TALON COMPANIES

WWW.TALONCOMPANIES.COM

www.talonexec.com www.taloncyber.com www.securestrat.com

Professional Risk & Security Management

PI License 18180 • PPO License 12194

151 Kalmus Drive Suite A-103, Costa Mesa, California 92626 • (800) 808-2566 Phone • (714) 434-7350

Cyber Security Audit Report

Prepared For:

State Center CCD

Prepared By:

Talon Companies

June 17, 2012

CONFIDENTIAL: State Center CCD

CONFIDENTIAL

Table of Contents

Statement of Purpose

The Cyber Security Audit was performed with the purpose of identifying technical security weaknesses and deficiencies by assessing State Center CCD's technical infrastructure's network environment, host- and network-based resources, and server-based platforms. The assessment activities, which represent a point-in-time examination, did not encompass business vulnerabilities stemming from the numerous facets of State Center CCD's operations or all the policies and procedures governing these operations.

The focus of the Cyber Security Audit surrounded searching for security weaknesses and deficiencies that negatively impact State Center CCD's information security posture so that they could be communicated as findings and recommendations as the results from the assessment efforts. The Cyber Security Audit did not serve to explore or communicate all of the components of State Center CCD's technical infrastructure that are operating strongly and without security weaknesses and deficiencies.

Executive Summary

Talon performed a Cyber Security Audit at the request of State Center CCD in conjunction with Alliance of Schools for Cooperative Insurance Programs (ASCIP). The primary objective of this Cyber Security Audit was to assess a core elements of State Center CCD 's technology infrastructure to identify and evaluate technical weaknesses, deficiencies, and vulnerabilities impacting their information security posture, as well as technical controls and mechanisms related to information security, so that recommendations could be defined to improve security and remediate security issues.

The Cyber Security Audit, which followed a robust methodology using advanced tools, as well as recent and up-to-date vulnerability research, demonstrated that State Center CCD's technical infrastructure is currently operating in a stable environment, functioning as intended, and does not possess any critical or high-risk security vulnerabilities that can be easily exploited by an attacker to directly breach security and compromise sensitive information assets. However, certain information security measures have not been enhanced to thwart attacks and safeguard information assets to their fullest potential. While State Center CCD is not being affected by any critical or high-risk security vulnerabilities that directly place their technical infrastructure in immediate jeopardy, the lower risk security weaknesses uncovered during the course of the Cyber Security Audit should be addressed to minimize the likelihood that they will be leveraged to breach security, access sensitive information assets, or cause a denial of service attack.

It is important to note that the lower risk security weaknesses impacting State Center CCD's network environment are not systemic in nature and do not severely jeopardize the confidentiality, integrity, or availability of their technical infrastructure or information assets through the presence of easily exploitable security vulnerabilities. As such, State Center CCD has been shown to be demonstrate due diligence surrounding information security and their information security risk management program.

The Cyber Security Audit has clearly demonstrated that meaningful improvements towards addressing information security proactively have been undertaken and are directly contributing to the strength and robustness of State Center CCD's security posture, as well as the effectiveness of the security mechanisms currently in place within their technical infrastructure. State Center CCD will be able to further enhance their ability to neutralize threats and safeguard information assets by adopting the recommendations communicated in the form of this report surrounding the lower risk security weaknesses that the Cyber Security Audit uncovered.

Engagement Phases

The Cyber Security Audit performed in support of State Center CCD consisted of an overarching and integrated iterative approach that combined manual and automated technical information security survey and assessment activities.

The Cyber Security Audit began with reconnaissance and baseline testing to obtain an understanding of State Center CCD's technical infrastructure's components and current security

mechanisms from an external perspective. These external activities escalated to the performance of penetration tests and attack simulations in an attempt to exploit security vulnerabilities to explicitly demonstrate how someone or some event can violate the technical infrastructure's integrity, confidentiality, and/or availability.

This initial phase was followed directly by thorough evaluations of a sampling of State Center CCD's architecture and the hosts and resources contained within their network environment from an internal perspective. In doing so, it was possible to search for and explore specific security weaknesses, deficiencies, and distinct vulnerabilities.

