Principles of Information Security

Jacob L. Silva, Network Security

University of Advancing Technology

12 Principles of Information Security Success

Principle 1: There Is No Such Thing As Absolute Security

In Manchester, England, there was an art gallery where three famous paintings by Van Gogh, Picasso, and Gauguin were stolen. The value was more than $7 million. The paintings had alarm systems, 24-hour patrols, and closed-circuit television. Proving that even some of the most highly secure buildings can be broken into. This goes to show that even the best security can be compromised. What we can do is to be sure to have the latest security systems and guards to try and prevent any breaches in security.

Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability

Confidentiality is measures taken to prevent sensitive information from reaching the wrong people. Integrity is maintaining consistency, accuracy, and trustworthiness of data. Availability is the maintenance of all hardware and repairs. So, handling data should not be taken lightly. Access should be restricted to only those that are authorized to access, while the users should be using usernames, good passwords, and two-factor authentication when available.

Principle 3: Defense in Depth as Strategy

Defense in depth is a setup of multiple security measures to protect the integrity of information assets. To ensure the security of our assets, we should have in place firewalls, Intrusion detection systems (IDS), vulnerability scanning, and patches. This is to help monitor and stop malicious traffic on our network.

Principle 4: People can be the Biggest Loophole in Network Security.

One of the greatest security vulnerabilities in systems today is people with weak passwords and their willingness to click on things. Our security team will provide a companywide test to check and see which employee will need further training. In these tests, the users will not know, but they will be facing phishing attacks all the way to social engineering. If that employee falls for any of the attacks, they will be required to attend a week-long training course on how to be secure when using company assets.

Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance

Functional requirements are what a system should do. Assurance requirements are how functional requirements should be implemented. If an issue rises, like the blue screen of death, you must ask a few questions: Did you install a new program, update a driver, install a windows update? It’s recommended to scan your computer for viruses. And if you cannot run a virus scan within Windows, you can use a free bootable antivirus tool.

Principle 6: Security Through Obscurity

Hiding security details of security mechanisms is a sufficient method to help secure systems. So, closely guarding specifications of security functions and only allowing trusted people to see it can be beneficial. Security of systems should be maintained by keeping security implementation a system secret.

Principle 7: Value of Security

It’s important to buy security for your systems, but you shouldn’t spend more money than what it’s worth. This is the equivalent of buying a $500 safe to protect something that’s only worth $200.

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

Firewalls must be implemented as one of the controls to help prevent a compromise. However, there should be a procedure to use for an incident response. If the firewall is compromised, you will need to respond to the compromise; or if the firewall is under attack, there should be an appropriate response written guide, in the event that does happen as well.

Principle 9: Complexity Is the Enemy of Security

With complex systems, it will become harder to secure systems. That’s why it’s important to try to keep things as simple as possible. There are many more moving parts or interfaces between other systems or programs. Securing systems may be difficult while still allowing them to operate the way they are intended to. It’s important to take note of all the necessary services and to not block or prevent them from operating as intended.

Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security

At one point, a tactic to get more funds to spend resources on security was effective fearing the uncertainty. However, this tactic no longer works. IT departments are too mature now. All matters must be justified if there will need to be investments in security. I would say this is a good thing, to have a better understanding on how network security works. And it will force admins to make a case to management for more funds, instead of scaring them into giving.

Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

With a security professional, they will need a series of countermeasures and controls implemented on a network. A security professional may use dual control, a practice used from the military. Dual control protocol is used to secure the nation’s nuclear arsenal. Meaning, two on-site people must both agree to launch a nuclear weapon. If only one person was in control, they may make an error in judgment or act deviously. But with dual control, both people act as a countermeasure to one another. A security professional may establish process controls so that one person cannot gain complete control over a system.

Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!

In some cases, open disclosure of vulnerabilities is a necessity. If software is being distributed and there is an issue with the software, the users should have the right to know about that issue. This is so that they know the risks of having that software installed on their system and that it could potentially put their system at risk. Of course, it’s also important to notify the users when the issue is resolved.

References:

Pearson IT Certification. (n.d.). Retrieved January 14, 2018, from http://www.pearsonitcertification.com/articles/article.aspx?p=2218577&seqNum=2

Security Slideshow: 12 Information Security Principles To Put Into Action Today. (n.d.). Retrieved January 14, 2018, from https://www.cioinsight.com/c/a/Security/12-Information-Security-Principles-To-Put-Into-Action-Today-467962

What is confidentiality, integrity, and availability (CIA triad)? - Definition from WhatIs.com. (n.d.). Retrieved January 14, 2018, from http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Fisher, T. (n.d.). How to Fix a Blue Screen of Death. Retrieved January 14, 2018, from https://www.lifewire.com/how-to-fix-a-blue-screen-of-death-2624518