White Paper

Insider Threat:

Reducing Gaps and Increasing Visibility for a Remote Workforce

While the rapid shift from office to home or remote-based activity has allowed work to continue, the idea that corporate assets are physically leaving the corporate space, and with them access to proprietary or sensitive data, could be a disaster if your security policies and practices are not adapting to this new norm. Now more than ever, companies need to be evaluating information technology and security practices surrounding insider threats.

The Risk

Many companies do not require their users to connect to a Virtual Private Network (VPN) in order to use their laptop or other asset remotely. In these cases, users connect corporate assets to home networks and access content that would otherwise be restricted within the corporate network. The lack of security controls in a home or public network compared to a corporate environment increases the potential for inadvertent data disclosure. Most home networks are used to connect personal devices and Internet of Things (IoT) systems, many of which are highly vulnerable. Without the right security measures in place on the corporate asset, the user could accidentally run malicious files or share sensitive information. How do you know what your workforce is doing with your data?

The Gap

Corporate security teams should have a deep understanding of what tools are within their own security stack, what logs are generated from those tools and what depth of information can be found inside those logs. Unfortunately, few security teams can claim that level of visibility and knowledge.

Whether you have an existing insider threat program or are rapidly trying to adapt to the new remote work reality, corporations should review their security stack in the context of a gap analysis. Performing a gap analysis enables security teams to better understand what logs they are collecting, the fields within those logs as well as understand the new limitations of previously deployed on-prem solutions, which may not function the same with a remote workforce. Understanding what datasets are captured from the endpoint, network perimeter, and applications when a user is connected and disconnected from the corporate VPN can provide a security team with a baseline of the current posture as well as a roadmap to better visibility. With the ultimate goal of enabling the security team, the same level of visibility exists into users who are either on-site at their desks or off-site connected through the VPN. Employees using their assets without the VPN not only increases risk to the corporate data but also makes it difficult for security teams to see what is happening on those systems.

Visibility

The level of visibility is dependent on the endpoint security stack and the location of the servers collecting logs and other data from these security tools in relation to the rest of the network.
For example, if a laptop is pushing security event logs to an internal SIEM within the corporate environment, it is likely that the SIEM will not be able to index the logs until the user connects to the VPN. What if the user doesn't need to connect to the VPN in order to complete his or her work? Is visibility out the window?

This is only a single example, but consider the security stack of your organization and the reliance of centralized logging, DLP, AV, Network logs; are all of those lost if a user does not connect to a VPN?

If the company doesn't want to force users to connect to the VPN, the options to collect logs or other artifacts from the remote endpoint involve public facing servers. Companies can install, or migrate, existing security appliances within the DMZ, or Demilitarized Zone, of the firewall which is a common place for public-facing assets such as web and email servers. The downside to this option is the increased risk to the corporate network from a malicious outsider.

The other option is to integrate a cloud-based solution which aggregates and correlates security data from the endpoints without putting the corporate environment at risk since it isn't physically connected to it. Migrating to cloud solutions during the remote work reality ensures continual coverage of assets and logging regardless of connectivity to corporate VPNs.

Detection & Response

Nisos breaks down the investigative portion of insider threat into two parts: Detection and Response. Detection is looking for behavioral indicators of negligence or malicious behavior which are out of the norm for the workforce as a whole. Response is tailored and focused to an identified threat and the observed behaviors, typically using a combination of SIEM logging and enhanced monitoring of behaviors using User Activity Monitoring (UAM) tools.

Throughout the Detection phase, if employees are observed performing actions which rise to the potential threshold of transitioning to the Response phase, the insider threat team performs a risk assessment to prioritize each case. A risk matrix should be tailored to your organization or industry to ensure the limited resources within the insider team are focused on individuals who pose the greatest threat to your organization.

The matrix may include questions like: Do they have access to the "Crown Jewels"? Or, are there indicators of other behaviors historically? However, it is important to remember insider threat responsibilities do not flow from Detection to Response and back to Detection. Detection is an ongoing process.

During this remote-based activity period, previously implemented perimeter protection is irrelevant when the traffic flow does not pass through corporate network assets (i.e. proxy, firewall, NSM) for both Detection and Response. The lack of logging opens up new gaps of untraceable actions, for example accessing "threat sites" to include pastebins or competitor job sites, performing high volume/size uploads, or using log clearing software.

For organizations which have not implemented public facing solutions for user behavior monitoring or endpoint management and security, these gaps force analytics of user pattern of life or behavioral review to be derived from severely limited datasets, often resulting in incomplete or inaccurate conclusions. Taking the time to lay down the appropriate security stack on your endpoints now is a giant step in the right direction and will set up your insider threat team for success when the users and assets come back to the office after we have weathered this storm.

For additional information, visit www.nisos.com or contact info@nisos.com.