EQUIPMENT LEASING & FINANCE FOUNDATION
Your Eye on the Future

JOURNAL OF EQUIPMENT LEASE FINANCING

VOLUME 39 • NUMBER 2 • SPRING 2021

Working from Home: A Hacker's Perspective

The best way for companies to defend their remote workers and their organizations is to start thinking like a cybercriminal. Employees are isolated, often with reduced communication about critical business processes. As this article details, any discussion about preventing cyberfraud should address areas of potential weakness as well as remediation options.

Table of Contents

Foundation Home

By Joseph Granneman

The COVID 19 pandemic has impacted our professional and personal lives in many ways. Business models shifted to online services in almost every business niche, or vertical. Retail shopping, grocery delivery, and even religious services moved to online platforms. Businesses quickly shifted their office operations online, with many employees quickly sent home to work remotely using their existing consumer-grade hardware.

There will be some return to the physical workplace for many of these services, once people start to transition to a post-COVID world. However, many employers and employees are not in a rush to return to the office anytime soon. Working from home may be one of the changes the pandemic leaves behind along as part of a new definition of *normal.*

Cybercriminals, having taken notice of the new remote working model, have adapted their techniques to be more effective in this new paradigm. Working remotely increases opportunities for cybercriminals, as many of the defenses available in the office are no longer available otherwise.

Remote employees become more dependent on technology and interconnectivity, which are then targeted by cybercriminals. With employees isolated, communication between staff members about critical business processes is reduced — potentially exposing the opportunity for fraud.

The best way for companies to defend their remote workers and their organizations is to start thinking like a cybercriminal. It is critical to identify not only the potential technical vulnerabilities but also threats from the physical environment and social engineering.

This article will examine some areas of potential weakness and remediation options to kickstart these discussions. This

Critical business processes that involve the transfer of funds also need to be shored up with manual approval and verification processes. Never rely solely on email communications.

article is not intended to be an all-inclusive list. Security teams should conduct their own threat-modeling exercises to identify specific vulnerabilities of their own organization.

SOCIAL ENGINEERING

Phishing is still the most popular form of social engineering and the most common cyberattack. Criminals continue to find success by sending fake email links to malicious websites or fraudulent invoices. Although phishing is a big enough problem for employees working at the office, it can be even more so for those working remotely.

For example, there is a level of distraction when working remotely that reduces the level of diligence that employees must exercise to identify fraudulent messages. Employees are more comfortable working from home and may not be as cautious in this environment as they would have been in the office.

Increased technology usage in the home office creates more targets for phishing remote employees. An organization that allows the employee to "bring your own device" (BYOD) can be especially hazardous. Family members may use the shared family computer for other tasks and get phished through other means such as social networks, instant messengers, and personal email accounts.

The attacker may still gain access to the network through a family member, even if they use a separate computer, and launch an attack against the employee. They could recover the password to the Wi-Fi network from a family member's computer, for example. Many attackers will target family members of company VIPs for this very reason.

Training and Device Management

Training and device management are key to defending remote employees against these types of social-engineering attacks. As the rush to send people home in response to COVID overrode information security concerns, many companies implemented remote-work programs without sufficient training. Employees must be continually reminded and tested on recognizing phishing, including threats that come from non-company-related sources such as social media or personal email.

Critical business processes that involve the transfer of funds also need to be shored up with manual approval and verification processes. Never rely solely on email communications.

BYOD should actually stand for "bring your own data breach": the risk of using personally owned computer systems for business is almost untenable. Organizations should own and manage the personal computer equipment that is used for their business processes. These systems should not be shared with family members or used for any personal business.

Table of Contents
Foundation Home

Home firewalls also allow for insecure practices for other consumer-grade technology. The employee's child may play games on an Xbox that requires inbound network traffic.

Personal smartphones and tablets that can be managed through mobile device management (MDM) tools are the only exceptions. MDM on Windows computers is far less effective while being more intrusive on a personally owned computer. Companies will find that providing a company-owned Windows desktop instead will improve both employee satisfaction and cost savings in the long run.

CONSUMER GRADE TECHNOLOGY

An organization that provides a company-owned computer for its employees working from home has other risks that need to be considered. An often-overlooked risk — one of the most critical — is the consumer-grade technology that comprises the employee home network. For example, enterprise firewalls used by organizations to protect their networks have cutting-edge features and are frequently updated.

By contrast, firewalls used in homes are usually disposable units (under $100) that came from a retail store and run old versions of Linux, with basic inbound traffic blocking and no updates. Home firewalls typically allow all outbound network traffic, whereas enterprise firewalls require specific rules.

