From: Todd Stefan [[tstefan@taloncyber.com](mailto:tstefan@taloncyber.com)]

Sent: Thursday, April 19, 2012 10:40 PM

To: John Bengtson

Cc: Ed Eng; Don Lopez; Gary Sakaguchi; Phil Nelson; Russell O'Donnell ([O'Donnell@ascip.org](mailto:O'Donnell@ascip.org)); Kevin Hobby ([Hobby@ascip.org](mailto:Hobby@ascip.org)); Gregory Taylor; Harry Zahlis; Teng Her; Charlie R. Lochbaum

Subject: Initial Findings - Cyber Audit of SCCCD

Hi John,

The Cyber Security Audit has continued to proceed smoothly and I am pleased to let you know that our efforts thus far are validating the strength and resiliency of key components of your technical infrastructure and that your systems are not being negatively impacted by serious security vulnerabilities or deficiencies.

While many of the subnets we have surveyed thus far do not contain any systems or very few systems, those systems that are present within the subnets we have surveyed thus far only possess minor security issues, if any at all.  As we spoke about, our lack of domain admin privileges prevents our ability to audit key resources in great detail and, as such, our focus has been on penetration testing and detecting exploitable security weaknesses.  In doing so, one security weakness we have detected entails missing patches.

Patching is an integral part of any information security program.

While many of the systems we evaluated are adequately patched, we uncovered systems that were not operating with the most up-to-date version.  As patches are often designed to address stability and performance issues, it is possible that missing patches are designed to address susceptibility to security breaches.  The potential issues that stem from missing patches can be mitigated by applying the appropriate patches, updates, and service packs.

A specific example of this is Squid operating at IP 10.96.4.135, which is susceptible to multiple vulnerabilities and denial of service attacks.  The updated version of Squid does not possess these same susceptibilities.  Additionally, this same IP address allows SSH v1 connections, which should be disabled.

In addition to missing patches, we have detected the presence of unnecessary services and open ports.  Such unnecessary services and open ports present an increase in the risk of a successful security breach against SCCCD's network environment as they present an avenue of attack and a means for an attacker to communicate with SCCCD's network resources.  The unnecessary services can be used to cause serious Denial of Service attacks, gather sensitive technical information that could be used to facilitate a security breach, and directly compromise network resources, placing SCCCD at unnecessary risk.  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.

As our Cyber Security Audit activities continue, we will be evaluating resources located in subnets not yet surveyed, as well as working to delve deeper with the analysis of key servers.

In summary, the Cyber Security Audit has clearly validated that meaningful improvements towards addressing information security proactively have been undertaken and are directly contributing to the strength and robustness of SCCCD's security posture, as well as the effectiveness of the security mechanisms currently in place within their technical infrastructure.

Talk to you soon.

Todd Stefan

Talon Cyber Tec

151 Kalmus Drive Suite A-103

Costa Mesa, California 92626

Office: (800) 808-2566

Direct: (323) 243-9928

Fax: (714) 434-7350

[tstefan@taloncyber.com](mailto:tstefan@taloncyber.com)

[http://www.taloncyber.com](http://www.taloncyber.com/)