CSO Outlook

JUNE - 2015 CSOOUTLOOK.COM

In My Opinion

Andrew Wild,
CISO,
Lancope

CXO Insight

Scott Brandt,
CIO & Director of IT,
Texas Office of the
Secretary of State

CXO Insight

Ondrej Krehel,
MD & Founder,
LIFARS

Company Of The Month

Madhan Kanagavel,
Founder & CEO,
FileCloud

BetterCloud: Taking Cloud Office to the Next Level

Michael Tweddle,
CSO

CSO OUTLOOK
44790, S Grimmer Blvd.
#202, Fremont, CA-94538

Taking control of IT Operations through the Critical Security Controls

By Matthew J. Harmon, Principal Consultant, IT Risk Limited

A common thread among most breached organizations is the entry point for attackers was unknown, deemed too fragile to patch, unimportant, or was considered low risk because it didn't hold or process regulated data. These systems become a pivot point for infiltration, allowing for escalation of privileges and network visibility through a patient and opportunistic approach slowly spreading through the environment. The strategy to prevent this type of infiltration is one that has frequently been lost due to organic growth, shadow IT, and cloud outsourcing– the defender's' advantage–knowing your environment better than your adversaries.

By integrating the SANS Institute and Center for Internet Security "20 Critical Security Controls" (CSC) into an organizational security roadmap, organizations can take control of their environment, reduce maintenance costs, and have better visibility and metrics to measure the effectiveness of IT operations and as a result reduce the cost of operations and the time to detect infiltrations.

As an introduction to the CSC, we're focusing on controls 1-5 and their place within the "First Five" which provide the greatest immediate impact and measurability of an improved security posture. Each control maps to NIST Special Publication 800-53 ("Security and Privacy Controls for Federal Information Systems and Organizations"), contains entity relationship diagrams, automation metrics, and the advanced sub-controls built on the quick wins, visibility and hygiene controls as determined by an international collective of security experts, government agencies and standards bodies. Most organization take upwards of 100 days to detect unauthorized access and in worst case scenarios infiltrations can last for years before being discovered by external entities. To illustrate these points, let's take a look at these controls from an attacker's perspective and what can be done to prevent the attacks.

Matthew J. Harmon

Inventory of Authorized and Unauthorized Devices

Without an inventory of devices on the network, a malicious individual can plug in a device to an exposed network port in an office or connect to the internal wireless network via stolen credentials. Once physically connected, an attacker can create a tunnel and remotely control their on-site device.

Meeting this control requires knowing what network enabled devices on the network are authorized, these devices can be inventoried by matching IP address assignment via DHCP (Dynamic Host Configuration Protocol) to IP addresses live on the network obtained via network mapping and comparison to ARP (Address Resolution Protocol) retrieved from switches and NAT (Network Address Translation) from routers and firewalls. This inventory of systems should be mapped to known system owners and data custodians.

Inventory of Authorized and Unauthorized Software

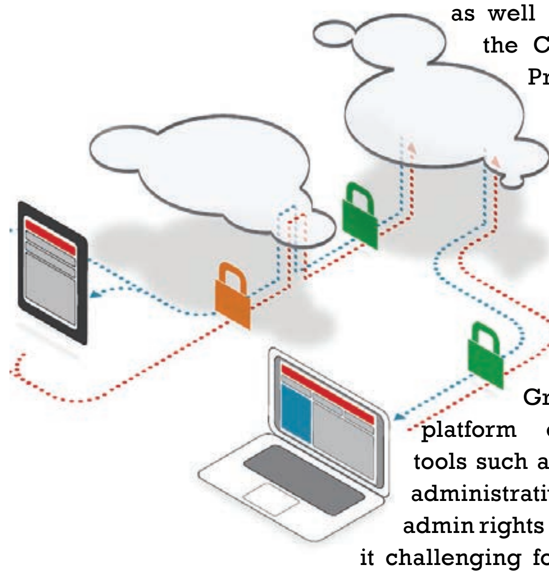
Failure to have an inventory of authorized (and unauthorized) software enables an attacker to trick targets into installing malicious software via phishing, malicious advertisements, or exploiting exposed USB ports. Once a backdoor or remote access tool is installed, an organization relies on anti-malware tools to detect known software signatures while attackers can remotely control the host and pivot to attack additional hosts. When employees install unauthorized software, the IT department is unaware of it and is unable to patch the software increasing the attack surface.

Implementing this control requires a software approval process that allows for patching and upgrades as necessary within 48 hours in response to critical vulnerabilities. In AD controlled Windows environments this is accomplished via SCCM (System Center Configuration Manager) through the "Enable software inventory on clients" setting, using WMIC (Windows Management Instrumentation Command) or PowerShell to remotely collect the installed product name and version. In Linux, package managers such as RPM and APT can quickly display installed software versions for remote collection. After the first software inventory, application whitelisting is possible with reduced administrative burden and significantly limits the ability for attackers to install malicious software.

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Without secure configurations, operating systems and software packages come with feature rich configurations enabled including default settings such as office suite macro languages which enable worms, autorun on removable devices which can lead to automated back door installation, remote content loading for email clients and automated sharing of workstations all provide a rich attack surface. The Hak5 Rubber Ducky automated keystroke injection attack platform is a preferred tool among IT professionals and attackers alike.

Secure configuration guidelines are readily available from operating system vendors and government agencies such as the NSA and DISA as well as industry groups such as the Center for Internet Security. Products such as Nipper and Paws from Titania Security automate this analysis process. Each disabled (unnecessary) feature reduces the attack surface when uniformly applied to standardized system images and enforced via Windows Group Policy Objects and cross platform configuration management tools such as Puppet and Chef. Limiting administrative access and removing local admin rights from non-admin users makes it challenging for an attacker to establish a foothold within an environment.



Continuous Vulnerability Assessment and Remediation

Vulnerabilities in IT infrastructure are weaknesses waiting for attackers to leverage and exploit. While servers get the lion's share of attention, client side software vulnerabilities allow an attacker to become an authenticated user and move through the environment undetected. Advertising networks, hidden HTML frames, Java Applets, ActiveX components and fake security pop-ups are frequently used as drive-by-download attacks enabling an attacker to opportunistically choose the compromised systems for organized campaigns to exfiltrate sensitive data.

Assessing vulnerabilities within an IT environment is easy when the first two inventory controls are completed and through secure configurations it becomes more difficult for attackers to leverage Zero-Day vulnerabilities, for which patches don't yet exist. Through prioritized and scheduled patch deployment and tiered infrastructure including testing and staging of patches before mass deployment, remediating vulnerabilities becomes routine maintenance for IT infrastructure. Critical and high vulnerabilities should be patched within the first 48 hours after release.

Malware Defenses

Malicious software is the cornerstone of the most successful attack campaigns and most organizations have not taken the most basic measures to prevent. Almost 100 percent of all environments have traffic being sent to hostile hosts and have at least one piece of malicious software installed.

While up-to-date anti-virus software is typically heralded as an optimal defense, it is only one of several defensive measures that should be taken. Enabling workstation and server firewalls, disabling autorun of removable media, checking DNS traffic for known bad hosts through services such as OpenDNS, checking for known bad actors through a threat intelligence service such as ThreatConnect, and forcing web traffic through a filtering web proxy are key components to successful malware defense.

With this introduction to the Critical Security Controls, the next step should be to determine a security baseline for the environment, then conduct a gap assessment against the remaining controls comparing the organization security stance to determine what has already been implemented and what controls remain outstanding. Once this gap assessment is complete, a roadmap should be created to fill these gaps and to schedule the implementation in phases working the controls into system management operations. CSO