Improving Application and Privilege Management: Critical Security Controls Update

Written by John Pescatore

April 2016

Sponsored by
AppSense

The threats that organizations face change continually, but almost all successful attacks exploit a core set of security weaknesses. The Center for Internet Security regularly updates its Critical Security Controls,[1] a prioritized list of 20 security controls that, when implemented well, have proved effective in blocking most advanced target threats and supporting faster detection and resolution of those that do get through initial defenses.

A subset of the highest-priority controls within the CIS Controls provides "quick wins," with immediate risk reduction against advanced target threats. For example, almost all forms of attack use privilege escalation when installing malware that needs administrative privileges. Phishing, which continues to be the most common front end for damaging attacks, is used to obtain user credentials from which to start the escalation, and phishing succeeds because of poor hygiene in application and privilege management.

The highest-priority controls within the CIS Controls provide "quick wins," with immediate risk reduction against advanced target threats.

The latest update of the controls, Version 6.0, recognized this common weakness and elevated the priority of these areas. For example, "Controlled Use of Administration Privileges" moved up from control number 12 to control number 5, and "Controlled Access Based on the Need to Know" moved up slightly, from number 15 to number 14. "Inventory of Authorized and Unauthorized Software" remained the most critical control, while "Secure Configuration for Hardware and Software" remained the third-most critical control.

Other efforts at defining security controls have placed similar emphasis on application and privilege management. For example, "Controlling Administrator Privileges" is second on the National Security Agency's IA Top Ten Migration Strategies,[2] and application whitelisting controls, as well as operating system patching, application patching and the restriction of administrative privileges, are listed in the Australian Signals Directorate Top 4 Strategies to Mitigate Cyber Intrusions[3] (see Figure 1).

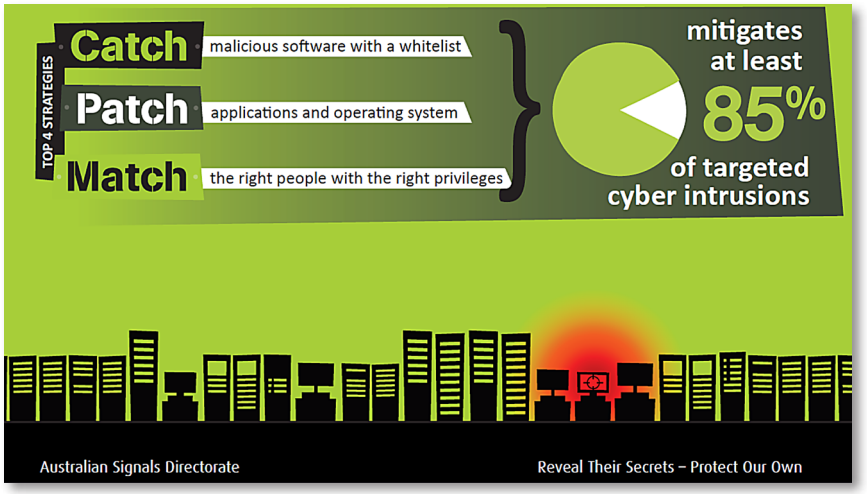

Figure 1. Australian Signals Directorate Top 4 Strategies to Mitigate Cyber Intrusions[4]

[1] The CIS Controls for Effective Cyber Defense Version 6.0, www.cisecurity.org/critical-controls.cfm

[2] National Security Agency, Information Assurance Guidance, www.nsa.gov/ia/mitigation_guidance/

[3] Australian Government Department of Defense, Strategies to Mitigate Targeted Cyber Intrusions, www.asd.gov.au/infosec/mitigationstrategies.htm

[4] Australian Government Department of Defense, Strategies to Mitigate Targeted Cyber Intrusions, www.asd.gov.au/infosec/mitigationstrategies.htm

The security benefits of application control and privilege management are well known—they are often considered to be Security 101. Nonetheless, the majority of breach reports have determined that attacks succeeded because of either missing or ineffective controls and processes in these areas.

The biggest barrier to enabling application control and privilege management has been fear of self-inflicted wounds: causing business disruption or huge increases in help desk calls as legitimate software and business-critical access are blocked. But products and techniques have improved over the past few years, and today you can find many success stories that show what works in enabling application control and privilege management with minimal or no interference to business operations.

