protiviti®
Face the Future with Confidence

Work from Home Cybersecurity Practices

The following overview provides guidance for organizations to consider when enforcing new and existing security measures for remote workforces and broader enterprise security programs during this accelerated work from home (WFH) transition. The security actions and activities noted below depict items that should be addressed at both the personal and an enterprise level due to some of the limitations presented in the transition to working remotely.

Personal Cyber Practices

Activities that people working from home need to be aware of and implement daily:

- Spearphishing and phishing vigilance
  - Coronavirus/COVID-19 related campaigns
  - Password resets
  - Unanticipated attachments
  - Social media activities (e.g., LinkedIn connection requests)
- Complete enterprise phishing awareness and WFH security trainings
- Update and maintain security levels of home networking equipment
- Send all sensitive company data via secure, encrypted file solutions (e.g., ShareFile, Microsoft Teams, etc.) and not via personal email
- Keep others off work device (lock screen)
- If home device is only option:
  - Disable browser password caching
  - Install all patches
  - Obtain antivirus, personal firewall and general internet protection software
  - Update browser to latest version
  - Avoid downloading work related files to local hard drive
    - Leverage software to securely delete locally stored files
- Limit printing of all company confidential data if shredder is not available

Enterprise Cyber Practices

Activities and controls organizations need to consider and extend enterprise wide:

- General practices
  - Distribute a general WiFi security checklist for common consumer wireless router brands
  - Distribute WFH security considerations and requirements checklist (see personal cyber practices, left) and require employees to review and acknowledge (i.e., signoff)
  - Increase communication across the employee base
    - "How do I" series to WFH security tips and tricks
    - Phishing reminders
    - Ensure employees have a path to provide real-time feedback and questions on all fronts

Work From Home Cybersecurity Practices

Enterprise Cyber Practices (continued)

Network

- Review bandwidth and stress limits for mission critical technologies (I.e., VPN, VDE, collaboration tools, etc.)
- Ensure VPN access is available and (if possible) only allow registered devices
- Ensure VPN is fully patched and properly configured
- Ensure only authorized individuals can access the VPN
- Enforce multi-factor authentication (MFA) for all remote points of connection to the enterprise network and environment (also block legacy authentication protocols that bypass MFA)
- Review and continuously update spam filters to include recent threats
- Review and continuously update web filtering/proxy configurations to limit browsing to essential business activities
- Deploy network data loss prevention (DLP) software and ensure configuration/signature are up-to-date

Endpoint

- Deploy endpoint firewall software to limit local network visibility and protect against threats from the internet
- Deploy antivirus/malware detection and prevention software and ensure configuration/signatures are up-to-date
- Deploy endpoint detection and response (EDR) software and ensure configuration/signatures are up-to-date
- Deploy endpoint data loss prevention (DLP) software and ensure configuration/signature are up-to-date
- Enable device/data backup
- Enable device (hardware) encryption

Collaboration Solutions

- Review and enable security best practices for all collaboration platforms (i.e., email, chat, video conferencing, file share, etc.)
- Ensure only authorized individuals can access
- Ensure file sharing can take place in a secure manner and distribute secure file sharing practices
- Enable data loss prevention controls (if available)
- Require password protection for video conferencing
- If possible, consider a one-time push to update critical patches across all devices

Security Operations

- Focus security monitoring and operations on newly designated mission critical assets that enable WFH.
- Review incident response plans to ensure they are adoptable to WFH scenarios.
- Disseminate the security event reporting procedures to employees and contractors.
- Consider temporarily relaxing password change requirements to reduce Support Desk stress

Other Considerations

- Partner with procurement to ensure newly purchased hardware is inventoried into assess management tracking systems and properly configured and secured prior to distribution to employees.
- Create a process to collect and inventory all newly deployed hardware prior to employees returning to corporate office
- Leverage retired hardware if new systems cannot be obtained
- Utilize cellular hotspots for employees that do not have internet access
- Keep overall IT/cyber decision making to a small and agile group (promotes collaboration, speed, avoids “red tape”)
- Implement a code freeze across all systems until stability has been reached
- Be ready to answer questions from executives and Board members about new business risks created by WFH, what steps have been taken to reduce said risk and how operational excellence/focus can be maintained in the interim

Protiviti.com/TechnologyConsulting

TechnologyConsulting@Protiviti.com

TCblog.Protiviti.com