FS-ISAC

Work From Home Security Tips for Institutions

Introduction

As a result of COVID-19, many organizations are now a few weeks or even months into a wholesale shift in their business operations to a virtual model. Doing this successfully requires new technology and security considerations to be embedded into operations.

On 12 March 2020, FS-ISAC, along with the ABA and SIFMA, conducted a webinar for thousands of members on best practices for this new way of doing business. We believe many organizations will find value in this guidance and so have summarized some key tips below.

Technology

- Embed technology and security representatives in the various planning groups to ensure proper consideration of the technical aspects of a wide scale work from home (WFH) scenario and the security considerations that come along with working from home.
- Overcommunicate with personnel. Make sure how-to documents and FAQs about WFH are readily available. Widely re-share IT, Security, and HR contacts.
- Remind personnel what technology and services are allowed, as they will be working hard to get their jobs done in a new model that they may not be comfortable with, and you don't want to end up with any unsanctioned services happening in your environment. Reiterate how to share documents and collaborate on information while working remotely. For example, if you're utilizing Office 365, remind employees to use Teams, SharePoint and OneDrive to share documents and collaborate. Ensure that employees are not trying to use services such as Google Drive or Dropbox if those are not allowed. Explicitly block unsanctioned services.
- Plan for last mile/home internet connectivity limitations which may be based on physical location or impacted by an increase of family and neighbors online.
- Monitor performance, consumption and load – this applies to both internal technologies such as VPN as well as critical business tools such as collaboration and communication platforms (O365, Google Suite, Zoom, WebEx) and carriers (Verizon, AT&T, Orange, Vodafone, etc.) Consider what services (e.g. streaming) you can exclude from your VPN tunnel to reduce the impact on your network while meeting your security requirements.
- Review and update auto-routing of phones for call centers, help desks, operation centers, etc. as appropriate.

Security

- With a distributed workforce, ensure that security tooling is going to work off the network and there is a requirement or security control in place to monitor all web traffic.
- Define the options for staff around the world to access your environment. Be sure to set proper user-level and admin-level accesses. Connectivity options include corporate devices with VPN, VDI, cloud workspaces, bastion hosts, and potentially even personal devices with your corporate VPN and robust host checking.
- Security, privacy, risk and compliance teams in particular will be adjudicating policy exception requests. Many of these requests to be valid business needs but not all of them will be wise business decisions. When evaluating them, ask: does this align with our risk appetite?
- Make sure the governance around the exception management process and decision criteria is well laid out and good tracking mechanisms are in place so that you can revert back to business-as-usual operations at a future point. To allow previously restricted behavior such as adding printers, create an exception policy for specific users or groups or use a just-in-time admin provisioning tool coupled with a service desk approval process.

- Monitor for unsanctioned data access and movement. Adapt your data loss prevention (DLP) and user behavior monitoring rules to account for remote workers which may include but not be limited to concerns around printing at home, email forwarding, external storage drives, and alternate work schedules.
- If using managed service providers (MSPs) for security monitoring, notify them of the shift in operating models so they can tune and tailor their notifications to you and adjust their monitoring activities.
- Double down efforts on security patching and updates to remote access management solutions.
- Ensure security controls such as web filtering support a remote workforce.
- FS-ISAC members should monitor FS-ISAC traffic to stay up to date on evolving threats and best practices

Please be on the lookout for future communications on best practices from FS-ISAC.