This whitepaper will describe the recent update to Version 6.0 of the CIS Critical Controls, with a focus on application control and privilege management as high-payback, quick wins—when done right.

Why Targeted Attacks Succeed

Each year, the Identity Theft Resource Center (ITRC) publishes statistics and analysis on all data breaches that are publicly announced. In 2015, according to the ITRC, 781 breaches were disclosed, with an average of 216,000 records exposed per breach (see Figure 2).

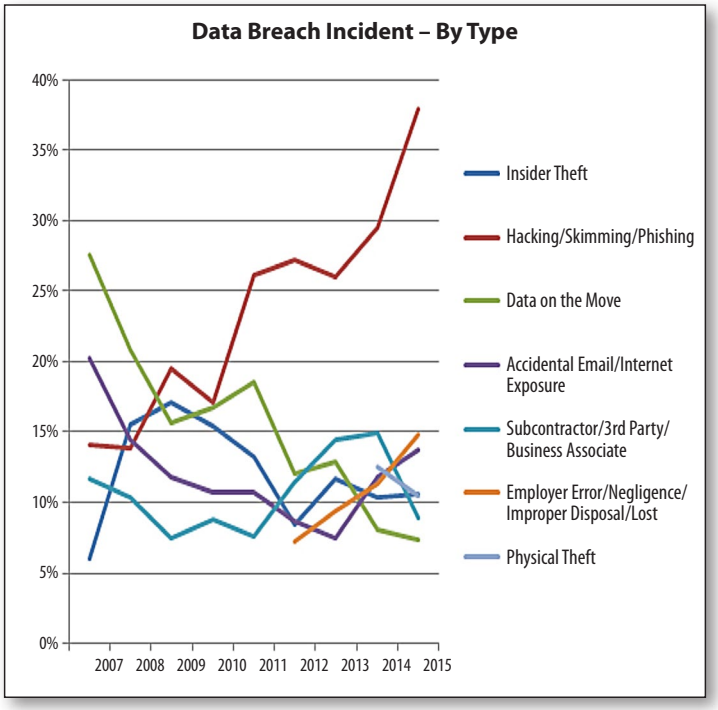

Figure 2. Phishing-Related Activity on the Rise[5]

[5] Identity Theft Resource Center, 2016 Data Breach Reports 2016, www.idtheftcenter.org/2016databreaches.html

The report found the largest and fastest-growing attack method to be hacking/skimming/phishing, with phishing techniques dominating that grouping. The Verizon Data Breach Investigation Report (DBIR) has reached similar conclusions (see Figure 3).

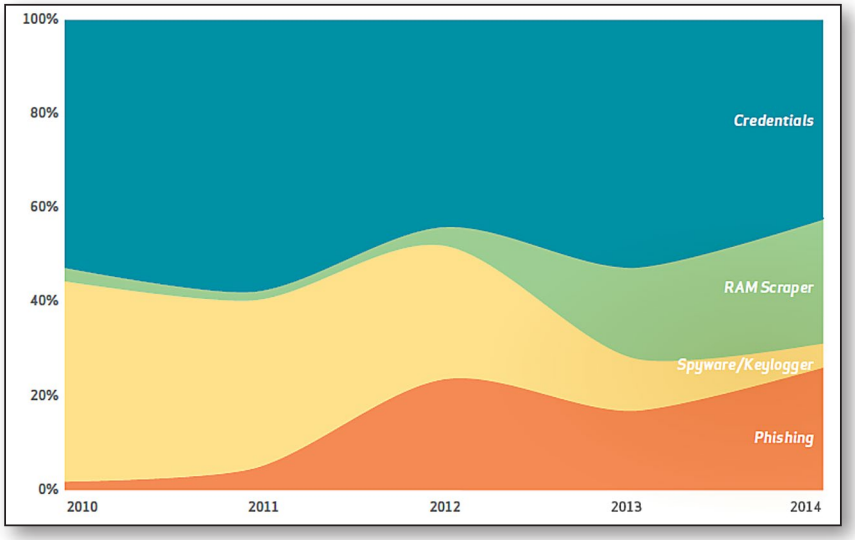

Figure 3. Success of Credential Theft and Phishing[6]

Phishing succeeds for several reasons:

- Reusable passwords continue to be in widespread use.
- Email and web browsing do not provide strong authentication to different legitimate connections from fraudulent connections.
- Users continue to be fooled by clever, targeted phishing attacks and give up their credentials.
- Enterprises continue to over-provision user rights for installing software and accessing data.

