Cyber Security

Mr. Rob Zitz
Vice President/Chief Systems Architect, National Security Sector
Leidos

The threats, risks and consequences of cyber-attacks on our networks, systems and data dictate a unified approach to defense which encompasses organizational, behavioral and technical aspects. The proposed presentation will discuss how each of these aspects has evolved, how integrating the three into a unified approach works, and discuss key technical advances today and on the horizon to combat cyber-attacks.

Traditional organizational approaches to cyber security saw the issue as the IT department's problem. Organizations often allowed individual components to develop and implement their own unique risk and management methods. The modern organizational approach is to view cyber security as the Commander's (CEO and Board in the private sector) concern that directly impacts mission effectiveness, with a corresponding level of focus on risk and consequence management. This has led to a much more centralized approach with top leadership infusing awareness throughout all levels of the organization, making continuous cyber security integral to decision making.
Traditional behavioral approaches often confined information security experts to the IT department, and provided only limited training and education for the workforce. Cyber security was largely a rules-based method with controlled access, networks and device restrictions. Limited information sharing across organizational boundaries prevented sharing of best practices and sometimes, prevented early warning of new and emerging threats. The modern behavioral approach encourages a culture of deep understanding of the threats, risks and consequences, asks each individual to own the problem, and requires everyone to be an active member of the cyber security team. More modern approaches provide continual review and revision of training programs, and require employees to agree to sophisticate monitoring for adherence to policy. Modern behavior instills an atmosphere of cross-organizational training, information sharing and lessons learned.

Traditional technological approaches implemented rigid network perimeter defenses that were based on limiting administrative privileges, access points, platforms, operating systems and applications. Use of Virtual Private Networks emerged. Concern regarding BYOD (Bring Your Own Device) grew. Traditional technical methods were heavily focused on intrusion detection and forensics using signatures-based defenses, which are inherently reactive. Modern technological approaches employ a defense-in-depth construct which implements a layering of basic hygiene (i.e., maintenance of basic firewalls, anti-virus software, strong passwords, and signature-based detection) with a mitigation strategy that includes white listing, prompt patching and policy tuning. The modern layering then adds Continuous Diagnostics and Mitigation (CDM) which conducts real time comparison of network performance and trends and provides real time risk assessments. Modern approaches add another layer which is the use of Big Data analytics, employing cutting edge change detection and warning tools and sensors that are deployed both internally and externally.

Next steps in technology recognize that networks do not attack networks, people do. This has led to research regarding next generation automation tools including Automated Behavioral Analysis technology which shows promising in prediction of cyber security threats before they penetrate the network and do damage.