D. E.; C. Krauss; N. Perlroth; "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," *The New York Times*, 8 May 2021, *https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html*

2 Kastner, E.; "How Can I Create and Secure a Strong Password?" SOS Can Help, 21 April 2020, *https://www.soscanhelp.com/blog/how-to-create-and-secure-a-strong-password*

3 Turton, W.; K. Mehrotra; "Hackers Breached Colonial Pipeline Using Compromised Password," Bloomberg, 4 June 2021, *https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password*

4 Kumar, P.; "Why Zero-Trust Models Should Replace Legacy VPNs," SearchCloudSecurity, *TechTarget*, 23 August 2021, *https://searchcloudsecurity.techtarget.com/post/Why-zero-trust-models-should-replace-legacy-VPNs*

5 *Ibid.*