



Enterprise Information Security Solutions

Improving security in a dynamic environment

Recent changes in the IT&C security landscape

The vulnerability-threat window is continuing to close. The historical period of 6 months to address an identified vulnerability is no longer being afforded. For example, in August 2003, MSBLAST followed identification of the associated RPC DCOM vulnerability by only 26 days and the more recent Sasser worm - April 2004 - followed the Windows LSASS vulnerability by only 17 days.

The propagation times for threats is rapidly decreasing. Slammer doubled its infection count every 8.5 seconds, reaching 90% of vulnerable hosts within 10 minutes.

The broader perspective to consider involves the fact that information technology continues to rapidly evolve and even expand into new areas. Wireless networking, instant messaging, voice over IP, Web services and grid computing are just a part of the latest technological changes of the IT&C system.

Mobility is another example with the additional consequence of diminishing the effectiveness of traditional Internet – Demilitarised Zone based approaches to providing security. The number of potential unauthorized entries in the networks is rapidly increasing and the implementation of the security policy should be changed accordingly.

One other important factor influencing the security landscape is the need to comply with various governance and privacy regulations, such as the Sarbanes-Oxley Act.

New problems caused by recent changes in IT&C security

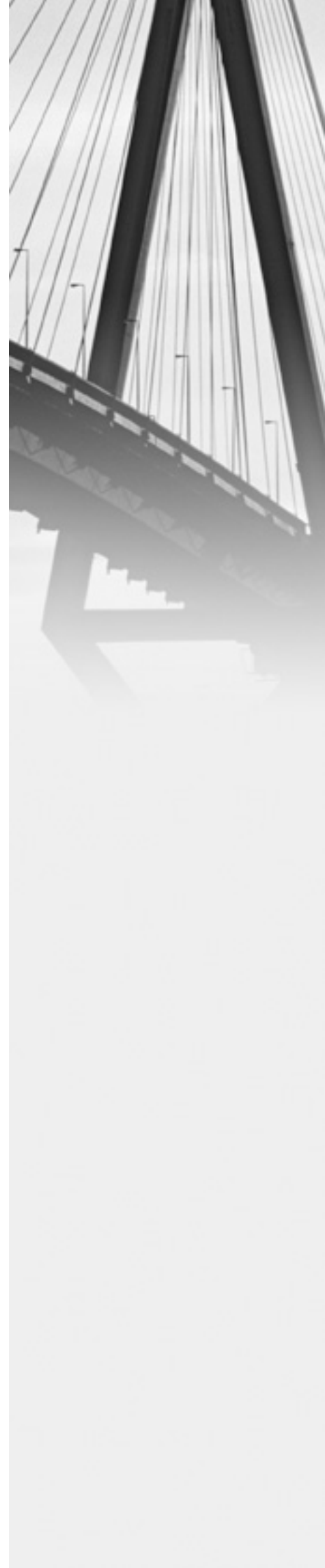
Those changes require that IT security professionals find solutions for the following problems:

- ⇒ Drawing a distinction between an external threat and an internal threat is increasingly pointless. The source of a threat has simply become less relevant as network perimeters have become less well defined. As a consequence, being effective from a security perspective will depend on establishing new/additional perimeters in closer proximity to the resources that are being protected.
- ⇒ Perimeter-oriented security strategies, while at one time adequate, are not now and never will be sufficient.
- ⇒ The scale of the environment requiring protection is significantly greater, involving numerous networks and potentially thousands of systems.
- ⇒ The scope of the environment is significantly greater, involving a much wider variety of both business applications and underlying protocols - not just HTTP, SMTP and the others associated with the DMZ.
- ⇒ More types of users or groups of users must be managed.
- ⇒ The internal network involves greater throughputs.
- ⇒ Antivirus and Intrusion detection systems products are limited by their dependency on foreknowledge of attack signatures.
- ⇒ Most firewalls lack sufficient application coverage and performance capabilities.
- ⇒ Switch and other network infrastructure-based products typically lack the visibility above the network layer.

The traditional information security approach is to build the defence system on several layers in order to reduce the chances of an attack to neutralizing all layers.

This has led to the concept of “Defense in Depth.” Until recently, most companies selected and implemented point products for reducing threats: anti-virus, intrusion detection systems, intrusion prevention systems, enhanced VPNs, firewall technologies, patch and configuration systems.

The implementation of the security policy was completed by physical security, patching and configuration for OS hardening, user administration and system audit.