Home firewalls also allow for insecure practices for other consumer-grade technology. The employee's child may play games on an Xbox that requires inbound network traffic. Home firewalls support a protocol called Universal Plug and Play (UPnP), which allows the game to initiate opening the inbound firewall ports. This can expose the home network to inbound network traffic that in turn could expose the company-owned computer to potential security risks.

Attackers may also trigger UPnP to add additional inbound rules to the firewall once a computer has been compromised initially. This allows an attacker direct access into a home computer by effectively bypassing the firewall for all remote connections.

Web Content Filtering and Logging

Home firewalls also lack the capability of providing web content filtering and logging. Most organizations utilize some type of web content filter on their network that prevents access not only to objectionable content but also to malicious websites. The company-owned computer on this type of home network may be exposed to web-based malware that would have been prevented in the office. The lack of web-content filtering and logging also means that the organization will not have these logs for use in incident response.

A Shorter Life Span

The life span of home network equipment including firewalls, switches, and wireless routers is far shorter than their business-class counterparts. Most home users

Table of Contents
Foundation Home

Consumer network equipment has another potential security vulnerability in the way it is managed. Many technology companies are linking these devices through cloud-based services to allow for configuration from a smartphone.

purchase their home equipment and never run updates; nor are they even aware of when their equipment is unsupported.

Criminals are scanning the internet repeatedly for flaws in many of these outdated consumer firewalls that allow for full remote administrative control. They can use these compromised devices to attack the home workstations and potentially steal data through network traffic analysis. These old firewalls are commonly used as nodes in distributed denial of service (DDoS) attacks by criminals against other targets.

Consumer network equipment has another potential security vulnerability in the way it is managed. Many technology companies are linking these devices through cloud-based services to allow for configuration from a smartphone.

Multi-Factor Authentication

Remote workers may not set the best passwords for these sites and seldom enable multi-factor authentication (MFA). Attackers can test simple passwords against these services and will undoubtably gain access to many consumer systems. This allows them to grant access through firewalls and to gain access to wireless networks, security cameras, and any other internal network equipment.

At this point, the company-owned computer is now operating on a compromised network and stands little chance of not being compromised itself.

Home networks have become complex environments, with potentially many different systems in operation. Examples are gaming consoles, smartphones, network-attached storage (NAS) appliances, audio equipment, exercise equipment, home automation systems, and security systems.

The compromise of any of these systems could pose threats to the company-owned computer and the employee working from home. For example, the Ring video doorbell system had a vulnerability that was identified in 2018 that allowed access to the Wi-Fi password for the home network.

Vulnerable Network Devices

The Internet of Things (IoT) explosion of consumer devices continues to produce insecure and highly vulnerable network devices. These devices are typically running outdated versions of Linux that are never updated and utilize no security best practices. Data is usually sent unencrypted, including passwords or other authentication tokens.

A lightbulb with a network connection could provide a vulnerability where an attacker gains access to a home network. The attacker can then target internal systems including the company-owned computer.

Securely configuring network equipment is difficult even

Table of Contents
Foundation Home

An attacker can use administrative access to install backdoors to capture keystrokes, dump the contents of memory, and steal files from local storage.

in enterprise environments. Most home users do not have the experience necessary to understand the potential risks of weak security configurations. The home wireless network is a good example: users must select a strong passphrase to secure their networks.

Wireless Passwords

A wireless password needs to be at least eight characters, but it could still be something as simple as the user's last name, their address, or even their phone number. Because most home users are not monitoring their logs, an attacker can simply spray these basic passwords at the remote worker's wireless network until they gain access.

Secure configuration goes beyond just wireless passwords. Many consumer technology platforms require inbound firewall rules. The popular video game Minecraft allows a player to set up their own private server, for example. Parents that configure their firewall to allow their children to host a private Minecraft server may not be aware that this could be used by an attacker to gain access to internal systems. If their children have access to open the connection themselves, the parents may not even be aware of the firewall change.

Password Selection

The selection of passwords for computer systems on the home network is another aspect of secure configuration that can be a vulnerability. Ransomware attacks prey on both weak passwords and weak authentication for administrative accounts. An employee using BYOD will probably utilize a very weak administrative password for their system. The company systems they access could be very secure, but an attacker may be able to compromise the employee computer to steal passwords and gain access.

An attacker can use administrative access to install backdoors to capture keystrokes, dump the contents of memory, and steal files from local storage. These types of compromises can be devastating for the company: it may not even know how passwords from its systems were leaked.

An attacker may not even need to apply brute force to a weak password if they can get the employee to install the backdoor software themself. Home users tend to search for free software utilities to accomplish basic tasks like editing PDF files or drivers for their computer system.