These factors all combine to enable phishing attacks to succeed. Improvements in security controls are needed in all areas, but eliminating passwords, hardening email and web applications, and changing user behaviors are long-term campaigns. Security programs can have near-term impact in disrupting common attack patterns by improving security controls around installing and executing applications and assigning user-access levels.

[6] Verizon, 2015 Data Breach Investigations Report, www.verizonenterprise.com/DBIR

Application Control and Privilege Management as Critical Security Controls

For many years, real-world experience and studies such as the Verizon DBIR have been finding that the majority of attacks are enabled by failures in basic security hygiene: the failure by businesses and government agencies to focus on the security basics that raise the highest barriers against real-world attacks. Back in 2008, penetration testers at the National Security Agency responsible for assessing the security of critical infrastructure systems kept running into this and developed the initial version of what is now known as the Critical Security Controls.[7]

The CIS Critical Controls are a community-driven effort that focuses on a simple but time-proven methodology for prioritizing the investments and actions that are most effective and efficient in reducing the risk of real-world threats.

The controls, now maintained by the nonprofit Center for Internet Security, are a community-driven effort that focuses on a simple but time-proven methodology for prioritizing the investments and actions that are most effective and efficient in reducing the risk of real-world threats. Key steps include the following:

- **Let offense inform defense:** Continually monitor attacks, determine root cause and focus on security controls that would eliminate attack paths, reduce time to detect, minimize attack impact and/or reduce time and cost to recover.
- **Validate controls with "what works" operational data:** Security controls that disrupt business operations will not succeed even if they are effective against real-world attacks. The CIS Critical Controls effort prioritizes security controls where there are proven, working implementations that have shown a measurable ability to reduce risk while minimizing business disruption.
- **Integrate and automate:** Simply adding more security processes and controls rarely increases security levels—often, new "solutions" that require high levels of staffing and unavailable skills turn into shelfware. Hiring and keeping skilled security staff continues to be a problem for CISOs, according to multiple SANS surveys.[8] The controls effort prioritizes security controls where proven tools and processes are available to act as force multipliers for reasonably skilled security analysts and to support integration of security-relevant data across multiple security processes.

The Critical Controls are updated roughly every 18 months through an open, community-driven effort that revisits these factors in light of changes in threats, business technology demands and solutions' maturity. The controls are then ranked in effectiveness and efficiency, and a new version of the controls (and validation guidelines) is documented and released.

[7] The SANS Institute, "CIS Critical Security Controls: A Brief History," www.sans.org/critical-security-controls/history

[8] The SANS Institute, "SANS 2013 Critical Security Controls Survey: Moving from Awareness to Action," June 2013, www.sans.org/media/critical-security-controls/CSC_Survey_2013.pdf

CIS Critical Security Controls Version 6.0 Overview

The latest update cycle occurred during the third quarter of 2015, resulting in Version 6.0 of the CIS Critical Controls.

The threat data and solution effectiveness evaluation during the Version 6.0 update resulted in a number of changes. The most significant include the following:

- "Controlled Use of Administrative Privileges," "Maintenance, Monitoring, and Analysis of Auditing Logs," "Data Protection," and "Controlled Access Based on the Need to Know" were significantly **elevated** in priority.
- "Malware Defenses," "Wireless Access Control," "Security Skills Assessment and Appropriate Training" and "Application Software Security" were **lowered** in priority.
- "Secure Network Engineering" was **eliminated** as a stand-alone security control, with its concepts included in other areas.
- "Email and Web Browser Protections" was **added** as a new control.

These changes were largely motivated by the recognition that in 2015 the vast majority of damaging, successful attacks used phishing or other email- or web-based techniques to obtain credentials and take advantage of legitimate user privileges to install targeted executables that evaded detection. Other changes in the wording and priority of subcontrols also reflect this approach. See Figure 4 for the new order of the controls.

Figure 4. CIS Critical Security Controls Version 6.0 Updated Order of Controls

The net result of Version 6.0 was to increase the emphasis on a few control areas that have shown to be immediately effective against real-world attacks. Several other organizations have validated these as the highest-payback security controls. For example, SANS has listed five controls—the SANS "First Five"—as providing the most immediate increase in efficient and effective reduction in risk from advanced targeted attacks: 1) software whitelisting, 2) secure standard configurations, 3) application security patching, 4) system security patching and 5) minimization of administrative privileges.

