Remote WORKFORCE - The NEW NORMAL

The Unrehearsed scenario (COVID-19 pandemic) has put the Cybersecurity Team with two immediate priorities. First to secure the remote work force arrangements on an unprecedented scale now that organizations have told employees to Zero traveling and Zero gathering, and government officials in many places have advised or ordered their people to stay home as much as possible. Second is maintaining the Confidentiality, Integrity, and Availability of consumer-facing network traffic as volumes spike.

Securing Remote Workforce

Quick adoption on the remote work (Work from home) has put considerable strain on Cybersecurity teams, which must safeguard these tools without making it hard or impossible for employees to work. How Cybersecurity (SOC Team) are securing these new work-at-home arrangements highlight the changes brought in three areas: technology, people, and processes.
Technology: Evaluate right controls are in place

Patching Critical systems
Organization must break the traditional patching cycle and has to adopt shortening of patching cycle for systems like Endpoint Security (Antivirus, Data Loss prevention, Firewall and Encryption), Virtual Private Network (VPN) and Perimeter security of both On-Prem and Cloud Environment.

Virtualization adopting
VDI (Desktop as a service) can make it easier for staff to work from home because many of them can be implemented more quickly than on-prem solutions. But we should also implement more controls over the VDI such as write control (Image altering control) Remote brokers and MFA. It will provide the Organization to secure the image accessed from the internet world.

Multi Factor Authentication
Remote workers must be enforced with multifactor authentication (MFA) to access networks and critical applications. Several practices make the rollout of MFA more manageable. One is to prioritize users who have elevated privileges (such as domain and sys admins, and application developers) and work with critical systems. Elevated privilege users should be targeted in pilot rollout will allow cybersecurity teams to learn from the experience and use that knowledge to shape more extensive implementation plans. MFA is just a flip of switch which the cloud providers and other technology vendors are already integrated with existing process.

Shadow IT
In many Organizations, employees use so-called shadow IT systems, which they set up and administer without formal approval or support from the IT department. Extended work-from-home operations will expose such systems because business processes that depend on shadow IT in the office will break down once employees find themselves unable to access those resources. IT and security teams should be prepared to transition, support, and protect business-critical shadow assets. They should also keep an eye out for new shadow-IT systems that employees use or create to ease working from home, to compensate for in-office capabilities they can’t access, or to get around obstacles.
Alternate Controls for On-prem based applications for remote access
Some of the On-Prem hosted applications like CRM and ERP are available only for onsite (On Office network) workers. To make such facility-based applications available to remote workers, companies must protect those apps with special controls. For example, companies might require employees to activate VPNs and use MFA to reach what would otherwise be facility-based assets while permitting them to use MFA alone when accessing other parts of the corporate environment.

People: Educate users about the Risk
With all above said stronger Technology controls, Remote workers must still exercise good decision making to maintain information security. With the unexperienced lockdown scenario at home will put the employees under stress and prone to social-engineering attacks. Some employees may notice that their behavior isn’t monitored as it is in the office and therefore choose to engage in practices that open them to other threats, such as visiting malicious websites that office networks block. Building a “human firewall” will help ensure that employees who work from home do their part to keep the enterprise secure.

Creative Communicate
Security Awareness to users may bring down many cyber security risks. Security team must be proactive and as well as creative to send communications on the emerging threats and risks. Security team as to set up a two-way communication channels that let users post and review questions, report incidents in real time, and share best practices; Explore effective communication using existing channel to reach the maximum audience in the network.

Focus on Do's and not on Don'ts
Security Team must provide guideline on the Do's and Don'ts while employee working from home. Most often employees assume the internet and email usage from work from home is not monitored. It is the responsibility of the Security team to explain the use of approved messaging, file-transfer, and document-management tools to do their jobs.

Awareness of social engineering
Users needs to be educated with Phishing (COVID-19 Theme), vishing (voice phishing), and smishing (text phishing) campaigns have started. Security team must test such campaigns with the employees to avoid surprise incident reporting.

Classify and Monitor high-risk user groups
Some users, such as those working with personally identifiable information or other confidential data, pose more risk than others. High-risk users should be identified and monitored for behavior (such as unusual patterns or bulk downloads of Organization data) that can indicate security breaches.

Processes: Promote Flexibility
Few business processes are designed to support extensive work from home, so most lack the right embedded controls. For example, an employee who has never done high-risk remote work and hasn't set up a VPN might find it impossible to do so because of the in-person VPN-initiation requirements. In such cases, complementary security-control processes can mitigate risks. Such security processes include these:

Supporting secure remote-working tools
Security and IT help desks should add capacity while exceptionally large numbers of employees are installing and setting up basic security tools, such as VPNs and MFA. It might be practical to deploy security-team members temporarily at call centers to provide added frontline support.
Test and Adapt IR and BC/DR capabilities
Even with increased traffic, validating remote communications and collaboration tools allows companies to support incident-response (IR) and business-continuity (BC)/disaster-recovery (DR) plans. But companies might have to adjust their plans to cover scenarios relevant to the current crisis. To find weak points in your plans, conduct a short IR or BC/DR tabletop exercise with no one in the office.

Securing physical documents
In the office, employees often have ready access to digital document-sharing mechanisms, as well as shredders and secure disposal bins for printed materials. At home, where employees might lack the same resources, sensitive information can end up in the bins. Define norms for the retention and destruction of physical copies, even if that means waiting until the organization resumes business as usual.

Expand monitoring
Now with the pandemic situation in place the scope for monitoring activities has widened in specific to endpoints and data, is important for two reasons. First, cyberattacks has thrived and second, perimeter security like firewall, IDS and IPS will not secure people working from home. To increase the monitoring view Security team has to update it SIEM with new rules, IOC and STIX.

Incident-response Playbook
When cybersecurity incidents take place, SOC teams must know how to report them. Cybersecurity leaders should create playbooks with multiple scenarios and response to such protocols as the normal escalation pathways are interrupted because people are working from home.

ABOUT GAVS
GAVS Technologies is focused on automation-led digital transformation services. GAVS’ IP led solution, Zero Incident FrameworkTM is an AIOps solution that enables organizations to trend towards a Zero Incident EnterpriseTM.

For more information on how GAVS can help solve your business problems, write to inquiry@gavstech.com
www.gavstech.com