Can It Be…

NUC 2012 Kenneth B
stay updated via rss

Security Policies and Models (2.1)

Posted: January 22, 2013 in **NUC**

0

A noted computer security expert has said that without integrity, no system can provide confidentiality.1. Do you agree? Justify your answer.
Integrity means that information is correct, and that data has not been corrupted in any way. integrity ensures that information has not been compromised, that the information is valid and is a result of authenticated and controlled activities. If we don't have any way to confirm and ensure that this is true, we can't guarantee confidentiality. (Additional note on question 3).

Can a system provide integrity without confidentiality? Again, justify your answer
In a case where sensitive information needs to be protected it cannot provide integrity if it don't have Confidentiality. Confidentiality requires authentication of people, and integrity requires the information to be a result of authenticated and controlled activity.
(Additional note on question 3).

A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify or refute the cryptographer's claim.
It is possible to have some sort of integrity and confidentiality if you encrypt or put tamper resistant configurations to a document. But when we talk about information security used in for example an enterprise where human works (which is bad security in itself), I would conclude that integrity and confidentiality need each other to work as intended.

How are the standards ISO/IEC 27001 and ISO/IEC 27002 related?
Department of trade and Industry previous security standard was named BS 7799. The continued work with BS 7799 was done by British Standard institute, BS7799 contained two parts, part one was turned into NS ISO/IEC 27002:200 and part two NS ISO/IEC 27001:2005.

Which one of the standards can be used for certification, and why?
NS ISO/IEC 27001:2005 makes the foundation for certifying security products and companies. The certification work contains a process called Information Security Management System (ISMS). The ISMS describes how to establish, maintain and improve the information security in a company. A third part will ensure that a company fulfills the requirements of a ISMS.

Some reasons to certify safety related products or a company is:
- Increased security/quality in the company.
- Some customers requires that their suppliers are certified with NS ISO/ 27001.
- Shows that the company priorities security.

How should an organisation determine which security controls to implement?
ISO 27002 focus on a variety of measures to improve information security. It is a standard that provides recommendations for management of security relation to all information. It is an important tool in the design of the company's own security design, By following the recommendations of ISO 27002 you ensures that the security policies are in compliance with applicable laws and regulations.

Answer to the group activity:
"A policy is a set of rules and guidelines that specify how certain things should or should not be done. It can be said to function as a law, or set of rules/principles within an organization that has implemented the policy. Policies are usually not governed by public authorities and are used mainly to maintain and protect a company's interests and concerns for security, integrity and confidentiality. However, an unfamiliarity of a policy can be used as a defence by an individual while ignorance of a law cannot – this is because a Policy must be issued and taught to every person that is bound to follow it." written by Ole B, Tom D and Kenneth B…