April
2020

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

THE COVID-19 CHECKLIST

Detailed Steps to Better Protect Your Organization

A COLLABORATION BETWEEN

MICRO FOCUS® Government Solutions

ICIT SOLUTION INSIGHTS

ICIT would like to thank the following experts for their contributions to this report:

Parham Eftekhari
EXECUTIVE DIRECTOR, ICIT

Kevin Hansen
CHIEF TECHNOLOGIST, MICRO FOCUS GOVERNMENT SOLUTIONS

Drew Spaniel
LEAD RESEARCHER, ICIT

David Wray
CHIEF TECHNOLOGY OFFICER, MICRO FOCUS GOVERNMENT SOLUTIONS

ABOUT ICIT SOLUTION INSIGHTS

ICIT Solution Insights offers use case based education on technology products and how they address problems facing our nation's critical infrastructure sectors. These reports are designed to help our community navigate the crowded vendor ecosystem with trusted knowledge from ICIT.

ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

ICIT SOLUTION INSIGHTS

Just because we are in the midst of a global pandemic does not mean we get a reprieve from cyber threats. Reports of COVID-19 related incidents show that many adversaries appear emboldened by the ongoing chaos and aim to compromise sensitive networks and systems while the workforce is adapting to the turmoil. For instance, a malicious coronavirus tracker was found to be spreading malware[1], the FBI has reported phishing campaigns with COVID-19 themed lures[2], and the Department of Health and Human Services (HHS) experienced DDoS attempts from multiple sources[3].

Regardless of how long this current pandemic lasts, the age of mass teleworking is here[4], [5]. Adversaries are aware of the challenges that telework has introduced into the security landscape and they are leveraging the dynamics of the ongoing crisis to exploit corporate systems that may not have been adequately secured or prepared for the telework migration. Below are some nontechnical and technical steps that will improve your security posture.

Step 1: Triage and Update Existing Security Policies and Procedures

1. REDUCE THE RISK OF INSIDER THREATS

Telework introduces opportunities for remote workers to become non-malicious, unintentional insider threats. In the corporate environment, insider threats are mitigated via "see something, say something" policies, physical security, and employee monitoring. In telework spaces, the paradigm is almost reversed. Some specific mitigation recommendations include:

a. **Ensure that confidential discussions do not occur near IoT devices, such as NEST, Alexa, or Siri, that could be digitally weaponized into monitoring devices.**

b. **Work devices, whether bring-your-own-device (BYOD) or corporate issued, should only be used in a designated work environment and should not be shared with family members, even during off-work hours.**

c. **Personal devices used for work, routers, work-related applications, and employee accounts should be secured with complex credentials that are unique and not saved in browsers or unapproved password managers.**

d. **User accounts should be separate from admin accounts and the latter should only be used when authorized.**

e. **Auto-play functionality should be disabled to prevent infection through malicious, remote media.**

f. **Employees should only use applications approved by the corporate security policy. Applications such as hardened or safe browsers that block cookies and exploitable plug-ins should be specified by the security policy or approved by the information security team.**

2. SECURE WI-FI CONNECTIONS

Most staff precariously operate their home WiFi on the settings and credentials that came preinstalled on the device, often directly issued by a telecom company. While convenient to the average end user, since the device installation is essentially plug and play, digital attackers can easily breach these routers, infecting connected computers with malware, which will laterally move onto corporate networks.

Organizations should instruct staff to reconfigure their router settings to accomplish the following:

a. **Avoid broadcasting their service set identifier (SSID) and to feature WPA-2 security**

b. **If operating on wireless, staff may be more secure if the computers designated for work are isolated on a GUEST account instead of the network their family utilizes daily.**

c. **Instruct employees that devices connecting to corporate networks and assets should never be connected to public or shared WiFi.**

3. ESTABLISH CLEAR AND CONSISTENT COMMUNICATION

Communication is one of the most significant challenges in information security. If personnel do not know what tools to use, how to use them, or how to create good cyber-hygiene habits, then the entire security strategy fails. The challenge of proactively inciting security-conscious behavior may be exponentially more difficult in the current telework environment, especially when personnel also have to worry about mitigating COVID-19, social distancing, and caring for their families.