Upon completion of the above described analysis and evaluation efforts, Talon assembled this Cyber Security Audit report to convey the findings and recommendations that stemmed from these activities.

Engagement Limitations

The Cyber Security Audit techniques and activities employed, although thorough, possess limitations that restrict the comprehensiveness of the overall findings and conclusions. As the evolution of new security vulnerabilities and methods to exploit security flaws is highly dynamic, the Cyber Security Audit does not represent a comprehensive evaluation of State Center CCD's security posture, as the findings only reflect the point-in-time in which the Cyber Security Audit activities were conducted and will not provide information about security vulnerabilities discovered or publicly released after the Cyber Security Audit was performed.

The Cyber Security Audit did not include Social Engineering attacks designed to exploit the recognized greatest security weakness, the human element. Additionally, no Denial of Service attacks were launched to shut down or disrupt the ability for the technical infrastructure to function normally.

Summary Findings

The Cyber Security Audit has identified that State Center CCD is directly minimizing the likelihood of a successful security incident perpetrated by an attacker by effectively utilizing security controls and reducing the number and type of targets for attack that they present. In light of this, no high-risk or easily exploitable critical security vulnerabilities were identified and it is clear that State Center CCD's technical infrastructure has been designed in a security conscious manner that effectively neutralizes a wide array of common security vulnerabilities.

As lower risk security weaknesses and deficiencies were uncovered during the Cyber Security Audit that impact State Center CCD's technical infrastructure, the following summary findings provide a high-level illustration of these security vulnerabilities and weaknesses that degrade State Center CCD's security posture, which are further detailed in Section 2 of this report:

1. Unnecessary Services Running – The presence of unnecessary services in operation and the associated ports of these services being open presents a target of opportunity for an

attacker to focus on and attempt to compromise security weaknesses to bypass security controls and gain unauthorized access.

2. Lack of Patches – Systems within State Center CCD's network environment are currently operating without the most current and up-to-date patches applied, including security fixes that mitigate software flaws and other security issues.

Summary Recommendations

In response to the Cyber Security Audit's identification of select security issues that degrade State Center CCD's security posture and certain deficiencies hampering the security readiness of key elements of State Center CCD's network environment, methods to resolve identified security issues were developed through the form of tactical recommendations. Adoption and implementation of the recommendations outlined in this report will allow State Center CCD to garner an immediate improvement towards operational security effectiveness and efficiency. The following summary recommendations will serve to govern the mitigation of security vulnerabilities degrading State Center CCD's security posture:

1. Reconfigure select systems to remove unnecessary services and close their associated open ports, while enhancing logging capabilities to capture and record system-based activity.
2. Enable firewalls on Windows Servers to restrict remote accessibility and minimize the exposure of services that remain in operation and their associated open ports
3. Apply missing patches and establish a patch management system so that resources within State Center CCD's network environment do not remain in use for extended periods of time after security patches and other fixes become available.

Conclusion

The Cyber Security Audit has identified that State Center CCD has and is taking distinct actions to manage risk, enhance security, and implement effective information security controls and mechanisms. The results of the Cyber Security Audit demonstrate State Center CCD's understanding that achieving and sustaining a strong information security posture is a priority to protect critical digital assets. While the presence of lower risk security weaknesses and deficiencies do slightly degrade State Center CCD's security posture, these security vulnerabilities are not systemic in nature and do not jeopardize the intrinsic trustworthiness of State Center CCD's technology infrastructure. The remediation activities and findings laid out in this report will aid in the direct mitigation of both external and internal security weaknesses, deficiencies, and vulnerabilities and will significantly improve upon State Center CCD's overall information security posture.

Section 1 – How to use this Report

1.1 Purpose

Talon is committed to providing quality analysis regarding information security. Every effort has been made to ensure the accuracy, precision, and reliability of the information within this Cyber Security Audit report. However, as the nature of information security is highly dynamic and ever-changing, it is strongly recommended that State Center CCD address the security issues presented in this report in a timely manner.

This report is designed to convey reasonable and applicable solutions for addressing and mitigating the identified security weaknesses and deficiencies. The recommendations are based upon industry best practices, proven methodologies, and extensive experience, and are designed to specifically fit the perceived needs of State Center CCD.

