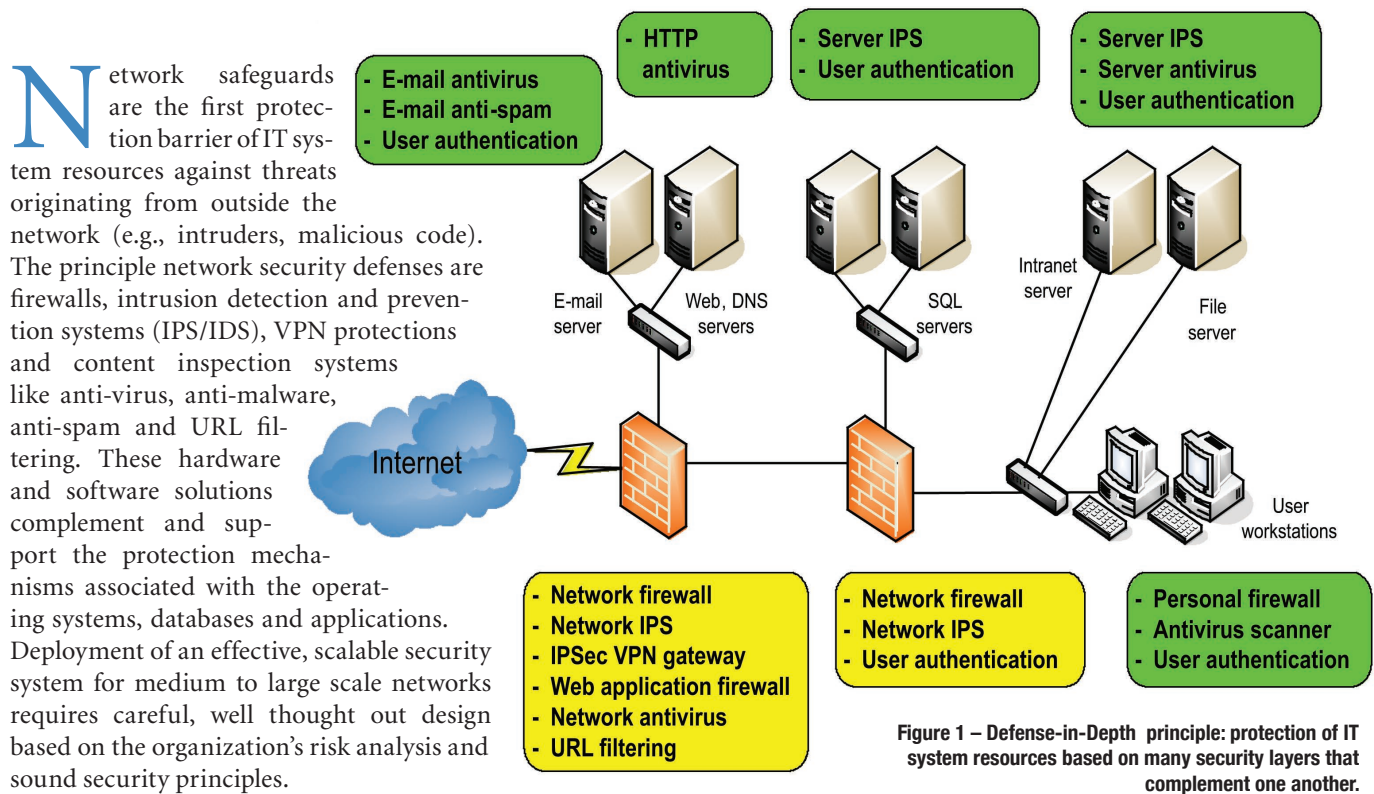# The Principles of Network Security Design

By Mariusz Stawowski

Deployment of an effective and scalable network security system requires proper designing according to risk analysis results as well as security principles.