CISOs and CIOs should quickly develop and communicate telework cybersecurity and cyber-hygiene policies and procedures, working with human resources and other business leaders to ensure communication is effective and reaches every employee. It is imperative to explain what applications are in use and why they are used. Every device which connects to your network should have properly installed applications which are set to automatically update. Avoid the temptation to let employees decide what platform to use for their daily tasks, instead providing clear instructions that keep everyone safe.

4. RESTRICT TRANSMISSION OF ORGANIZATION DATA

If an adversary laterally compromises the corporate network while the workforce is remote, they may establish a foothold and remain on the network until well after the COVID-19 crisis has subsided. While teleworking, secure communication clients, like video conferencing, emails, and messaging systems. Additionally, file transfer and cloud platforms should be approved by the information security team and used uniformly throughout the workforce. Many secure applications offer a business-exclusive product line designed to support a remote workforce. Though it may seem an unnecessary expenditure in a time of economic downturn, the future security of an organization can be better ensured by relying on a business product line instead of a "free" or trial offering.

5. UPDATE SECURITY POLICIES

As more and more staff start working from home, it is important for businesses to update and patch their remotely accessible and mission critical systems. After all, if an incident occurs during the ongoing pandemic, staff are unlikely to be on site to mitigate and remediate the threat. Though most of the workforce will use BYOD systems, staff should be instructed on how to update and secure personal systems. Any corporate-owned systems should likewise be updated and secured. For guidance on how to secure systems for remote access and how to craft a telework security policy, consider the National Institute of Standards and Technology: User's Guide to Telework and BYOD Security[6], the Center for Internet Security: CIS Controls Telework and Small Office Network Security Guide[7], and the FTC Online Security Tips for Working From Home[8][9].

6. PROVIDE TELEWORK SUPPORT

Not all staff will transition to teleworking well. A responsive and proactive support hotline or help desk is essential to ensuring that personnel understand the new security policies, comply with the control mechanisms, and practice cyber hygiene. Do not trust nontechnical people to perform technical tasks. In lieu of adequate support, productivity will decline and security will be jeopardized as staff implement workarounds or ignore best practices out of frustration or confusion.

In addition to dedicated support contacts, a clearly communicated security policy should specify which secure applications can be relied upon and for what purposes. Remote staff should not be modifying settings, relying on unapproved software, or disabling necessary controls. A dedicated support staff should manage applications and system configurations as needed.

7. EDUCATE ON THE RISK OF PHISHING SCAMS

The FBI's Internet Crime Complaint Center has already issued warnings of phishing scams that target teleworkers by promising stimulus checks, fake CDC information, a COVID-19 tracking map, or vaccination information[2]. These lures were designed to appeal to a wide swath of potential victims in the hopes that a few recipients would unintentionally infect their telework systems. The attacker could then sell access or laterally compromise the enterprise's network. They are attacks of opportunity, and they succeed if even one employee fails to practice proper cyber hygiene.

If an employee succumbs to a phishing lure, but was not trained or equipped to mitigate the threat, is the employee or the company more to blame? With the passage of time, phishing lures are becoming more sophisticated and targeted. As the risk to organizations drastically increases, companies must take responsibility for training employees to recognize phishing attempts. To laterally compromise the corporate network, an attacker only needs one employee to succumb to one phishing attempt.

Organizations should adopt a zero-trust culture to mitigate phishing attempts. Any attempts to share confidential information, access critical systems, or transfer funds should be confirmed over a phone or a video call, as emails, texts, and messages can be easily spoofed. Whether using a personal or company-issued device for work, personnel should avoid social media, personal email accounts, unsecured messaging clients, and untrusted webpages.

If adversarial activity is detected, staff should know how to report the suspect emails or communications to the information security team so they can warn the entire workforce.

8. SECURE PHYSICAL WORKSPACES

Working from home can be a difficult transition even in the best of times. For the sake of productivity and security, it is recommended that teleworkers establish a fixed and physically secure work environment that precludes distractions and temptations to deviate from the traditional workflow.

