CERT’S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

NIST Catalog of Security and Privacy Controls, Including Insider Threat

Key Message: Security controls, including those for insider threat, are the safeguards necessary to protect information and information systems.

Executive Summary

“The selection and implementation of security controls for organizations and information systems are important tasks that can have major implications on the operations and assets of organizations as well as the welfare of individuals and the Nation. Security controls are the safeguards/countermeasures employed within organizational information systems to protect the confidentiality, integrity, and availability of the information systems and the information that is processed, stored, and transmitted by those systems.” [1]

In this podcast, Dr. Ron Ross, with the U.S. National Institute of Standards and Technology (NIST), discusses major updates to NIST Special Publication 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*. Ron is the Project Leader for the FISMA (Federal Information Security Management Act) Implementation Project. Ron is joined by Joji Montelbano, a member of the Insider Threat team at CERT. Joji discusses the recommendations that his team made for control updates and additions to NIST SP 800-53.

PART 1: EVOLUTION OF NIST SPECIAL PUBLICATION 800-53

Background and Scope

NIST SP 800-53 was one of the original guidance documents that NIST was asked to develop in response to the Federal Information Security Management Act of 2003 (2002).

Its publication in 2005 was preceded by the development of FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* and FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems*.

NIST SP 800-53 is a security and privacy controls catalog. It covers:

- safeguards and countermeasures
- management, operational, and technical controls
- for information systems and their operational environments

Revision 3

The most historic revision prior to Revision 4 was Revision 3 (August 2009). NIST partnered with the US Department of Defense and the Intelligence Community under the Office of Director of National Intelligence and in collaboration with the Committee on National Security Systems.

Revision 3 included security controls for both national and non-national security systems.

Revision 4

This revision was the most extensive NIST has ever done. It involved the first public call for input. The drivers for this revision included the following:

- the evolving threat landscape: nation-state threats, organized crime, terrorists, and hactivists
- availability of empirical attack data: attack origins, composition, targets, capabilities, and intent
- gaps in insider threat, application security, and advanced persistent threat
- trustworthiness and assurance of information systems, during development and during operations via continuous monitoring

NIST received over 1000 comments.

Evolution of the Use of NIST SP 800-53

The first catalog described a set of baseline security controls, a starter set. The intent was that these be applied to the three categories of systems defined in FIPS 199 – low, moderate, and high impact. Impact describes the potential adverse effects on an organization's mission if that system is compromised or breached.

Typically baseline controls were implemented without much change. The catalog of controls has expanded from 600 controls to 850 controls, so some level of specialization is now required when developing a security plan.

Security plans and controls are being tailored to address specific missions, technologies, and operational environments. Examples include a military tactical overlay for military operations in combat environments, operations in space, and operations of nuclear power plants.

PART 2:RECOMMENDED INSIDER THREAT CONTROLS BASED ON MORE THAN 500 CASES

CERT Insider Threat Recommendations

CERT insider threat recommended practices and controls derive from over 500 cases of actual insider attacks.

Recommendations for updates to NIST SP 800-53 were developed in response to the question "If organizations were to implement these controls, would they be more able to mitigate insider threats?"

CERT staff provided recommendations for 10 NIST SP 800-53 control families (AC, AT, AU, CA, CM, DP, PE, PS, SA, SI) and 20 controls across those families. Recommendations ranged from technical controls to enterprise, organization-level controls and focused on:

- access control: for example, increased emphasis on controls for shared accounts, given these are often used by insiders to launch their attacks to hide their tracks. Shared accounts often provide privileged access.
- personnel security: for example, increased emphasis on interdepartmental communication among human resources, legal, and physical security and with IT and information security. This is particularly important when a staff member is terminated and their account is not immediately deactivated, which provides them with remote access.

CERT staff also recommended a new control for the Project Management (PM) family – the creation of an insider threat program. The Office of Management and Budget mentions this in Memorandum M-11-08. Executive Order EO-13587 calls for an insider threat program to help safeguard classified data.

PART 3: DEVELOPING REVISION 4 AND BEYOND; MONITORING CONTROL EFFECTIVENESS

Revision Process

NIST uses a disciplined, structured process for reviewing public comments as follows:

- Every team member reviews each comment and provide a recommendation.

Dr Ron Ross provides his recommendation, review all team input, and works to develop a consensus solution (make a change, reject the comment, etc.).
- A markup of Revision 3, which becomes Revision 4, is developed and released for public review by federal agencies, the private sector, and reviewers worldwide.

Addressing Insider Threat

The series of WikiLeaks incidents highlighted the need to pay more attention to insider threat. As NIST was reviewing CERT's recommendations, they asked themselves "Would these kinds of changes have stopped something like WikiLeaks?" and concluded that they would.

Advanced persistent threat also emphasizes the importance of an insider threat program. If boundary safeguards fail, organizations have a greater ability to detect, respond, and limit damage once the attack is detected.

How Do We Know Controls Are Effective?

NIST's philosophy is to "build it right initially and then continuously monitor over time to ensure the security state of your system and your environment of operations is maintained."

NIST constantly monitors the types of attacks and implemented controls in collaboration with the DoD and the Intelligence Community and collects empirical data. Successful attacks indicate that the current set of controls are not effective, we don't have the right controls, or we need additional, stronger controls.

CERT insider threat staff work closely with the Department of Homeland Security Federal Network Security and other customers to determine how insider threat controls are working. They share their insights with NIST.

Future Plans

NIST plans to release the next verions of SP 800-53 Revision 4 in the July 2012 timeframe. There may be a final draft based on the number of comments received during this public review process.

NIST plans to maintain a two-year update cycle. Revision 5 will not be nearly as extensive.

Going forward, NIST will focus on:

- enterprise-wide control integration, implementation, and communication
- the overlay concept: developing specialized security plans for specific missions, environments of operation, or technology (for example, cloud computing and mobile devices)

Resources

[1] National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, February 2012.

NIST Computer Security Division Computer Security Resource Center Publications website

NIST CSD CSRC Special Publications website

CERT Insider Threat website

CERT podcasts on insider threat

- Indicators and Controls for Mitigating Insider Threat (January 2011)
- Mitigating Insider Threat: New and Improved Practices (August 2009)
- Insider Threat and the Software Development Life Cycle (March 2008)
- Protecting Against Insider Threat (November 2006)