New NIST report advises: Securing critical computer systems begins at the beginning

August 4 2010

Nothing beats the feeling of starting up a new computer - be it a laptop, desktop or a major, custom-designed computing system. A new system is a blank slate with no worry of botnets, viruses or any other cybersecurity hazards.

Not so, explains computer researcher Marianne Swanson at the National Institute of Standards and Technology (NIST), lead author of a draft report, Piloting Supply Chain Risk Management for Federal Information Systems. Information systems and components are under attack throughout the supply chain from the design phase—including specification and acquisition of custom products—through disposal. "Computer systems are under attack before installation by adversaries enabled by growing technological sophistication and facilitated by the rapid globalization of our information system infrastructure, suppliers and adversaries," Swanson says.

NIST has released a public draft of the new report for comment.

The supply chain report is geared to information systems that are categorized as "high-impact level," systems for which the loss of confidentiality, integrity or availability could be expected to have a "severe or catastrophic adverse effect on organizational operations, organizational assets or individuals."* The report provides an array of practices designed to help mitigate supply chain risk throughout the life cycle, not just on accepting systems and products "as they are" and managing risks after delivery. The practices are based on security procedures found in NIST special publications, and those from the National Defense University and the National Defense Industry Association, and these are expanded to include implementations specific to mitigating supply chain risk.

Typical examples of good practices recommended in the report include integrating information security and supply chain requirements from inception of the project, protecting the supply chain environment, hardening the supply chain delivering mechanisms and configuring the product to limit access and exposure.

Other recommendations:

- Ensure your information system security, acquisition personnel, legal counsel, and other appropriate advisors and stakeholders are participating in decision making from system concept definition through review and are involved or approving each milestone decision.
- Ensure the proper funding is allocated for information system security and supply chain risk management
- Follow consistent, well-documented processes for system engineering and acquisition
- Provide oversight of suppliers
- Audit the development process
- Perform quality assurance and control of security features
- Assign roles and responsibilities and follow them

- Fully implement the tailored set of baseline security controls in NIST Special Publication 800-53** appropriate to the system's impact level.

The supply chain security report is intended for information system owners, acquisition staff, information security personnel and systems engineers.

More information: * Categorizing system impact level is described in a NIST document, Standards for Security Categorization of Federal Information and Information Systems (Federal Information Processing Standards Publication 199), available on-line at csrc.nist.gov/publications/fip … PS-PUB-199-final.pdf
** Recommended Security Controls for Federal Information Systems and Organizations (Rev. 3), available on-line at csrc.nist.gov/publications/nis … rrata_05-01-2010.pdf

Provided by National Institute of Standards and Technology

Citation: New NIST report advises: Securing critical computer systems begins at the beginning (2010, August 4) retrieved 24 April 2024 from https://phys.org/news/2010-08-nist-critical.html