Fundamental Principles of Information Security

Source:

Jim Breithaupt and Mark S. Merkow, **Information Security: Principles and Practices (2nd Edition)**, 2014

http://www.pearsonitcertification.com/articles/article.aspx?p=2218577

- Principle 1: **There Is No Such Thing As Absolute Security**
- Principle 2: **The Three Security Goals Are Confidentiality, Integrity, and Availability**
- Principle 3: **Defense in Depth as Strategy (layered security)**
- Principle 4: **When Left on Their Own, People Tend to Make the Worst Security Decisions**

- Principle 1: **There Is No Such Thing As Absolute Security**

- Principle 2: **The Three Security Goals Are Confidentiality, Integrity, and Availability** (aka. Security triad)

- Principle 3: **Defense in Depth as Strategy (layered security)**

- Principle 5: **There exist two types of requirements: Functional versus Assurance**

  - **Functional requirements** describes what the system should do (as specified earlier).
    - Does the system do the right things (behave as promised)?
  - **Assurance requirements** describes how functional requirements should be implemented and tested.
    - Does the system do the right things in the right way?

Functional/Assurance requirements vs Verification/Validation

- **Verification**: the process of confirming that one or more predetermined requirements or specifications are met. (c.f., functional rqts)

- **Validation**: the process of determining the correctness or quality of the mechanisms used to meet the specified requirements (c.f., assurance)

- Principle 6: **Security Through <u>Obscurity</u> Is Not an Answer**

  ➢“毋恃敵之不來，恃吾有以待之。”

  Do no count on your enemy’s not coming, but count on your readiness against attacks.

  – from the *Art of War* by Sun Zi (544 - 496 BC)

- Principle 7:

  Security = Risk Management

- Spending more on securing an asset than the intrinsic value of that asset is a waste of resources.

- Security is concerned not with eliminating all threats within a system or facility, but with eliminating known threats and minimizing losses if an attacker succeeds in exploiting a vulnerability.

- Risk assessment and risk analysis are concerned with placing an economic value on assets to best determine appropriate countermeasures that protect them from losses.

Matrix for Risk Analysis

- What is the consequence of a loss?
- What is the likelihood that this loss will occur?

Likelihood	Consequences				
	1. Insignificant	2. Minor	3. Moderate	4. Major	6. Catastrophic
A (almost certain)	High	High	Extreme	Extreme	Extreme
B (likely)	Moderate	High	High	Extreme	Extreme
C (moderate)	Low	Moderate	High	Extreme	Extreme
D (unlikely)	Low	Low	Moderate	High	Extreme
E (rare)	Low	Low	Moderate	High	High

- Principle 8: **The Three Types of Security Controls Are Preventative, Detective, and Responsive**

- **Examples**
  - **Preventive controls?**
  - **Detective controls?**
  - **Responsive controls?**

- Principle 9: **Complexity Is the Enemy of Security**
  - The more complex a system gets, the harder it is to secure.

- Principle 10: **Fear, Uncertainty, and Doubt Do Not Work in Selling Security**
  - Now IS managers must justify all investments in security.
  - Security practitioners must help the managers to justify the investments.

- Principle 11: **People, Process, and Technology Are All Needed to Adequately Secure a System or Facility** (aka. The three pillars of security)
  - Do not count on only one of them.
  - Examples:
    - "Dual control": No one person in an organization should have the ability to control or close down a security activity.
    - "layered security"

- Principle 12: **Open Disclosure of Vulnerabilities Is Good for Security!**
  - The issue: whether to let users know about a problem before a fix or patch can be developed and distributed
  - A raging and often heated debate
  - **Trade-offs?**
    - ✓ Pros
    - ✓ Cons