Though it may not seem pertinent now, once the COVID-19 crisis passes, physical security will be significant. Employees accustomed to telework may choose to remain remote. After social distancing ends, these telework converts might be tempted to work from cafés or other public environments. The physical security lessons employees learn now will establish the foundations for their telework security in the future. No company can say for certain how the workforce is going to evolve from this crisis; it behooves them to establish best practices now, so that all scenarios are accounted for in the future.

Step 2: Plan for the Future

1. IMPLEMENT AND REQUIRE A VIRTUAL PRIVATE NETWORK (VPN)

Companies should require a VPN to access the office network and resources. Think of a VPN like the drawbridge leading into your corporate castle. It restricts traffic to only authenticated parties, thus limiting the vectors an adversary can exploit to attack the network. If left untested, mismanaged, or inadequate, it can also be the single point of failure for an otherwise secure organization. Now, more than ever, these applications should be tested and supported by a firewall and associated infrastructure to ensure they can handle the inbound telework traffic.

Professional IT operations and network monitoring tools, such as Micro Focus' Network Operations Management (NOM) Suite[10], can help organizations increase teleworkers' access to applications and networks without compromising security or disrupting business operations. For telework in particular, NOM can analyze, model, and monitor VPN capacity and scalability. Meanwhile, tools like Micro Focus' LoadRunner[11] can help measure system behavior and performance under the increased telework traffic load. LoadRunner can be used to test the performance and scalability of websites, portals, and other applications to ensure that both networks and applications are reliable given the dramatic increase in load.

2. PROTECT ENDPOINTS

Every device connected to the corporate network or used to communicate Every device connected to the corporate network, or used to communicate with work accounts, is an endpoint. More simply, any device used for work should be treated as a work device. Opening the network to unmanaged devices is tempting fate. The network will be breached and the cost of that impact will be greater than mitigating the risk. Telework devices should be managed to enforce the same security configuration and governing policies as any other corporate device. Unified endpoint management solutions, such as Micro Focus' ZENworks Endpoint Security Management[12] product, are location-aware, policy-based solutions that can protect the data on computers, control how endpoints communicate and access information, and monitor and maintain the health of endpoint devices.

3. SECURE APPLICATIONS

Attackers are looking for vulnerabilities they can exploit to infect a network. A successful campaign only needs to trick one user or compromise one application for an adversary to plant malware or establish a backdoor in a mission critical system. While all systems should be updated and patched and all users should be adhering to cyber-hygiene practices, the threat landscape is frustratingly dynamic. Application scanning and monitoring tools, like Micro Focus' Fortify Static and Dynamic Application Security Testing Offerings[13], help ensure that the applications you rely on are not jeopardizing your security or sensitive data. This is particularly true for public network facing applications and applications now being accessed remotely.

4. CONSIDER VIRTUALIZATION

If managing personal devices and securing the applications used by remote employees seems daunting, consider relying on virtual desktops, application virtualization, or thin clients. Virtualized applications and systems decrease the technical, cost, and logistical impediments to securing telework access while simultaneously providing remote users quick access to the business applications and processes they need for their jobs. For example, Micro Focus' ZENworks Desktop Containers[14] do this for Microsoft Windows based applications, while their Host Access for Cloud product[15] provides virtualized applications for mainframe, terminal, and green-screen applications.

5. ENFORCE MULTIFACTOR AUTHENTICATION

Multifactor authentication (MFA) is critical to telework and should be applied to all users and applications that want to access sensitive information within the work environment. Credentials alone are wholly insufficient to establish trust, but some mechanisms, such as hardware tokens, may prove burdensome to some workforces. Solutions such as Micro Focus Advanced Authentication[16] can help measure risk and establish the MFA solution that will seamlessly secure the organization without disrupting workflow.

6. ENCRYPT SENSITIVE DATA WHILE IN STORAGE, PROCESSING, AND TRANSIT

Work devices and their associated data should be encrypted to prevent digital exfiltration or compromise via physical theft. However, disk encryption is no longer sufficient protection against attackers or efficient when users expect to quickly read or write data. Micro Focus' Voltage[17] product line can secure sensitive data by leveraging format-preserving encryption of both data-at-rest and data-in-motion, securing it for the entire data lifecycle. This renders any stolen data useless in the hands of attackers and does not waste limited resources on encrypting everything, including nonsensitive data.