Attackers have modified these utilities and added their own malicious content and placed them on the internet. The modified utilities get indexed by web-search engines and are now presented to the employee as a solution to their problem. Users unwittingly install the backdoor into their system, and

Table of Contents
Foundation Home

The firewall can then utilize a virtual private network (VPN) that connects back through the employee's network so that any traffic is encrypted and cannot be intercepted.

the attacker gains access to any company data, including remote-access passwords.

Home networks need to be bypassed using a corporate VPN or managed by organizations to provide adequate security. The organization can provide a managed firewall and wireless access point to the employee to install on the home network. This segregates the network traffic and prevents other devices from communicating with the company computer systems.

The firewall can then utilize a virtual private network (VPN) that connects back through the employee's network so that any traffic is encrypted and cannot be intercepted. The employee computer can then be fully managed just as if it were in the office on the enterprise network.

In short, the basic convention is to treat the home network as an internet connection — not a trusted network.

REMOTE-ACCESS TECHNOLOGY RISKS

Companies had to quickly increase capacity as workers moved out of the office and back to their homes. This included increasing network bandwidth, upgrading VPN hardware, and adding additional remote desktop and Citrix servers to handle the load. Attackers quickly adapted their tactics as these systems increased the opportunity ("surface area") for password-based attacks.

There may have been a limited number of users who had access to the company VPN before the pandemic. However, the movement of users to their home offices increased the number of username and password combinations that could be tested against these devices. Password-spraying attacks increased dramatically and continue to this day.

Remote access using any type of remote desktop technology like Citrix, Microsoft RDP, or VMware virtual data interface (VDI) are particularly targeted because they provide a desktop on the inside of a network. This allows an attacker to immediately move to targeting internal systems by stealing additional credentials to move laterally through the network.

Because the attacker will be using valid user credentials, these types of compromises are difficult to detect. The motive for these attacks is typically ransomware based, with devastating business impacts.

Dramatic Increase in Vulnerabilities

The number of identified vulnerabilities in remote-access systems increased dramatically in 2020 as attackers adapted to remote working. Vulnerabilities identified in remote-access systems from Cisco, Citrix, F5, SonicWall, and Fortinet could allow an attacker to gain access remotely. All of

Table of Contents
Foundation Home

Organizations can use sender IP reputation filtering to block known attack addresses. They may want to use geographic blocking as well.

these companies responded with software updates to address the issues that had been identified.

Organizations that were not paying attention to these software updates may have been unknowingly compromised. Attackers are still actively scanning the internet for these vulnerabilities, and organizations will see evidence of these attacks in their firewall logs.

Multi-factor authentication should be considered a mandatory requirement for remote access. This will prevent the success of the password-spraying attempts. However, organizations still need to monitor their logs to identify password-spraying attacks and take defensive actions. This could include network rate limiting to slow the attempts.

Organizations can use sender IP reputation filtering to block known attack addresses. They may want to use geographic blocking as well. The important point is to monitor and react to changes in attack vectors rather than simply trust that the technology alone will provide adequate defense.

CONSUMER VPN ISSUES

A growing issue with remote access is the use of consumer virtual private network solutions. These products advertise security and privacy for home users. The problem is that the users do not realize that they just changed who has access to their usage data from their internet service provider (ISP) to their VPN provider.

That can be a problem, because not all VPN providers are equally interested in privacy and security. Remote users are then connecting to company resources through these untrusted networks, thus creating the potential for interception or data leakage. Also, many VPNs offer connections through foreign countries, which could impact organizational compliance as well.

The effectiveness of defending remote-access infrastructure through log activity monitoring is greatly reduced when employees use consumer VPN solutions. The metadata that would help identify the authenticity of a user authentication (like geographic location) is missing. Attackers are aware of this and utilize these consumer VPNs to hide their activity.

The IP addresses used by consumer VPNs are often identified as threats due to the amount of malicious activity conducted over these networks. Information security teams are not able to separate the attackers from legitimate remote-access users.

There is no security benefit gained by using a commercial VPN when connecting remotely to company resources. Organizations should utilize their own VPN solutions and block access from any anonymous

Table of Contents
Foundation Home

The monoculture of most businesses using the same cloud platform allows for economy of scale for attackers. They can target a single technology platform and then target most businesses with a single attack.

source. The listings of these IP sources change frequently and will require a subscription to a threat intelligence or IP reputation feed.

The cultural impact of blocking commercial VPNs can be difficult because of the way VPNs are marketed to consumers. However, this problem can be addressed by focusing on the fact that permitting anonymous access to any company resources is a bad practice.

CLOUD SECURITY ISSUES

The movement to the cloud was well underway before the COVID-19 pandemic. However, the rapid migration to a remote workforce accelerated this movement.