Network safeguards are the first protection barrier of IT system resources against threats originating from outside the network (e.g., intruders, malicious code). The principle network security defenses are firewalls, intrusion detection and prevention systems (IPS/IDS), VPN protections and content inspection systems like anti-virus, anti-malware, anti-spam and URL filtering. These hardware and software solutions complement and support the protection mechanisms associated with the operating systems, databases and applications. Deployment of an effective, scalable security system for medium to large scale networks requires careful, well thought out design based on the organization's risk analysis and sound security principles.

Figure 1 – Defense-in-Depth principle: protection of IT system resources based on many security layers that complement one another.

Security principles

When designing the network security system, the following fundamental IT systems security principles should be taken into account:

Defense-in-depth

Protection of IT system resources is based on many security layers as shown in Figure 1. Extensions of the defense-in-depth principle are the following rules:

- **Layered protections** – security layers complement one another: what one misses, the other catches.

- **Defense in multiple places** – security defenses are located in different places of the IT system.

- **Defense through diversification** – safety of IT system resources should be based on the protection layers consisting of different types of safeguards. When two layers of the same type are being used (e.g., two network firewalls), they should come from different vendors. This rule should be used with caution as it increases the complexity of the security system and can make management and maintenance more difficult and costly.

Compartmentalization of information

IT system resources of different sensitivity levels (i.e., different risk tolerance values and threat susceptibility) should be located in different security zones. The concept of this principle is shown in Figure 2. An extension of this rule is "information hiding": the IT system makes available only such data that is necessary for conducting the IT system tasks (e.g., only servers providing services to the Internet are registered in public DNS).
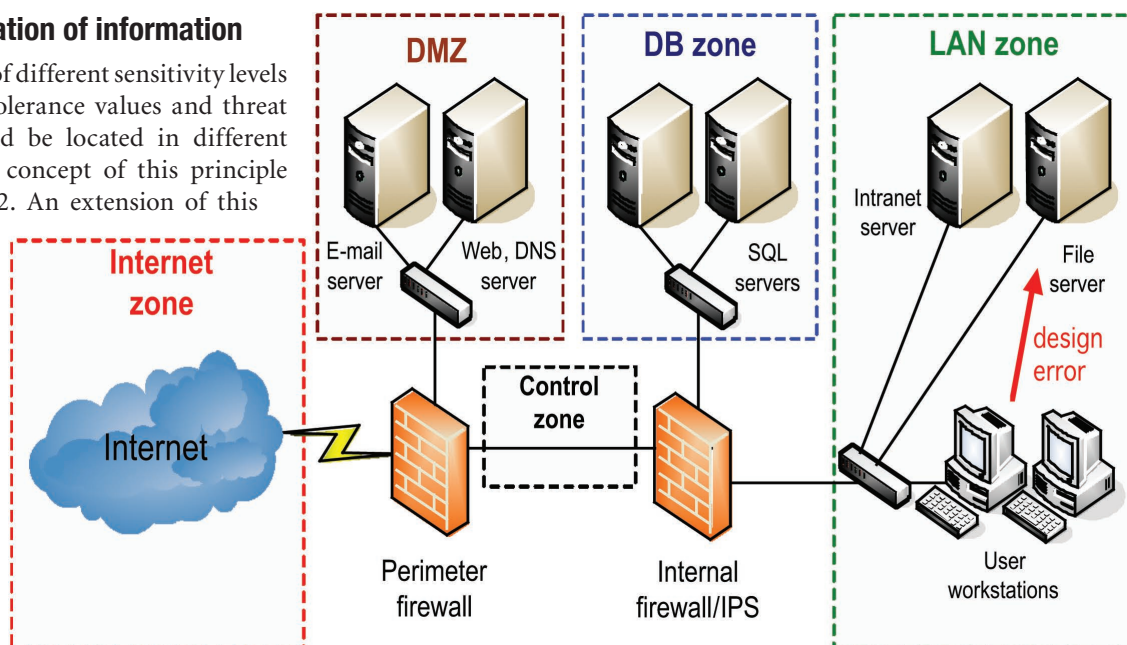

Figure 2 – Compartmentalization of information: IT system resources of different sensitivity levels should be located in different security zones.