7. MONITOR USER BEHAVIOR

Security information and event management systems with user and entity behavior analytics capabilities, such as Micro Focus ArcSight[18] and Interset[19] products, enable information security personnel to see, in real-time, anomalous activity occurring on the network between users, applications, and data, including remote users and devices. These features are critical in the fight to rapidly detect and mitigate remote digital adversaries and are paramount when securing a company with remote workers. They prevent attackers from masquerading as trusted users, flag anomalous behaviors, and help mitigate malicious exfiltration attempts by triggering counterattack measures.

Invest Now in Solutions to Defend our Future

Only time will tell how long the COVID-19 crisis will last or what paradigm shifts it will inspire. Nevertheless, future business operations will inevitably feature more telework elements.

Before the crisis, only 7% of civilian workers in the US, or roughly 9.8 million of the nation's approximately 140 million civilian workers, worked remotely[20]. Now, the white-collar workforce has witnessed the feasibility of telework and has begun adapting to it. Exact metrics are scarce, but it is reasonable to assume that, as the crisis continues, every job capable of telework will undergo some transition. Implementing best practices and investing in reliable solutions could prove foundational for the future of any organization that wants to acquire and retain talent as well as reap the economic benefits of a remote workforce.

In the public sector alone, one organization estimates that 43% of the federal workforce is eligible to telework and that doing so during the COVID-19 pandemic will save $570 million a day. Kate Lister of Global Workplace Analytics estimates that" if federal workers who both can and want to work remotely did so just half of the time, the government could save up to $4B a year"[21].

The COVID-19 epidemic has devastated the US economy, and it is unclear what effect the federal stimulus will have or how long the economy will take to recover. Adopting reliable solutions that empower secure telework, such as those offered by Micro Focus, would enable organizations to recover faster by reducing operational costs. Furthermore, these organizations would be better equipped to acquire and retain new talent, offering an improved work/life balance to their entire staff. Investing in secure telework solutions now mitigates breaches, reduces overhead, and establishes a competitive advantage for the future.

The COVID-19 crisis will pass, but it will not be the last pandemic or disaster. This is a defining moment in history and the shape of our workforce will change as a result. With the global economy in flux, organizations should invest in any competitive advantage they can, establishing secure telework policies and adopting trusted solutions from reliable vendors. This will help businesses recover faster from this crisis and be prepared for any future workforce turbulence.

About this ICIT fellow program member

MICRO FOCUS Government Solutions

Micro Focus Government Solutions helps protect, run, and transform US Public Sector agencies. Driven by customer-centric innovation, our software provides the critical tools needed to build, operate, secure, and analyze the enterprise. By design, these tools bridge the gap between existing and emerging technologies–which means you can innovate faster, with less risk.

15 Our software products are in use by all 15 Federal Departments

40k Globally, 40,000 companies use our solutions

50 We operate in 50 US states

98/100 We help 98 of the 100 largest companies in the world

Micro Focus Government Solutions is a proud ICIT Fellow Program Member. Micro Focus supports their research by providing subject matter expertise and core research teams, engaging on key legislative topics around cybersecurity.

CERTIFICATIONS & COMPLIANCE

We strive to comply with alignment with FISMA, NIST RMF, ISO, SOC 2 and other standards & controls across our portfolio

SOLUTIONS EXPERTISE

Our products span:
DevSecOps
Hybrid IT
Predictive Analytics
Security, Risk, and Governance

OUR MARKET SPACE

Analytics & Big Data
Application Delivery Management
Application Modernization & Connectivity
Business Continuity
Collaboration
Information Management & Governance
IT Operations Management
Security

CUSTOMERS

Department of Defense
Energy and Utilities
Federal Civilian Agencies
Financial and Citizen Services
Healthcare Agencies and Services
Higher Education
Homeland Security
State and Local Government

To learn more, contact GovCovidResponse@microfocus.com

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

MICRO FOCUS Government Solutions

ICIT SOLUTION INSIGHTS

Sources

[1] T. Brewster, "Coronavirus Scam Alert: COVID-19 Map Malware Can Spy On You Through Your Android Microphone And Camera", *Forbes*, 2020. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/#7218ca4475fd. [Accessed: 27- Mar- 2020].