In just a few short years, Microsoft 365 has become the dominant office collaboration suite used by the majority of companies. This has had both positive and negative impacts to information security risk. The monoculture of most businesses using the same cloud platform allows for economy of scale for attackers. They can target a single technology platform and then target most businesses with a single attack.

The volume of data stored in Microsoft 365 makes it a prime target for attackers as well. They can get access to email as well as files through SharePoint and OneDrive. They get access to logs of Microsoft Teams messages and, potentially, phone calls and voicemails.

An administrative account on Microsoft 365 would allow the attacker to modify security settings, including workstation software deployment, through Endpoint Configuration Manager and antivirus settings through Microsoft Defender. The combination of being a one-stop shop for data access, along with the popularity of the platform, makes Microsoft 365 a primary target for attackers.

Microsoft has started implemented multi-factor authentication for new Microsoft 365 accounts as a primary defensive control. Attackers have been using password-spray attacks aggressively against Microsoft 365 accounts in the past year. Surprisingly, Microsoft has not addressed complex passwords in Microsoft 365. It requires only an eight-character password, making multi-factor a mandatory requirement for secure access.

Disabling Older Protocols

A default installation of Microsoft 365 allows attackers to bypass multi-factor authentication by using older email protocols that do not support stronger authentication measures. To prevent these attacks, the older protocols should be disabled during configuration of Microsoft 365.

The primary benefit of using cloud-based collaboration tools is that they easily share data. This is great for companies looking to increase efficiencies, especially when working remotely. It also

Table of Contents
Foundation Home

The overriding design concept for any of these security solutions is to maintain visibility and control into the networks, devices, and cloud solutions used by remote workers. The approach to securing remote workers is to extend the same types of security controls in place on the enterprise network to the home network.

means that it is very easy for an employee to accidentally leak data by inadvertently sharing something as public (for example, within Microsoft 365 or collaboration tools) — or sharing with the wrong individuals.

The default configuration of Microsoft 365 allows wide-open sharing with no regard for security controls. The platform does provide very granular security controls with a variety of options for preventing data leakage including data loss prevention (DLP) tools. Before deploying Microsoft 365, organizations need to review the security capabilities of controls and ensure their appropriate configuration.

CONCLUSION

There is no silver bullet for providing secure remote-access solutions for home-based workers. However, there are a variety of approaches and solutions that can be used to manage the risk to appropriate levels.

The overriding design concept for any of these security solutions is to maintain visibility and control into the networks, devices, and cloud solutions used by remote workers. The approach to securing remote workers is to extend the same types of security controls in place on the enterprise network to the home network.

Organizations that jump too quickly and use consumer-grade technologies that rely on employee configuration are accepting critical risks to their business that could be managed with simple solutions and a plan.

In summary, here are nine recommendations for protecting the organization and its employees:

1. Provide company owned equipment for remote workers where possible
   - computers
   - firewalls and routers
   - Wi-Fi access
2. Utilize strong mobile device management controls for any personal or company-owned devices.
3. Utilize corporate VPN solutions to isolate business traffic from personal traffic.
4. Utilize multi-factor authentication for all websites and remote access.
5. Harden and secure cloud-based productivity systems like Office 365.
6. Monitor security logs from any cloud-based system and onsite remote-access systems.
7. Restrict usage of consumer VPNs that anonymize traffic to company resources.
8. Provide frequent training on social engineering to all employees.
9. Require alternative communications channels for approving financial operations like wire transfers, direct deposit, and vendor payment changes.

Table of Contents
Foundation Home

Joseph Granneman

jgranneman@illumination.io

Joseph Granneman is CEO of illumination.io in Cherry Valley, Illinois. He founded the cybersecurity company in 2013 following more than 20 years of experience as an executive IT leader in healthcare and financial trading institutions. He is an expert in penetration testing in the banking, manufacturing, and healthcare vertical markets; incident response; and forensic analysis as well as regulatory compliance with HIPAA, PCI, and NIST security frameworks. He has worked closely with the FBI and Secret Service on behalf of his clients who have been victims of cybercrime. Mr. Granneman has written articles for Information Security and CIO/CSO magazine and publishes online with TechTarget at http://searchsecurity.techtarget.com. He is an adjunct professor of IT strategy for the MBA program at Northern Illinois University's College of Business in De Kalb, where he also received an MBA in 2011. He is involved in developing as proposal for secure healthcare data exchange for the state of Illinois. In addition, he helped develop security standards for emergency medical responders as part of serving on the Certification Commission for Health Information Technology Security Working Group. Mr. Granneman received a BS from Millikin University, Decatur, Illinois, in 1993 and also holds the CISSP (certified information systems security professional) credential. His last article for this journal was "The Business Guide to Improving Information Security," in the Fall 2018 issue (vol. 36, no. 3).

Table of Contents

Foundation Home