Work-At-Home and Remote Access – It's Time for a Security Review

By Jeffrey R. Wells, David G. Ries / May 19, 2020

As shut down and stay/shelter-at-home orders and guidance took effect in response to the COVID-19 pandemic, businesses and organizations of all sizes faced challenges in providing and supporting technology for working at home and remote access. Some companies had to start from scratch; others had to scale up existing capabilities. For some, security took a back seat to get the technology up and running. For others, while security was addressed, it was in the context of rapidly evolving remote work conditions and increasing demands and capacity in the face of the pandemic.

As companies and employees have now settled into work-at-home routines and there's a movement toward partial reopening, this is an excellent time to step back and review security controls and practices, document any changes or improvements to processes, procedures, and adoption of new or additional technologies.

Government agencies and security organizations have recently provided updated standards and guidance to address these remote work challenges. Examples include the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute for Science and Technology (NIST), the National Security Agency (NSA), the Center for Internet Security (CIS), and the SANS Institute. There's much valuable information to be found at each site. It's best to review these resources, select one or more that best fit a company's circumstances, and use it or them in the security review process.

Security for remote work should be part of a risk-based, comprehensive cybersecurity program. Risks from constantly evolving remote work, remote access, and collaboration technology should be included in the process of improving or developing an inclusive program. As with other areas of security, safeguarding of remote working should be appropriately scaled to the size and complexity of the business, increased levels of demand on the business' technological capacity and the sensitivity of the information.

Some important considerations include:

- Security, physical and digital, of the laptop, desktop or tablet used by the remote worker,
- Special attention to securing worker-owned, bring your own device (BYOD) access to the company network,
- Network security guidance for wired and wireless networks for the remote user,
- A Virtual Private Network (VPN) or other secure connection, securely configured, between the remote device and the company network,
- Strong authentication, including multifactor authentication, for access to the company network, applications, and services,
- Automatic log-off after 15 minutes (or less) of inactivity,
- Segmentation of the company network, to limit access to resources necessary for the remote worker,
- Analysis of the increasing needs of the business regarding remote working and impact on the configuration and capacity of the network,
- Use of data loss prevention (DLP) tools,
- Logging of remote connections and activity by remote users and log retention,
- Use of secure collaboration and conferencing services, securely configured,
- Ensure current and correct operating systems and security patches are installed,
- Include remote users in backup, business continuity and incident response plans,
- Training in remote work security, including protection against phishing and social engineering, and
- An efficient and scalable process for answering user questions and reporting incidents.

Now is an appropriate time for businesses and organizations to review the risks presented by their current remote work environments and address the risks by updates to their cybersecurity programs and, if and as needed, increasing capacity and service levels of hardware and software used. Periodic reviews and updates and training will be essential parts of the process.