International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

BASIC PRINCILPLES TO IMPROVE IT SECURITY OF AN ORGANISATION

T. Narsimhappadu[#1] and R.SeethaRam[*2]

[#]*Asst. Professor, Department of CSE, UshaRama College of Engg & Tech, Telaprolu, Vijayawada, A.P., India*

[*]*Asst. Professor, Department of CSE, St. Mary's College of Engg for Women,Budampadu, Guntur, A.P., India*

Abstract— — Private businesses and government agencies, both foreign and domestic, are becoming increasingly reliant on information technology to fulfil many basic functions. Businesses are making changes simply to remain competitive in the changing global marketplace. Likewise, government agencies are seeking to provide better service to their citizens. Regardless of the reason, the move to a digital economy has caused information and information technology to become valuable business assets that need to be protected. With this development has come the recognition that fulfilling these basic functions requires as a matter of course comprehensive, well-designed, and reliable information system security programs. Information system security program standards, guidance, and implementation strategies have been, or are being, developed by public and private sector organizations in the United States and abroad. These wide-ranging efforts are designed to address many aspects of information security at many levels of detail. They address technology aspects such as public key infrastructure (PKI) and certification and accreditation (C&A) processes, and more operational aspects such as organizational good practices. In this paper, we discussed the security principles which are very potential to become common fundamentals for users, designers, and engineers to consider in designing information system security programs.

Index Terms— Security Policy, portability, interoperability, mission critical resources

I. INTRODUCTION

The purpose of the Engineering Principles for Information Technology (IT) Security (EP-ITS) is to present a list of system-level security principles to be considered in the design, development, and operation of an information system. Ideally, the principles presented here would be used from the onset of a program—at the beginning of, or during the initiation phase—and then employed throughout the system's life-cycle. However, these principles are also helpful in affirming and confirming the security posture of already deployed information systems. The principles are short and concise and can be used by organizations to develop their system life-cycle policies. Securing information and systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. This is due to the highly interactive nature of the various systems and networks, and the fact that any single system cannot be adequately secured unless all interconnecting systems are also secured. By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. Through user training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, layered protections enable effective protection of information technology for the purpose of achieving mission objectives.

To aid in designing a secure information system, NIST compiled a set of engineering principles for system security. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed. While the primary focus of these principles is the implementation of technical controls, these principles highlight the fact that, to be effective, a system security design should also consider non-technical issues, such as policy, operational procedures, and user education and training.

The principles described here do not apply to all systems at all times. Yet, each principle should be carefully considered throughout the life-cycle of every system. Moreover, because of the constantly changing information system security environment, the principles identified are not considered to be a static, all-inclusive list. Instead, this document is an attempt to present in a logical fashion fundamental security principles that can be used in today's operational environments. As technology improves and security techniques are refined, additions, deletions, and refinement of these security principles will be required

II. SYSTEM LIFE-CYCLE DESCRIPTION

The five life-cycle planning phases used are defined in the Generally Accepted Principles and Practices for Securing Information Technology Systems.

Initiation Phase

Development/Acquisition Phase

Implementation Phase
Operation/Maintenance Phase
Disposal Phase.

Initiation: During the initiation phase, the need for a system is expressed and the purpose of the system is documented. Activities include conducting an impact assessment in accordance with FIPS-199.

Development/Acquisition: During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle. Activities include determining security requirements, incorporating security requirements into specifications, and obtaining the system.

Implementation: During implementation, the system is tested and installed or fielded. Activities include installing/turning on controls, security testing, certification, and accreditation.

Operation/Maintenance: During this phase, the system performs its work. Typically, the system is also being modified by the addition of hardware and software and by numerous other events. Activities include security operations and administration, operational assurance, and audits and monitoring.

Disposal: The disposal phase of the IT system life-cycle involves the disposition of information, hardware, and software. Activities include moving, archiving, discarding or destroying information and sanitizing the media.

III. SECURITY PRINCIPLES

Principle 1. Establish a sound security policy as the “foundation” for design.

A security policy is an important document to develop while designing an information system. The security policy begins with the organization’s basic commitment to information security formulated as a general policy statement. The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support, and these goals guide the procedures, standards and controls used in the IT security architecture design. The policy also should require definition of critical assets, the perceived threat, and security-related roles and responsibilities.

Principle 2. Treat security as an integral part of the overall system design.

Security must be considered in information system design. Experience has shown it to be both difficult and costly to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system.

Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies.

Information technology exists in physical and logical locations, and boundaries exist between these locations. An understanding of what is to be protected from external factors can help ensure adequate protective measures are applied where they will be most effective. Sometimes a boundary is defined by people, information, and information technology associated with one physical location. But this ignores the reality that, within a single location, many different security policies may be in place, some covering publicly accessible information and some covering sensitive unclassified information. Other times a boundary is defined by a security policy that governs a specific set of information and information technology that can cross physical boundaries. Further complicating the matter is that, many times, a single machine or server may house both public-access and sensitive unclassified information. As a result, multiple security policies may apply to a single machine or within a single system. Therefore, when developing an information system, security boundaries must be considered and communicated in relevant system documentation and security policies.