State Center CCD assumes all responsibility for the use or misuse of information presented in this report.

1.2 Findings Key

A rating system was utilized to indicate the level of severity and communicate the dynamics of the findings identified during the Cyber Security Audit.

For a detailed breakdown of the Findings Key utilized, please see Appendix A.

Section 2 – Network- & Host-Based Security Findings

During the course of the Cyber Security Audit, an array of distinct activities were undertaken to identify network- and host-based security weaknesses, deficiencies, and vulnerabilities impacting State Center CCD's technical infrastructure. In doing so, multiple facets of State Center CCD's technical infrastructure were assessed, including the network environment, host- and network-based resources, server-based platforms, and other components that constitute State Center CCD's architecture. Although activities were performed to isolate any major high-risk security weaknesses or vulnerabilities, Talon did not identify any such security weaknesses or vulnerabilities were negatively impacting State Center CCD's technical infrastructure. Rather, only lower risk areas of concern were uncovered and by addressing the following findings and adopting the tactical recommendations, State Center CCD will manage the risk they are exposed to.

Finding 2.1 – Unnecessary Services Running

Risk Factor: Low
Complexity: Medium
Popularity: Widespread
Impact: System Integrity, Confidentiality, Availability
Root Cause: Misconfiguration
Ease of Resolution: Trivial

Description:

Network-wide sweeps and direct per system verification have confirmed that the network resources are operating with unnecessary services running and their subsequent ports are open and exposed. Specifically, key network devices are operating with a dramatic reduction in their security posture.

Security Concern:

These unnecessary services and open ports create a wealth of security vulnerabilities and greatly increase the risk of a successful security breach against State Center CCD's network environment. These services can be used to cause serious Denial of Service attacks and directly compromise network resources, placing State Center CCD at significant, unnecessary, and preventable risk.

A selection of the unnecessary services in operation are daytime, echo, chargen, discard, terminal services, and telnet.

Recommendation:

It is strongly recommended that the configuration principle "deny first, then allow," be utilized, meaning that as many services and applications as possible must be turned off at all times and then selectively turned on only when essential.

If not necessary to remain in operation, Telnet should be disabled on the systems located at IP addresses 198.189.22.1, 10.6.4.1, 10.6.4.2, 10.128.4.2, and 10.128.4.1. Additionally, terminal services should be disabled at 205.155.151.40 and daytime, echo, chargen, discard should be disabled at 198.189.22.1.

State Center CCD should define the particular services that are authorized to remain in operation, as well as their associated open ports, and perform an enterprise wide rule enforcement to ensure all unnecessary services are suspended and their associated open ports are closed.

Finding 2.2 – Lack of Patches

Risk Factor: Medium
Complexity: Medium
Popularity: Popular
Impact: System Integrity, Confidentiality, Availability, Authorization, Intelligence
Root Cause: Misconfiguration
Ease of Resolution: Medium

Description:

Patching is an integral part of any information security program, especially on Windows based systems where new patches are issued frequently. While adequately patched in certain areas, State Center CCD's resources are missing patches throughout the network environment. While some of the missing patches address stability and performance issues, key missing patches are designed to address susceptibility to security breaches and should be addressed.

Security Concern:

As a result of unpatched systems operating within the technology infrastructure, internal resources are susceptible to a wide range of security vulnerabilities. However, it is important to note that other security mechanisms in place within State Center CCD's infrastructure minimize the exposure and likelihood that these security vulnerabilities can be exploited. Nevertheless, the security vulnerabilities stemming from missing patches place resources within State Center CCD's network environment at unnecessary risk, as patches protect against many of the widely utilized security exploits and attack techniques.

Recommendation:

The most current and up-to-date patches, updates, and service packs should be immediately applied and properly configured to directly address the associated security vulnerabilities.

In light of the large numbers of computers workstations and servers in operation within State Center CCD's network environment and the frequency of newly released patches, the task of monitoring for the release of new patches and applying them is a cumbersome undertaking. As such, this process could be greatly enhanced by adopting an automated patch management system. Such a system would be able to deploy the appropriate patches throughout State Center CCD's network environment without manual interaction and avoid having State Center CCD's personal deploy patches on a system by system manually.

