aunalytics

Security Maturity Improvement is Imperative as Cyberattack Risks Remain High

While advancing technology offers significant benefits, it has also made it easier for those who seek to gain an advantage by exploiting others. People intent on stealing your data or holding it to a hefty ransom are hidden in the digital web of interconnections, making the information age a double-edged sword.

An attack can be devastating for any business and impact it for many years to come—today's organizations need digital sentries and multiple lines of defense against cybercrime.

According to a report released by Ponemon and IBM, **83 percent of organizations studied have experienced more than one data breach**, and just 17% said this was their first data breach. Around 70% of successful cyberattacks exploited known vulnerabilities with available patches or known remediation steps. Identifying and resolving vulnerabilities is critical since a successful exploit can lead to a full-scale system breach.

Vulnerability management ensures that organizations have visibility around the latest known threats, preventing attacks before

they occur. However, managing scanning or patching can be a challenge for smaller teams due to the ongoing cyclical management required. Setting up and coordinating manual ongoing patching across an organization can be extremely cumbersome, taking days to organize, schedule, and execute.

McKinsey cites good patch management as a top proactive maintenance measure that can help organizations prevent cyberattacks. However, knowing the priority level for addressing risks, or deploying patches, can be confusing and lead to poor risk management as a result.

Enlisting the help of a partner to ensure vulnerability management best-practices can add true value to many organizations.

How Organizations Can Improve Their Security Posture

When coupled with existing security defenses, the following regiment can significantly strengthen an organization's security posture:

- **Vulnerability Management** - Continuous attention and a dedicated focus on assessing and remediating threats is required to minimize an organization's vulnerability. The preferred vulnerability management approach is overseen by security professionals, and involves discovering devices on the network, regularly scanning for vulnerabilities, and facilitating remediation of those findings. Remediation could be in the form of patching software or operating systems, or even configuration changes to resolve a known threat.

- **Security Awareness Training** – This type of training is necessary to educate employees about the dangers in their digital environment and how to properly recognize and handle them. Leveraging a well-established security training platform is key for the best information, strategies, and toolsets employees need to equip themselves to better protect their organization before data loss or other harm can occur.

- **Security Maturity Journey** – If your business security approach is not keeping up with the rapidly changing threat landscape, it will become obsolete and more vulnerable to bad actors. Security maturity means adapting and improving security as the environment changes and grows. It means taking strategic actions like improving visibility with the approach of expanding security telemetry from your company systems. Businesses can evolve from a legacy security state to security maturity with the help of a trusted partner supported by a team of cybersecurity experts.

The growing threat of cybercrime is a risk to literally all organizations. Attacks can arrive in a number of forms, including phishing, spear phishing, ransomware attacks, zero-day attacks, known vulnerability exploits, brute-force attacks, and other tactics. Incorporating a comprehensive mix of security-awareness education, proactive visibility, and continuous security posture improvements can offer peace of mind as well as significantly reduce business risks.

Better security means achieving full accountability of business assets from a security visibility perspective. Organizations can't protect what is not actively managed, monitored, and covered with security tool sets. It also means educating employees so they are aware of security threats and can play a role in reducing the likelihood of a successful attack from email, internet browsing, social media, or other modern tactics. These measures can significantly reduce risks of exposure or compromise while continuously improving security posture as threats evolve.

About Aunalytics

Aunalytics is a leading data management and analytics company delivering Insights-as-a-Service for mid-sized businesses and enterprises. Selected for the prestigious Inc. 5000 list for two consecutive years as one of the nation's fastest growing companies, Aunalytics offers managed IT services and managed analytics services, private cloud services, and a private cloud-native data platform for data management and analytics. The platform is built for universal data access, advanced analytics and AI—unifying distributed data silos into a single source of truth for highly accurate, actionable business information. Its Daybreak™ industry intelligent data mart combined with the power of the Aunalytics data platform provides industry-specific data models with built-in queries and AI for accurate mission-critical insights. To solve the talent gap that so many mid-sized businesses and enterprises located in secondary markets face, Aunalytics' side-by-side digital transformation model provides the technical talent needed for data management and analytics success in addition to its innovative technologies and tools. To learn more contact us at +1 855-799-DATA or visit Aunalytics at https://www.aunalytics.com or on Twitter and LinkedIn.