radware

ADAPTIVE SECURITY: CHANGING THREATS REQUIRE A NEW PARADIGM FOR PROTECTING CYBER ASSETS

by Enterprise Security & Risk Management at Tech Mahindra

As organizations continue to embrace the digital revolution, a growing number of assets are being connected to the Internet. In fact, most organizations are now using cloud-based applications to power operations. With this shift, IT infrastructures have become more distributed. Applications are now accessible from anywhere and personal devices are being used to conduct business. Together, these realities have blurred the boundaries of the traditional network perimeter.

Attackers operate under a host of motivations—from hacktivism to monetary gain. No matter their intent, attackers benefit from the trend toward distributed IT, which increases the threat surface. Gone are the days when bolt-in and “afterthought” security architectures were sufficient. Static firewalls and intrusion detection or prevention solutions (IDS/IPS) woven around the asset simply cannot provide adequate protection. That’s because static firewalls and IDS/IPS leverage a model whereby they are fed known attack & protocol behavior and are not aware about the assets they protect. They are not cognizant of network behavior and are unable to protect against emerging attacks. If those approaches don’t work, what does? Tech Mahindra believes there is a need to realign security architecture by focusing on ensuring application availability and preserving user experience while protecting applications from both volumetric DDoS attacks and exploitation of vulnerabilities.

In designing such a strategy, there are two important prerequisites for success:

1. **Know Your Assets.** This includes components such as web and mobile interfaces, databases, development and test cycles, operating systems, where applications are being deployed, by whom and from where the infrastructure is being accessed. Understanding these variables is an important requirement for reducing the attack surface within the environment.

2. **Map Your Risks and Take Steps To Reduce Them.** Often attack activity goes unnoticed for a significant periods of time. Thus, it's crucial to understand attackers: how attacks have evolved over time, which direct and indirect strategies an attacker might unleash against assets, and the hacker's "mindset" to help in identifying attacks that may have gone undetected and thwarting future attacks.

With applications being updated frequently, development and test cycles have shortened, and workloads have become dynamic. In many organizations, time-to-market pressures, lack of resources and lack of awareness and focus on security converge to create security gaps in applications. As a result, it has become critically important that security be highly adaptable—with continuous adjustments to address fast-changing applications and threats. With an adaptive security approach, an organization can establish an effective security architecture for mitigating threats—both known and unknown.

Tech Mahindra's View on Adaptive Security

At Tech Mahindra, we see three key building blocks for adaptive security:

1. **Continuous Proactive Assessment.** Adaptive security requires continuous assessment of an organization's infrastructure and applications. Continuous assessment via manual and automated tools generates a security baseline that can be tracked and improved upon. With applications as key attack targets, the assessment must also evaluate the application development phase, thereby preventing vulnerabilities from creeping into the production environment. Recent attacks originated in IoT devices have illustrated the danger of device manufacturers failing to consider potential risks and vulnerabilities within their devices. Just as manufacturers are being held to higher standards, so should application developers. Incorporating security right from the start will help identify any vulnerabilities during the development stage so that sufficient controls, such as secure communication, authentication and authorization, can be integrated. In other words, when new code or a new application is deployed into production, it must pass through these security assessments.

2. **Situational Awareness.** Adaptive security must continually evolve at run time to address ever-changing application and user behaviors. Contextual information from continuous monitoring is a key input for an effective adaptive security strategy. With this approach, the security architecture is not entirely dependent on the traditional signature-based threat information but is instead based on real-time situational awareness. Continuously evolving security requires complete awareness of the assets being protected—such as the core network, applications and endpoints—and user behaviors related to those assets. If new code or a new application is deployed, the architecture detects the change and fine tunes the policies vis-à-vis any new vulnerabilities. Volumetric DDoS attacks are a constant threat to online IT assets, with attackers typically merging malicious traffic with benign traffic (sometimes even using encrypted protocols). Thus, the ability to analyze traffic behavior and recognize user traffic patterns using various parameters, together with maximum detection accuracy, is key to dropping only malicious traffic and preventing any service degradation.

3. **Automation.** When organizations deploy best-of-breed security solutions, these solutions almost always operate in silos. Automation in security can enable organizations to design a security architecture where security functions coordinate with each other, share information and respond dynamically to attacks. For example, adaptive defense mechanisms can use signaling or other forms of messaging between security

controls; they can auto-learn new attack patterns; and they can accelerate time to mitigation through real time creation of protection. Ultimately, automation is about prevention versus detection—and it empowers organizations to secure themselves at the speed of attacks. Automation in security can enable siloed security modules to work as a synchronized system—operating with minimal intervention and significantly improving both incident response time and resource consumption. Just as dynamic business environments lead organizations to adapt, so does the threat landscape. With distributed, heterogeneous information architectures, application protection can no longer count on static models, but rather must include advanced mechanisms like real-time auto-learning and self-updating to provide seamless and continuous protection of an organization's most critical digital assets.

Tech Mahindra Security Service Portfolio includes Security Consulting, Identity Access Management, Application Security, Infrastructure Security and Threat Management. We continuously help our customers in their journey towards the mature security posture. Tech Mahindra's global partnership with Radware for on premise and cloud-based security solution is in line with the continuously adaptive security approach.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.