It is recommended that all patches to be deployed on mission critical servers be tested on a development system, if possible, before applying them to the live production systems. Furthermore, such patching should be done during a period of light network activity, as complications may arise. After the patches are installed, the updated servers will need to be tested to ensure no functionality was lost due to an update patch.

In addition to the lack of general Window's passwords, the Cisco security camera recording device located at 10.96.4.135 was found to be operating with an old version of Squid. Additionally, the system located at 205.155.151.40 should be patched in light of the presence of terminal service and the system SWIAS04B located at 10.160.32.57 and SRCCLASS located at 10.64.4.105 require updating to mitigation an Apache Mod_ssl vulnerability. Also, the system located at 10.136.4.1 should be updated to it only accepts Version 2 ssh connections and not Version 1 and the system located at 205.155.151.43 requires patching to mitigation a SSL brute force attack susceptibility.

Appendix A: Findings Key

The following findings key was utilized in this report to rate and quantify findings that constitute a direct risk to State Center CCD:

Risk Factor: The level of severity of a vulnerability

The rating system utilized in this report represents the indicated level of severity of the findings identified during the assessment activities. All findings are vulnerabilities that were analyzed and constitute a direct business risk to overall network environment.

Critical: This type of vulnerability is of critical importance and requires immediate attention.

High: This type of vulnerability is important and should be addressed as soon as is practical.

Medium: This type of vulnerability is moderately important and should be addressed in a timely manner.

Low: This type of vulnerability is only communicated for informational purposes at this time. They should be addressed the next time major reconfiguration of the host or network is performed.

Complexity: The difficulty involved in exploiting a vulnerability

All attacks against computer systems are not equal, as some are much more complicated than others are. Exploiting a vulnerability in a WWW CGI program may include simply inserting a "magic" character in form field, while other attacks may require a discreetly coordinated series of interactions with obscure network services. The intricacy level of an attack has a greater effect on the likelihood that it will be defended against, rather than the probability that it will be utilized by an attacker who most likely possesses an arsenal of complex attacks that can be used against a computer system. Additionally, the most elaborate attacks are often the most popular.

Low: A low-level attack can be committed by an untrained attacker, often through the use of standard Unix utilities or by using their web browser, although he/she does not possess any special tools. The problems caused by such an attack are often obvious to individuals without specific knowledge of computer security.

Medium: Specific software that is generally quite simple to use and understand, even by a novice attacker, is necessary to exploit a medium-level attack. Individuals who do not have specific knowledge about security or the attacker underground are less likely to be able to exploit such a vulnerability.

High: To commit a high-level attack, an exploit code must be utilized, which is difficult to write and requires access and knowledge of specific types of computer systems. Utilizing such a tool may also require specific knowledge of the vulnerability and the system on which it is present.

Popularity: The likelihood that a vulnerability will be exploited

The identification of obscure, intricate vulnerabilities may not be a strong indicator that a computer system has already been compromised; however, the presence of well-known, widely exploited problems may act as an immediate cause for alarm.

Obscure: An obscure attack is one that is not widely known or understood, and they are more likely to affect services that are also not well understood or require understanding not often known by casual attackers.

Widespread: A widespread attack is one that has been published and is widely known to attackers, however, they are not often the first form of attack against a system, as they are often difficult to exploit.

Popular: A popular attack is one that has been published, generally in underground computer publications or by "hacker" newsgroups, and are most often utilized by novice attackers and automated attacker tools. A computer system that is attacked is often done so because an attacker has identified the system's vulnerabilities by casually scanning large numbers of arbitrary addresses for vulnerable hosts.

Impact: The specific threat posed by a vulnerability

When a computer system becomes exposed to a security threat, it poses an unnecessary risk to the overall organization. Certain security issues are more serious than others, and the most threatening should be addressed before the more minor issues. This report breaks down the implications of each vulnerability into numerous categories, each representing the threats posed by the security vulnerabilities.

System Integrity: When an attacker gains complete control of the computer system's functioning, the entire system becomes compromised. This occurs when an attacker gains a shell access to the system and is able to execute arbitrary commands, as well as the ability to modify arbitrary files on the system, therefore reconfiguring it.