Principle of least privilege

IT system subjects (e.g., users, administrators) should have minimal privileges necessary for proper functioning within the organization. This rule applies also to data and services made available for external users. An extension to this rule is the "Need-To-Know" principle which says that users and administrators of IT system have access to only the information relevant to their role and duties performed.

Weakest link in the chain

The security level of the IT system depends on the least secured element of the system. An extension of this rule in respect to network services availability is the "single point of failure" principle, which says that on the network paths between users and mission-critical IT system resources, all the links, devices (networking and security) as well as the servers should be deployed in redundant configurations (so called High Availability – HA).

When designing the network security system, the principles of organizational security such as "Separation of Duty" and "Job Rotation" rules should also be taken into account. Their goal is to limit an employee's ability to neglect and break the IT system's security policy. Separation of duty dictates that important tasks/functions should be performed by two or more employees. Job rotation states that there should be rotation of employees in important positions.

Security zones

The basic means of keeping network traffic flowing where you want and restricting it where you do not is the firewall: dedicated firewall devices, firewall functions in IPS devices, and access control lists in network routers and switches. With proper placement and configuration, firewalls help

create secure architectures, dividing the IT system network infrastructure into security zones and controlling communication between them. The compartmentalization principle describes the following network security design rules:

1. IT system resources of different sensitivity levels should be located in different security zones:

   - Devices and computer systems providing services for external networks (e.g., the Internet) should be located in different zones (De-Militarized Zone – DMZ) than internal network devices and computer systems

   - Strategic IT system resources should be located in dedicated security zones

   - Devices and computer systems of low trust level such as remote access servers and wireless network access points should be located in dedicated security zones

2. IT system resources of different types should be located in separate security zones:

   - User workstations should be located in different security zones than servers

   - Network and security management systems should be located in dedicated security zones

   - Systems in development stage should be located in different zones than production systems

Intrusion prevention

IPS devices are responsible for detecting and blocking penetrations and attacks conducted by intruders and malicious malware applications. They should be installed in the network path between potential threat sources and sensitive IT system resources. When designing IPS systems, attacks

through encrypted sessions (e.g., SSL) should also be taken into account. Since the IPS would not able to inspect these encrypted sessions, an effective method would be to decrypt the sessions prior to IPS devices in order to inspect unencrypted packets.

An important requirement for intrusion prevention tightness is the proper design of network protections and control rules. For one, internal networks should not have direct access to the Internet so a Trojan sent to a user's workstation through a phishing attack would not allow the intruder to connect to the external network. This is shown in Figure 3. In this example the Internet services are available for internal users only through company email and HTTP Proxy servers.

Final considerations

Network security management includes the activities of IT staff related to configuration (e.g., device parameters setting, policy creation), monitoring of security operations, troubleshooting problems as well as reading, reporting and analyzing logged events (logs, alerts), and explaining detected security incidents. Maintenance and supervision of the protections in normal system operation conditions should be performed from dedicated management systems located in separate network zone, appropriately protected by the firewalls – management VLANs.

The risk analysis and security design primarily focus on the most valuable IT system resources (i.e., systems performing or supporting business tasks of the organization). However the protections scope should not be limited to the most valuable resources. The protections being designed should become an effective barrier against attacks conducted using the

"Island Hopping Attack" technique. This technique works by gaining unathorized access to weaker protected areas, usually less important for the organization, and using them as a base for penetration of better protected and more valuable IT system resources.

When developing security requirements for IT system resources, determine if they are mission-critical or data-sensitive resources, where data confidentiality and integrity are the most important requirements, or where the priority is continuity of operation (availability). For mission-critical resources the protections should be designed in High Availability configurations.

