



CSOinformer
Volume 1, Number 10
June 10, 2003
Edited by Jim Reavis
jim@csoinformer.com

Welcome to CSOinformer, the monthly newsletter briefing for information security professionals. This is a special reprint for the Center for Internet Security.



Talking to – *Clint Kreitner, the Center for Internet Security*

Clint Kreitner is the President and CEO of the Center for Internet Security. The Center is a not-for-profit cooperative focused on improving the security of Internet-connected computer systems. Clint has previously been president of a multi-hospital region of Adventist Health System and member of its Board of Directors, founder and president of two computer software and services firms, Director of Computer Aided Ship Design for the Navy and Director of the Design Division of the Pearl Harbor Naval Shipyard.

Q. What is the Center for Internet Security's vision and mission?

A. The CIS mission is to create detailed operational security best practices and foster widespread adoption of these practices. Our vision is a global Internet comprised of systems that have been secured to a much higher ambient level than is currently the case.

Q. How does the consensus process work? Who are the stakeholders?

A. CIS functions as a convening and facilitating mechanism. Our members, who are all users, establish priorities as to which target environments (Windows NT, 2000, XP, 2003,

Solaris, Linux, CISCO IOS, etc) to work on. Once a target environment is identified, a benchmark development team is formed from CIS members. They begin with whatever security hardening guidance is available, and develop the benchmark from there, based on technical consensus among the team members. The team members communicate via email and conference calls. Once team consensus is reached, the proposed benchmark is disseminated to CIS members for their input and comment. After incorporating that input, the benchmark and associated scoring tool are published via the CIS website.

The stakeholders doing the work are the CIS members. The stakeholders benefiting from the results of that work are all users around the globe who download and implement the CIS benchmark settings. The benchmarks and the associated scoring tools are available to everyone from the CIS website free of charge.

Q. Are government initiatives such as the National Strategy to Secure Cyberspace and the new Homeland Security department helping your mission?

A. They are helpful from the standpoint that they emphasize the importance of good IT security.

It is noted that the CIS effort directly supports three of the five priorities of the National Plan:

- (1) vulnerability reduction,
- (2) securing government systems
- (3) international cooperation.

Q. How do consensus baseline settings benefit organizations?

A. A number of recent studies have shown that implementing the security settings in the CIS benchmarks reduces the vulnerabilities identified by commercial scanners on "out of the box" systems by around 90%.

See

http://iac.dtic.mil/iatac/news_events/pdf/Vol5_N03.pdf for a report by the Defense Department for articles on some of these studies. Other studies are reported on the CIS website.

Q. What is the difference between baselines and standards?

A. We use the term benchmarks rather than standards to acknowledge the fast track process used in developing them, as distinguished from the more drawn out process most people think of when referring to standards.

The CIS benchmarks are stratified into Levels. Level I settings represent a minimum baseline level of security that is better than typical vendor defaults, but not as good as the Level II Gold Standard benchmarks, which represent a stronger level of security. Level I benchmarks are designed so that breakage of common applications is not likely.

About

CSOinformer is a service of Reavis Consulting Group. All content, unless otherwise noted, is the sole property of Reavis Consulting Group. Please send all inquiries to:

newsletter@csoinformer.com
www.csoinformer.com

Q. Once an organization has identified the holes they have in baseline compliance, how do they efficiently close the gap?

A. The scoring tools are designed to do just that - identify which of the benchmark settings have not been made on a particular system. After implementing the settings in a Level I benchmark, users can begin to implement the tighter settings in the Level II benchmark, being careful that additional security settings don't interfere with production operations.

Q. Take the recent Slammer worm for example, what was the difference between the impact on an organization that was not using consensus baselines versus one that had it fully implemented?

A. Simply put, users who had implemented the appropriate CIS benchmark were protected from the Slammer worm.

Q. What future areas do you think require consensus baselines?

A. We are anxious to develop security hardening guidelines for widely used application products being used on CIS benchmark secured operating systems.

Q. Do you see the Center getting beyond driving consensus baselines into other areas?

A. For now, there is plenty to do in the application and appliance arena.

CIS can be found online at www.cisecurity.org

Reavis Consulting Group
2553 Crescent St
Ferndale, WA 98248
(360) 739-9629

CSOinformer is released on the second Tuesday of each month. 12 month subscriptions cost \$89 USD. Corporate site licenses are available.