Confidentiality: Most computer systems retain highly sensitive information as a result of user privacy or organizational secrecy requirements, including the secure storage of email, financial data, and proprietary software. An attacker is able to gain access to this sensitive information when threats to confidentiality occur.

Availability: It is important for the computer system to remain available to its valid users by running smoothly and with moderate, anticipated performance. Attacks that occur and that compromise this availability are known as Denial of Service attacks.

Accountability: Many computer systems are capable of logging user actions, therefore, the actions taken by an attacker can often be traced back to the source. Systems that put a name to

the activities of system users are said to provide accountability and, because accountability often acts as a deterrent to attacks, disarming these capabilities is often a priority for attackers.

Authorization: Most authorized users are only given enough access to the computer systems to complete their necessary work and are not given the ability to directly manage the operation of the entire computer system. The authorizations of users' activities are tracked through the use of specific mechanisms for each computer system.

Data Integrity: It is necessary for data maintained by computer systems to remain correct and legitimate, as it is integral to the utilization of many applications in which incorrect information can be legally, financially, or even medically calamitous. Attackers who attempt to illegally alter information retained on a computer system are most often targeting the integrity of its data.

Intelligence: Before attempting to strike, many attackers gather information regarding targeted systems in order to increase their odds of successfully breaking into a system, as this often amplifies the rewards made available by such an attack. Attackers who collect information about a system prior to actually intruding impact intelligence.

Root Cause: The underlying cause of a vulnerability

By taking proactive security measures and maintaining security awareness in the planning and design stages of network engineering, many security issues can be averted. However, security issues can arise as the result of poor operational practices, often due to a lack of security focus by network administration. It is important to identify the root causes of the vulnerabilities discovered in a network to allow for patterns of such vulnerabilities to be distinguished.

Misconfiguration: When a component of the computer system is misconfigured, such as if default configuration values remain present, available access control mechanisms have not been enabled, or extensions have been made to the system that violate security, additional vulnerabilities can be created.

Software Implementation Problems: The vulnerability exists due to a bug in a program deployed in the system. Prior to the initial discovery of this security problem, there was no way for an organization to be aware of this problem, and, unless the vulnerable software is removed or restricted from normal users, the only way to fix the problem is to apply vendor patches.

Insecure Design: The vulnerability exists because the service implemented by the problematic software is fundamentally insecure, the design of the software neglects security concerns, or the protocol implemented by the software is inadequate. Similar software solutions for this service may have equivalent vulnerabilities, and there may not be any obvious way to defend against the threat without disabling the service provided by the vulnerable software.

Architecture Deficiency: Unnecessary risk is placed upon the network environment due to a security deficiency or gap involving the architecture or topology of the technology infrastructure. Such a deficiency, which may be resolved by modifying or applying architectural changes, amplifies collateral security issues and simplifies attempts to breach security.

Ease of Resolution: The simplicity of fixing a vulnerability

When faced with a large number of serious vulnerabilities, it is important that security problems be solved as efficiently as possible. Because some problems are easier to solve than others, quickly addressing the easy problems first may rapidly increase the security of a vulnerable system. Additionally, fixing some problems poses risks of disrupting services, and resolution for those problems may thus require careful scheduling.

Trivial: The problem can be resolved quickly and without risk of disruption by reconfiguring vulnerable software.

Simple: The problem might be solved by significant reconfiguration of the vulnerable system, or by a vendor patch. Minimal risk of disruption to services is present, but conscientious and immediate effort to resolve the problem is reasonable.

Moderate: The problem requires a vendor patch to solve and presents a significant risk of service disruption. It is possible that resolution of this problem may require an upgrade to a substantially different version of software, or that the reconfiguration required to solve the problem has far-reaching impact on legitimate users.

Difficult: The problem requires either an obscure, hard-to-find vendor patch to resolve, or requires manual source code editing to fix. Substantial risk of service disruption makes it impractical to solve this problem for mission critical systems without careful scheduling.

Infeasible: This problem is due to a design-level flaw, and cannot be resolved by patching or reconfiguring vulnerable software. It is possible that the only way to address this problem is to cease using the vulnerable software or protocol, or to isolate it from the rest of the network and eliminate reliance on it completely