The remainder of this document will focus on application control/whitelisting and privilege management.

Application Control/Whitelisting (Control 2)

The second highest-priority control is "Inventory of Authorized and Unauthorized Software." The action recommended by Control 2 is as follows:

> "Actively manage (inventory, track and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."

Actively managing which executables can run on a PC or server presents a high barrier to malware.

CIS Critical Security Controls Version 6.0 says actively controlling applications is important because

> "Poorly controlled machines are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws) or running malware introduced by an attacker after a system is compromised. … Managed control of all software also plays a critical role in planning and executing system backup and recovery."

Actively managing which executables can run on a PC or server presents a high barrier to malware—a positive approach to endpoint security—because only authorized software can run unhindered, while unauthorized software is either prevented from running or can run only with security policies applied.

Note that "actively managing" means more than doing a simple lockdown. Lockdown is where IT dictates which applications users can run, and users have no ability to install executables. While lockdown sounds like the most secure approach, the realities of today's business environment mean that lockdown invariably causes business disruption, leading to users bypassing lockdown through rogue or shadow IT efforts or to corporate management dictating so many exceptions to lockdown that the effort fails.

A step up from lockdown is "whitelisting," where IT approves a set of applications that users can run, consistent with licensing constraints. The success of whitelisting depends on the percentage of business-justified applications that are contained in the whitelist and how quickly IT can evaluate and add requested applications to the approved list. Keeping the approved list accurate and responsive can require high levels of IT staffing.

To address the operational difficulties caused by whitelisting, an alternative approach is to base each allow/block decision on file properties rather than a hash or signature of the executable. With this technique, a list of approved publishers and file owners is maintained, and all files from those sources are trusted. The file ownership is managed by the operating system, with the result that executables introduced into the system by users and other non-trusted sources cannot be executed, with the exception of executables signed by trusted publishers. Because a trusted publisher could produce a compromised executable, the list of trusted publishers should be minimal and restricted to highly trustworthy organizations.

Metrics for Application Control

A "Measurement Companion to the CIS Critical Security Controls (Version 6.0)" defines success metrics for each control. Metrics include counting the number of unauthorized applications that are on the network, how long it takes to remove them and the length of time to detect new software.[9]

Application control adds the ability to support a "gray list," where applications that are not on the whitelist (or blocked by simple blacklist approaches such as antivirus software) are allowed to run with security policies automatically applied to them. These policies can limit connectivity, privilege levels, times of use, etc. to reduce risk while allowing business needs to be met. This added flexibility has helped balance security, business demands and staffing levels.

Privilege Management (Controls 5 and 14)

In the Version 6.0 update, two control areas were elevated in priority because they provide a high level of risk mitigation against real-world attacks:

> **Control 5: Controlled Use of Administrative Privileges:** "The processes and tools used to track/control/prevent/correct the use, assignment and configuration of administrative privileges on computers, networks and applications."
>
> **Control 14: Controlled Access Based on the Need to Know:** "The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers and applications have a need and right to access these critical assets based on an approved classification."

[9] Center for Internet Security, Controls for Effective Cyber Defense V 6.0, download, www.cisecurity.org/critical-controls/download.cfm (token required)

Metrics for Privilege Access Controls

The "Measurement Companion to the CIS Critical Security Controls (Version 6.0)" defines success metrics for Control 5 ("Controlled Use of Administrative Privileges"), including how many unauthorized elevated operating system accounts are configured, which applications do not require two-factor authentication, changes in privileges and more. Measurements for Control 14 ("Controlled Access Based on the Need to Know") include the percentage of data sets for which access logging is not required and the percentage of business systems on which data loss prevention is not used.[10]

Both of those areas focus on preventing attackers from using administrative privileges or user access rights, raising the bar against both installing/executing software and reading/modifying sensitive data. Over-privileged accounts or widespread granting of administrative privileges are commonly exploited by attackers to cause severe business damage.

Similar to application control, privilege management done badly often causes unacceptable levels of business disruption. "Need to share" often violates simple "need to know" policies or group access controls. When restrictions are too static or complex, IT will need high levels of staffing to respond to requests for access or administrative privilege in a reasonable amount of time. Mechanisms are needed to allow limited exceptions to be granted during verification and to support user self-service approaches in low-risk cases.