[2] "Internet Crime Complaint Center (IC3) | FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic", *Ic3.gov*, 2020. [Online]. Available: https://www.ic3.gov/media/2020/200320.aspx. [Accessed: 27- Mar- 2020].

[3] J. Dunn, "DDoS attack on US Health agency part of coordinated campaign", *Naked Security*, 2020. [Online]. Available: https://nakedsecurity.sophos.com/2020/03/18/ddos-attack-on-us-health-agency-part-of-coordinated-campaign/. [Accessed: 27- Mar- 2020].

[4] L. Kyzer, "Telework Should Be an Option for Some Workers With Security Clearances", *Government Executive*, 2020. [Online]. Available: https://www.govexec.com/workforce/2020/03/telework-should-be-option-some-workers-security-clearances/164069/. [Accessed: 27- Mar- 2020].

[5]B. Fung and A. Marquardt, "Millions of Americans are suddenly working from home. That's a huge security risk", CNN, 2020. [Online]. Available: https://www.cnn.com/2020/03/20/tech/telework-security/index.html. [Accessed: 27- Mar- 2020].

[6] M. Souppaya and K. Scarfone, "User's Guide to Telework and Bring Your Own Device (BYOD) Security", NIST, 2020. [Online]. Available: https://www.nist.gov/publications/users-guide-telework-and-bring-your-own-device-byod-security. [Accessed: 27- Mar- 2020].

[7] "CIS Controls Telework and Small Office Network Security Guide", *CIS*, 2020. [Online]. Available: https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide. [Accessed: 27- Mar- 2020].

[8]"Online security tips for working from home", *Consumer Information*, 2020. [Online]. Available: https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home. [Accessed: 27- Mar- 2020].

[9]A. Fein et. al., "COVID-19 Cybersecurity Advice: FTC, NIST, and CISA Release Guidance on Secure Teleworking and Critical Infrastructure Jobs | Inside Privacy", *Inside Privacy*, 2020. [Online]. Available: https://www.insideprivacy.com/covid-19/covid-19-cybersecurity-advice-ftc-nist-and-cisa-release-guidance-on-secure-teleworking-and-critical-infrastructure-jobs/. [Accessed: 27- Mar- 2020].

[10] "Enterprise Network Management Software | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/network-operations-management-suite/overview. [Accessed: 27- Mar- 2020].

[11] "LoadRunner Professional - Application Load Testing Software | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/loadrunner-professional/overview. [Accessed: 27- Mar- 2020].

[12] "ZENworks Suite | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/zenworks/. [Accessed: 27- Mar- 2020].

[13] "Fortify Application Security Testing | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/solutions/application-security. [Accessed: 27- Mar- 2020].

[14] "Desktop Containers | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/desktop-containers/. [Accessed: 27- Mar- 2020].

[15] "Host Access for the Cloud | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/host-access-cloud/overview. [Accessed: 27- Mar- 2020].

[16] "NetIQ Advanced Authentication | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/netiq-advanced-authentication/overview. [Accessed: 27- Mar- 2020].

[17] "Voltage SmartCipher: Unstructured data security & file encryption | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/voltage-smartcipher/overview. [Accessed: 27- Mar- 2020].

[18] "ArcSight Security Information and Event Management: SIEM Software | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview. [Accessed: 27- Mar- 2020].

[19] "Interset UEBA Insider Threat Detection | Micro Focus", *Micro Focus*, 2020. [Online]. Available: https://www.microfocus.com/en-us/products/interset-ueba/overview. [Accessed: 27- Mar- 2020].

[20]"News Releases – Global Workplace Analytics", Globalworkplaceanalytics.com, 2020. [Online]. Available: https://globalworkplaceanalytics.com/brags/news-releases. [Accessed: 27- Mar- 2020].

[21] D. Desilver, "News Releases â€" Global Workplace Analytics", *Globalworkplaceanalytics.com*, 2020. [Online]. Available: https://globalworkplaceanalytics.com/brags/news-releases. [Accessed: 27- Mar- 2020].