CYBERSECURITY ADVISORY

Enterprise VPN Security

Last Revised: April 15, 2020 **Alert Code:** AA20-073A

Summary

As organizations prepare for possible impacts of Coronavirus Disease 2019 (COVID-19), many may consider alternate workplace options for their employees. Remote work options—or telework—require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology (IT) network. As organizations elect to implement telework, the Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to adopt a heightened state of cybersecurity.

Technical Details

The following are cybersecurity considerations regarding telework.

- As organizations use VPNs for telework, more vulnerabilities are being found and targeted by malicious cyber actors.
- As VPNs are 24/7, organizations are less likely to keep them updated with the latest security updates and patches.
- Malicious cyber actors may increase phishing emails targeting teleworkers to steal their usernames and passwords.
- Organizations that do not use multi-factor authentication (MFA) for remote access are more susceptible to phishing attacks.
- Organizations may have a limited number of VPN connections, after which point no other employee can telework. With decreased availability, critical business operations may suffer, including IT security personnel's ability to perform cybersecurity tasks.

Mitigations

CISA encourages organizations to review the following recommendations when considering alternate workplace options.

- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations. See CISA Tips Understanding Patches <https://www.us-cert.gov/ncas/tips/st04-006> and Securing Network Infrastructure Devices <https://www.us-cert.gov/ncas/tips/st18-001>.
- Alert employees to an expected increase in phishing attempts. See CISA Tip Avoiding Social Engineering and Phishing Attacks <https://www.us-cert.gov/ncas/tips/st04-014>.
- Ensure IT security personnel are prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery. Per the National Institute of Standards and Technology (NIST) Special Publication 800-46 v.2, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>, these tasks should be documented in the configuration management policy.
- Implement MFA on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords. (See CISA Tips Choosing and Protecting Passwords <https://www.us-cert.gov/ncas/tips/st04-002> and Supplementing Passwords <https://www.us-cert.gov/ncas/tips/st05-012> for more information.)

- Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications—such as rate limiting—to prioritize users that will require higher bandwidths.
- Contact CISA <https://www.us-cert.gov/report> to report incidents, phishing, malware, and other cybersecurity concerns.

References

NIST Special Publication 800-46 v.2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security <https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final>

CISA Cyber Essentials <https://www.cisa.gov/cyber-essentials>

CERT/CC: VPN - A Gateway for Vulnerabilities <https://insights.sei.cmu.edu/cert/2019/11/vpn---a-gateway-for-vulnerabilities.html>

National Security Agency Cybersecurity Advisory: Mitigating Recent VPN Vulnerabilities <https://media.defense.gov/2019/oct/07/2002191601/-1/-1/0/csa-mitigating-recent-vpn-vulnerabilities.pdf>

CISA Insights: Risk Management for Novel Coronavirus (COVID-19) <https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf>

Telework.gov Guidance <https://www.telework.gov/guidance-legislation/telework-guidance/security-it/>

Revisions

March 13, 2020: Initial Version

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

Give Feedback

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>