Title: How to Protect Critical Infrastructure From Hackers. By: Virgillito, Dan, CIO Insight, 15350096, 6/18/2015

Database: Business Source Complete

How to Protect Critical Infrastructure From Hackers

Listen American Accent

Guest Author

Enterprise security management is a time-intensive process, and to safeguard every aspect of the company, organizations can't afford to take any shortcuts.

.

With enterprises moving towards new technologies to minimize costs and optimize resources, they face increased security risks as cyber-criminals adopt new techniques to target BYOD devices, corporate networks and backend servers. As a result, it has become crucial for stakeholders to understand how to balance the security management landscape with enterprise operations. Organizations need to place more focus on ESM (enterprise security management) to create a security management framework so that they can create and sustain security for their critical infrastructure. Enterprise security management is a holistic approach to integrating guidelines, policies and proactive measures for various threats.

ESM pertains to all risks that may affect the core business of an organization. It includes failed software processes, inadvertent or deliberate mistakes committed by staff members, internal security threats, and

external security threats. The concept also takes into account the following factors related to security architecture framework:

*Enterprisewide compliance: The number of regulatory requirements can affect the end product/service delivery. The ESM framework aims to resolve conflicting business objectives, as well as fulfill regulatory and internal compliance requirements.

*Business-focused outcome: In a standard ESM framework, security risks and company objectives driv the selection of security implementations. As it is a top-down architecture, it ensures the identification and control of all policies.

*Clarity at data-infrastructure level: The key challenge for the enterprise is to gain clarity around resolving conflicts pertaining to data privacy requirements, vulnerability vectors and company objectives. The ESM approach to clarity enables the enterprise to gain transparency around the aforementioned, both at the infrastructure and data security level. *Transformation of security at all levels: ESM adopts the approach called "architecting a security framework at all levels'" of an organization. It defines security capabilities from the governance level all the way through architecture, and involves planning to build, monitor and deliver security within all organizational units, processes and business functions.

Deploying ESM Framework

All stakeholders will look to the CISO/CSO/CIO to deploy and manage ESM frameworks, as well as the steps the organization is taking to reduce risk to the enterprise. How does a CIO integrate ESM framework and cultivate a security culture that finds long-term success throughout the organization? The answer lies in adopting a strategic approach towards enterprise security management. The following steps should be undertaken:

Patch management

Software vulnerabilities are one of the leading issues in the enterprise environment. Patches are additional code to replace flaws in software. Patch management is part of the SDLC (software development life cycle) and can occur in any primary process of SDLC.

The importance of implementing patch management as a part of ESM is gaining value, as there have been a plethora of exfiltration and data breaches around the globe. Scanning and updating of patches to prevent and mitigate undiscovered vulnerabilities is important and requires security management at all phases: QA, development, staging and maintaining strict policies to avoid any unexpected events.

Threat modeling

Who might attack the enterprise? Is it only cyber-criminals, or nation states as well? What about company insiders? Start thinking about the list of possible adversaries and get detailed, without ruling out outlandish ideas your team may come up with. Threat modeling requires the following steps:

*Identification of security objectives

*Companywide survey

*Decomposition

*Identification of threats

*Identification of vulnerabilities

Typically, a threat model takes longer to construct, but a sample structured list can be followed. Usually, the model is based on the following assumptions:

*Data validation may enable SQL injection

*Authorization may fail, so authorization checks are required

*SSL should be used as the risk of eavesdropping is high

*Anti-caching directive should be implemented in HTTP headers as browser cache may contain man-in-the-middle vulnerabilities.

With these assumptions, organizations can consider the STRIDE or DREAD threat model.

Architecture Principles

ESM never assumes that developing a threat model can provide sufficient risk mitigation for specific threats. It aims to deploy multiple controls in order to prevent and minimize damage while an enterprise responds. Architecture principles in ESM include the following:

Security resiliency: Ensure security defenses throughout the organization by strengthening the resiliency of software, applications, networks, servers, and systems to recover from unforeseen circumstances.

Segregation: Security initiatives should be categorized in functional blocks, and organizational units will have distinct roles within each block to facilitate management and secure the critical infrastructure.

Regulatory compliance and efficiency: Industry best practices should be followed to achieve regulatory compliance. Efficient configuration throughout infrastructure lifecycle and increased visibility will allow for faster troubleshooting, incident response and auditing.

Systemwide confidentiality and collaboration: Security controls need to include accepted levels of confidentiality, and effective infrastructure security will require correlation, collaboration and sharing of information from all systemwide sources.

Risk Management

The compromise of R&D intelligence, customer data and company secrets leads to loss of millions of dollars in terms of trust, confidence and monetary value. As such, enterprises must employ a risk management approach against targeted attacks.

Because conventional security implementations are no longer sufficient against techniques such as hacking, DDoS, botnet, state-sponsored espionage and others, the latest ESM model includes the adoption of behavior detection and network virtualization to avoid becoming victims. It would be based on a custom defense strategy that utilizes a specific intelligence adapted to each enterprise and its potential attacker.

Additionally, risk management enforces stronger adoption of intelligence-based security solutions that are backed by reliable threat information sources. This will help enterprises to thwart attempts to vulnerabilities before patches are updated.

MDM & Mobile Safety

With the inception of BYOD there have been many issues pertaining to data protection and control arising when an enterprise defines the lines between personal and corporate data. Additionally, there are other threats such as data breaches through staff-owned devices and physical theft.

As a result, enterprise security management must address MDM (mobile device management) to protect enterprise data, devices and apps. Administrators in the IT department should be able to centrally manage all device users from a centralized console, enabling visibility and increased mobile use safety.

Software Defined Networking and Internet of Things

In ESM, the security control layer needs to be centralized for different parts of the critical infrastructure. That is where software defined storage (SDS) and software defined networking (SDN) comes into play. These two have been separated in the enterprise environment over the years, but need to come together in the future to deal with cyber-threats, which can reduce the damage across enterprise operational networks and industrial complexes.

Also, whatever air gaps and network segmentation methods an enterprise may have employed, there will be instances where the Internet of things (IoT) intersects the enterprise network, and these touch points will be vulnerable to cyber-attacks.

In fact, IoT can exacerbate the problem to a point where it can get messy to control internal and external networks and devices to gain access to enterprise data stored in the cloud, BYOD applications, networks and other places. This means a hacker can get into a Web-enabled device, and because of its connectivity with a corporate network, they can create a bridge to transfer malicious traffic back and forth.

These threats present an opportunity for enterprises to step in and implement security as a service in ESM for safeguarding those checkpoints and interactions, so the organization can continue to focus on gleaning security and corporate data.

Conclusion

Based on all this information, the enterprise security management landscape is expected to continue to change in 2015. Companies will need to start investing to upgrade their security beyond checkbox implementations to achieve compliance level of protection. Enterprises can no longer rely on keeping IT security as lean as possible in an attempt to cut operational costs.

ESM is a time-intensive exercise and to keep every aspect of their company secure, organizations can't afford to take any shortcuts. CIOs can use the above-mentioned information to make sure their organizations are being adaptive to the latest threats.

~~~~~~~~

By Dan Virgillito

Dan Virgillito is a security researcher at InfoSec Institute.

~~~~~~~~