Best Practice Deployment Guidelines

A common response to the Critical Controls and other efforts to define controls is to say that the controls are all well-understood security practices—nothing new. And that is true—but survey after survey, penetration test after penetration test and breach report after breach report show these basic controls were either not implemented or not maintained.

Conversely, enterprises and government agencies that avoid breaches or minimize the damage of advanced targeted attacks almost invariably have implemented controls such as "Application Control" and "Privilege Management" and have mature processes that both respond to changes in threat and meet business needs for flexibility and adaptability. Practices that such organizations tend to follow include these:

- **Get management and peer support before starting.** Change is difficult for all organizations, and increasing security does require change. Getting buy-in from both upper-level management and key peer organizations (such as IT, legal and business) is key to driving change. Proven ways to obtain buy-in and support for security change include the following three, in order of effectiveness:

    1. **Post-audit/breach report.** Unfortunately, change is always easier after a disaster. The best case is that another company in your industry suffers a breach, providing you with information about the root cause that helps you get approval for closing your gaps. The worst case (an after-action report from an external party investigating a breach at your company or agency) is an even more powerful catalyst, as is a negative audit report.

[10] Center for Internet Security, Controls for Effective Cyber Defense V 6.0, download, www.cisecurity.org/critical-controls/download.cfm (token required)

2. **Major business or IT transition.** Mergers and acquisitions often result in change to both business and IT operations as consolidation occurs. Major IT transitions (such as moving to Windows 10 or SaaS) also drive change. "Application Control" and "Privilege Management" can often be worked into these transition plans as part of process improvement.

3. **Compliance- or competition-driven.** Federal Information Security Management Act (FISMA), HIPAA, the North American Electric Reliability Corp. (NERC), PCI and every other compliance regime have requirements for "Application Control" and "Privilege Management." Case studies such as SANS What Works are documenting companies that are showing real business benefit from improvement in security in these areas.

- **Start smart.** Both "Application Control" and "Privilege Management" can be disruptive to business if implemented abruptly. Prior to any deployment of these controls, inventories of business-critical applications and access needs should be documented and understood. The first phase of deployment should be "monitor only": allow all operations to proceed without enforcement for at least a week, while potential enforcement actions are analyzed for potential disruption.

  The next step should be a small-scale prototype test with enforcement enabled, using only security and IT personnel and any motivated external volunteers. Once any process issues are shaken out, some problem users such as developers, managers and super-admins should be added to the trial.

- **Enforce when ready.** Once these trials have been completed and improvements made, management should announce that these features will be enabled on a certain date, **but you should not enable enforcement on that date.** Wait at least a week to see what complaints come in. You will be able to identify to management where organizational issues lie because enforcement has not even been activated. Only after resolving those issues should enforcement be enabled.

- **Minimize business disruption.** There will always be cases where risks need to be taken—an unknown executable absolutely has to be installed or a new user or business partner absolutely must have access. Processes and products should be chosen that support temporary exceptions, user self-service with alerting, enhanced monitoring of exceptions, etc.

- **Maintain effectiveness against threats.** All security controls in general, and "Application Control and Privilege Management" in particular, have value only when they reduce risk for the organization by increasing resistance to threats and exposures. As threats and IT/business practices evolve, these control strategies will need to be adjusted. Breach reports that involved compromised internal PCs should be analyzed to determine whether there are gaps in your processes and strategies.
- **Continuous monitoring.** The data provided by "Application Control" and "Privilege Management" controls can provide valuable data, both for adjusting controls to minimize business disruption and to detect new threat patterns or discern known indicators of compromise. All security controls should integrate to security information and event management (SIEM) or other analytic tools used by security operations.

Taking an incremental approach to deploying "Application Control" and "Privilege Management" fits the success pattern. Focus initial efforts on knowing which applications access critical business data, then tighten up access rights at the user level and application control at the server level. Use the lessons learned from there to assure a broader rollout that mitigates risk without causing unacceptable levels of business disruption.

About the Author

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTE, and service with both the National Security Administration, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems "and the occasional ballistic armor installation." John has testified before Congress about cyber security, was named one of the 15 most-influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank its sponsor:

AppSense®