Detecting and responding to incidents related to security breaches are important topics which should be elaborated during the design process. In reality there is no 100 percent effective protection and the situation that an intruder or a worm breaks into the network should be considered and planned for. For instance, a break-in can be accomplished utilizing an unpublished security bug (zero-day exploit) or from within the network, bypassing the IPS protections. These topics should be the elements of network security design and written in the incident response procedures.

References

— Zimmerman, S.C., *Secure Infrastructure Design*, CERT Coordination Center, 2001 CERT.

— *Infrastructure Security Technical Implementation Guide*, US Defense Information Systems Agency, DISA 2003.

— Stoneburner, G., Hayden, C., Feringa, A., *Engineering Principles for Information Technology Security*, 2004 NIST.

— *Defense in Depth - A practical strategy for achieving Information Assurance in today's highly networked environments*, 2000 NSA.

— Straub, K.R., *Information Security Managing Risk with Defense in Depth*, 2003 SANS Institute.

About the Author

Mariusz Stawowski, Ph.D., CISSP, is Director of Professional Services of CLICO, a security technologies distributor and service provider located in Poland. For more then 10 years he has been responsible for management of security projects. His doctoral dissertation was elaborated at the Military University of Technology in the special field of IT systems security auditing and network protections designing. Mariusz can be contacted at mstawow@clico.pl.
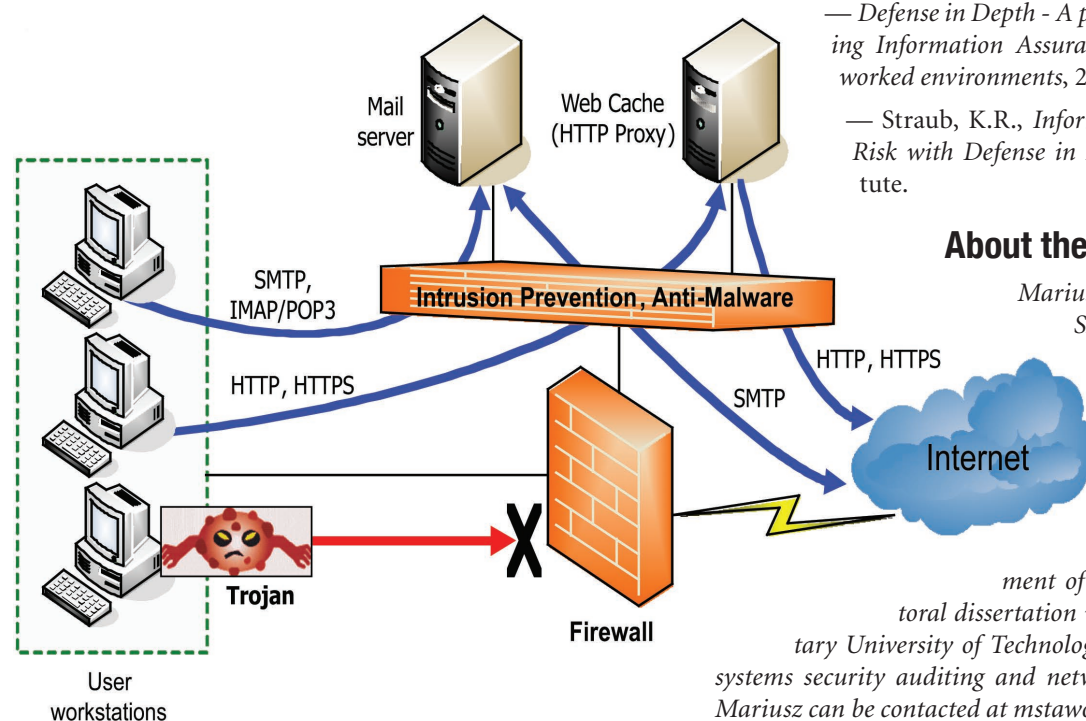

Figure 3 - Intrusion prevention requires restrictive access control of users in internal networks.