Digital Security Posture – A Competitive Advantage

Cybersecurity is a strategy of defense. No offense. No victories. No celebration. Progress is measured by reducing or eliminating exploits (to the best of one's knowledge) and having resiliency over time. However, the battle is becoming more complex on many fronts.

The human body is protected by a perimeter of skin with antibodies fighting when the intruders (viruses) are recognized. Likewise, organizations have used this perimeter and antivirus strategy effectively when they were centralized.

Today, firms operate in a distributed model with entities (HQ, branches, work-at-home employees) communicating with each other worldwide. This distributed exposure extends to business partners who themselves are becoming distributed. If an entity is compromised, communications with other entities are vulnerable to exploitation. Furthermore, new malware are created at an alarming rate. Antivirus vendors are challenged trying to keep up with signatures (fingerprinting) and distributing them to endpoints.

The digital world is changing rapidly – organizations are embracing the cloud, mobile is ubiquitous, social media are enhancing communications, and the Internet of Things (IoT) is proliferating. An updated approach is needed to manage an organization's cybersecurity posture – a digital security posture.

Baseline

During transition to the new digital world, organizations should maintain their traditional cybersecurity baseline. Some established leading edge vendors are helping firms maintain their baseline while moving cybersecurity management to the cloud. This reduces costs and allows endpoints to update without being connected to the organization's network.

Risk management should drive cybersecurity decisions based on an organization's needs and risk tolerance.

People, Technology, and Policies

As organizations change so do its people, technologies, and policies. Creating a digital security posture for this dynamic environment requires properly trained people, emerging technologies, and the right policies. You can't protect against today's threats with yesterday's thinking, yesterday's technology, and yesterday's policies.

Focus On Critical Data

In this new digital world, with an ever increasing and distributed attack surface, you can't protect everything. Bad actors learn about your organization, employees, partners, and supply chain through your digital shadow – your digital exposure. Their goal is to exploit assets which have value – assets with critical data.

Critical data can include sensitive information (e.g., PII) and critical infrastructure (e.g., Active Directory). Assets without critical data can be used as a basecamp to launch attacks against other entities with which they communicate. They repeat this strategy until they exploit assets with value.

If critical data are exploited there may be financial, legal, compliance, reputational, and operational consequences. Discover where your critical data reside (awareness) and create strategies to protect it. Use several layers of protection, including encrypting critical data in motion and at rest.

Perimeter Secured Applications

Applications are your gateway to critical data. Create perimeters around these applications to protect against virtually all threats. Focusing on this smaller perimeter surface can effectively and more economically provide protection.

Shrinking the perimeter around the application requires securing paths to critical data. It's about building trust for network access and host server access with applicable policies.

To thwart network access attacks shrink the perimeter around the application. This is best accomplished using the open source Software Defined Perimeter (SDP) which combines device authentication, identity-based access and dynamically provisioned connectivity. SDP is designed to provide on-demand, dynamically provisioned, air-gapped (trusted) networks. Shrinking the perimeter creates a new layer of defense around applications, hiding application servers from all users and devices – except those that are authorized for use.

To thwart server infrastructure attacks and shrink the perimeter around VMs they host, implement hyper secured servers. Hyper secured servers are a trusted and tamper-resistant computing platform with a hardware-based root-of-trust that integrates compute, security, virtualization and policy. The perimeter provides full visibility of communications, enforces access control policies, and features advanced proxy-protocol shields for network, web, identify directories, administration, and file system.

Cloud Apps

Organizations are embracing the cloud app model - Software as a Service (SaaS). After proper due diligence apps are approved for use in the organization, called sanctioned apps. However, apps are being used by employees without approval, called unsanctioned apps. In enterprises, unsanctioned apps number in the hundreds.

Technologies are needed to discover what apps are being used (sanctioned and unsanctioned), how they are used, who is using them, and if critical data are involved. Data Loss Prevention (DLP) ensures that critical data are encrypted or blocked, or alerts the user to the possible violation. Policies are needed to govern app usage.

Gartner has named this technology segment Cloud Access Security Broker (CASB) and it should be part of every digital security program.

Endpoint Protection
Critical data stored on endpoints (computing devices such as PC, Mac, Server, Smartphone, etc.) need to be protected against exploitation. Encryption is encouraged but is not a magic bullet.

Signature based anti-virus products cannot recognize new or morphed viruses. Consider next generation solutions which leverage artificial intelligence and machine learning to recognize malware and immediately block them before they can exploit critical data. This new generation of antivirus software is low-impact and can run with existing antivirus products, if desired.

Cyber Exposure Awareness
An organization's digital footprint, an electronic trail of their activities, is actively stored in the surface web and passively seeping into the dark web. A subset of the digital footprint is an organization's digital shadow – your digital exposure. It consists of exposed personal, technical or organizational information that are critical data - often highly confidential, sensitive or proprietary. Bad actors can exploit a digital shadow to find your organization's weak points and launch targeted cyber-attacks.

Fortunately, attackers also leave a digital shadow and this trail can be used to your advantage. It will help you understand the attacker's patterns, motives, attempted threat vectors, and activities on the dark web, in order to better assess and design your digital security posture. This attacker information should be shared with penetration testers so they can create more accurate tests tailored to your organization's threat profile.

Cyber exposure awareness is understanding your digital exposure to make better decisions to prevent, detect and help contain cyber-related incidents. Trained analysts with the right technology can alert you to potential threats, instances of sensitive data loss, or compromised brand integrity.

Conclusion
The best digital security posture includes an equal mix of people, technology, and policies driven by business needs and risk management.

You can't protect everything and the bad actors are going to get in. Therefore, concentrate on protecting critical data which are most valuable to your organization or if exploited can cause great harm. Properly implementing emerging technologies can improve your digital hygiene and protect you against bad actors.

A good digital security posture is a competitive advantage.

Wayne Scarano, CISSP, CCSK, SABSA
Cybersecurity Analyst
wscarano@sga.com
SGA Cyber Security, Inc.
sga.com