Principle 4. Reduce risk to an acceptable level.

Risk is defined as the combination of (1) the likelihood that a particular threat source will exercise (intentionally exploit or unintentionally trigger) a particular information system vulnerability and (2) the resulting adverse impact on organizational operations, organizational assets, or individuals should this occur. Previously, risk avoidance was a common IT security goal. That changed as the nature of the risk became better understood. Today, it is recognized that elimination of all risk is not cost-effective. A cost-benefit analysis should be conducted for each proposed control. In some cases, the benefits of a more secure system may not justify the direct and indirect costs. Benefits include morethan just prevention of monetary loss; for example, controls may be essential for maintaining public trust and confidence. Direct costs include the cost of purchasing and installing a given technology; indirect costs include decreased system performance and additional training. The goal is to enhance mission/business capabilities by mitigating mission/business risk to an acceptable level.

Principle 5. Implement tailored system security measures to meet organizational security goals.

In general, IT security measures are tailored according to an organization’s unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used – implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.

Principle 6. Protect information while being processed, in transit, and in storage.

The risk of unauthorized modification or destruction of data, disclosure of information, and denial of access to data while in transit should be considered along with the risks associated with data that is in storage or being processed. Therefore, system engineers, architects, and IT specialists should implement security measures to preserve, as needed, the integrity, confidentiality, and availability of data, including application software, while the information is being processed, in transit, and in storage.

Principle 7. Protect against all likely classes of "attacks."

In designing the security controls, multiple classes of "attacks" need to be considered. Those classes that result in unacceptable risk need to be mitigated. Examples of "attack" classes are: Passive monitoring, active network attacks, exploitation by insiders, attacks requiring physical access or proximity, and the insertion of backdoors and malicious code during software development and/or distribution.

Principle 8. Where possible, base security on open standards for portability and interoperability.

Most organizations depend significantly on distributed information systems to perform their mission or business. These systems distribute information both across their own organization and to other organizations. For security capabilities to be effective in such environments, security program designers should make every effort to incorporate interoperability and portability into all security measures, including hardware and software, and implementation practices.

Principle 9. Use common language in developing security requirements.

The use of a common language when developing security requirements permits organizations to evaluate and compare security products and features evaluated in a common test environment. When a "common" evaluation process is based upon common requirements or criteria, a level of confidence can be established that ensures product security functions conform to an organization's security requirements. The Common Criteria provides a source of common expressions for common needs and supports a common assessment methodology.

Principle 10. Strive for operational ease of use.

The more difficult it is to maintain and operate a security control, the less effective that control is likely to be. Therefore, security controls should be designed to be consistent with the concept of operations and with ease-of-use as an important consideration. The experience and expertise of administrators and users should be appropriate and proportional to the operation of the security control. An organization must invest the resources necessary to ensure system administrators and users are properly trained. Moreover, administrator and user training costs along with the life-cycle operational costs should be considered when determining the cost-effectiveness of the security control.

Principle 11. Implement layered security (Ensure no single point of vulnerability).

Security designs should consider a layered approach to address or protect against a specific threat or to reduce vulnerability. For example, the use of a packet-filtering router in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. Adding good password controls and adequate user training improves the system's security posture even more.

The need for layered protections is especially important when commercial-off-the-shelf (COTS) products are used. Practical experience has shown that the current state-of-the-art for security quality in COTS products does not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in series, requiring additional work by attackers to accomplish their goals.

Principle 12. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).

While the trend toward shared infrastructure has considerable merit in many cases, it is not universally applicable. In cases where the sensitivity or criticality of the information is high, organizations may want to limit the number of systems on which that data is stored and isolate them, either physically or logically. Physical isolation may include ensuring that no physical connection exists between an organization's public access information resources and an organization's critical information. When implementing logical isolation solutions, layers of security services and mechanisms should be established between public systems and secure systems responsible for protecting mission critical resources. Security layers may include using network architecture designs such as demilitarized zones and screened subnets. Finally, system designers and administrators should enforce organizational security policies and procedures regarding use of public access systems.

IV. Conclusion

Now, more than ever, IT security is a critical element in the system life-cycle. Security must be incorporated and addressed from the initial planning and design phases to disposal of the system. Without proper attention to security, an organization’s information technology can become a source of significant mission risks. With careful planning from the earliest stages, however, security becomes an enabler, supporting and helping to achieve the organization’s mission. As security awareness becomes a way of life within an organization, people at all levels, and roles in the system life-cycle, should have access to easily understood guidance. From users to system administrators and program managers, everyone should have a basic understanding of the security principles governing the system they are using, maintaining, or designing and developing.

V. REFERENCES

[1] http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2
[2] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
[3] Information Assurance Technical Framework (IATF), Release 3.0, October 2000.
[4] http://www.iatf.net/,
[5] http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
[6] http://www.nstissc.gov/Assets/pdf/4009.pdf.
[7] http://csrc.nist.gov/publications/nistpubs/index.html:
[8] Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A : NIST Special Publication 800-27 Rev