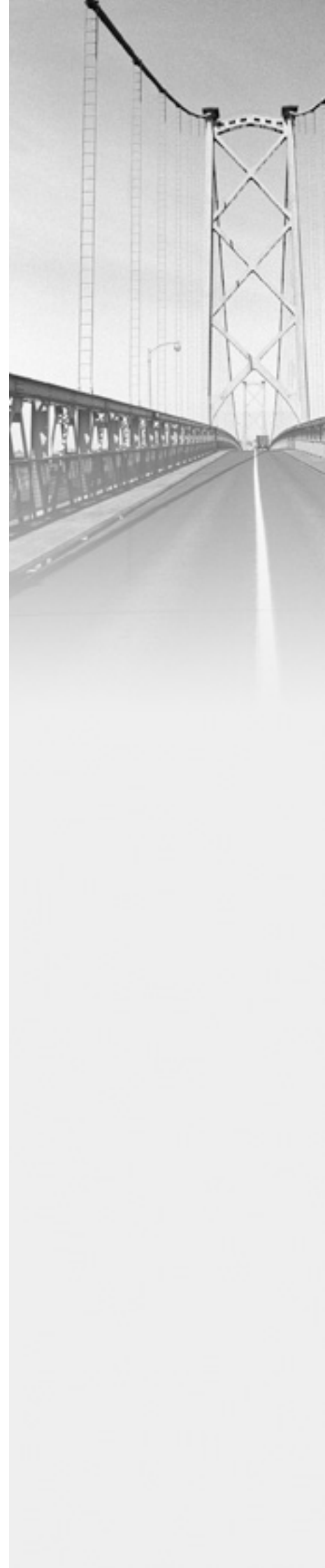


How to address the new problems in managing the information security

In order to address the above problems there are some measures that essentially contribute to reducing the security risks. Those measures lead to a smarter, more reactive network designed to protect the hosts. Such a network will identify and correct attacks as close to their points of ingress into the network as possible.

Compared with the perimeter security approach, the network and the corresponding operational processes should provide an enhanced security system with improved performance and because of the increased complexity of the attacks and security devices, enhanced management. To reduce the security risks today, the measures are the following:

- ⇒ **Internal segmentation**, using routers, switches, and virtual LAN technology, supports logically or physically separating resources that require different levels of security.
- ⇒ **Internal firewalling** provides the benefit of providing a more effective security barrier where needed.
- ⇒ **Operating system hardening** is essential at least for the most critical application platforms.
- ⇒ **User administration** involves explicitly provisioning which resources users have access to. Stronger user authentication is also very important. Reliance on simple username and password combinations was demonstrated to be insufficient in the long run.
- ⇒ **Monitoring for suspicious activity** within the internal environment and **attack protection** provides the ability to detect and stop both known and unknown threats from acting within otherwise allowed traffic streams. The goal is to stop both automated attacks, such as worms, and manually generated malicious activity.
- ⇒ **Application awareness and control** insures the ability to protect communications and computing resources based on application-layer information.
- ⇒ **Endpoint policy enforcement** - provides access to networked services be conditional upon the findings of a real-time audit of the security and configuration status of the involved client device.
- ⇒ **Endpoint Protection** - A new generation of host IPS products is implementing forms of behavioral security to detect and prevent viruses and worms from gaining a foothold on an endpoint system and prevents them from propagating across a network.
- ⇒ **Enhanced Management** - The security solutions implemented shall have centralized management. In addition, support for scalable and flexible management of policies and configuration settings is important. Today's networks must be able to respond to attacks in ways that maintain network availability and reliability and allow a business to continue to function. The management solution should offer a coherent view of the entire security system allowing the system administrators monitor, react to eliminate threats and audit the security of the IT&C systems.



Security solutions provided by Datanet Systems

The security solutions provided by Datanet Systems covers all the previously described implementation directions:

- ⇒ Internal segmentation and firewalling is insured by several families of routers and firewalls offered by Datanet Systems, such as Cisco IOS routers with advanced security features (VLAN, firewall, IPSec VPN) and Cisco firewall appliances or modules in the LAN switches.
- ⇒ Operating system hardening is insured as a service by Datanet Systems PS team.
- ⇒ Controlled access to network resources is insured by access control servers; enhanced user authentication is ensured by Datanet Systems using One Time Password and X.509 digital certificate systems.
- ⇒ Monitoring and attack protection is ensured by implementing IDS/IPS products. Those products insure enhanced protection based on application-layer information.
- ⇒ Endpoint policy enforcement is a central role of the Cisco Self Defending Network solution provided by Datanet Systems.
- ⇒ Endpoint protection is ensured with several host protection products, such as Cisco Security Agent.
- ⇒ All the security solutions provided by Datanet Systems have centralized management. In addition, Datanet Systems offers specialized solutions for centralized security log management.

Datanet Systems is a Cisco Systems Gold Partner and VPN Security Specialized Partner. An important role in the security solutions provided by us has the Cisco Self Defending Network (SDN) solution. The key abilities of the Cisco SDN “adaptive” defenses are that they:

- ⇒ Remain active at all times
- ⇒ Perform unobtrusively
- ⇒ Minimize propagation of attacks
- ⇒ Quickly respond to as-yet unknown attacks.

The Cisco Self-Defending Network insures:

- ⇒ The Threat Defence System that comprises several critical technologies and products enabling security integrated in routers, switches and appliances: firewalls, network-based intrusion protection sensors, detection instrumentation, and traffic isolation techniques. Endpoint protection is enabled through the Cisco Security Agent.
- ⇒ The Cisco Secure Connectivity System that uses encryption and authentication capabilities to provide secure transport across untrusted networks. The system uses IPSec, SSL and MPLS VPN technologies along with standard authentication mechanisms.
- ⇒ The Trust and Identity Management System - It provides access to business applications and networked resources based on a user’s specific privileges and rights. The system focuses on network- based admission control. After validating the identity of a user or device, and its compliance with corporate security policy, access to certain resources or portions of the network can be enabled. The network is responsible for identification, authorization, and enforcement.

Datanet Systems delivers to its customers all the products within the Cisco Self Defending Network strategy, integrated with complementary security products, offering a complete solution for the management of information security.

The technical team of Datanet Systems including CCIE, CCDP, CCNP, CCIP, CCSI, MCSE and ISO 17799 certified specialists offers:

- ⇒ expert-level design
- ⇒ implementation
- ⇒ service and support
- ⇒ security consulting and audit services

Datanet Systems solutions and services have been chosen by most of the major banks and telecom service providers in Romania.

14 Zarii st, sector 5
050461, Bucharest, ROMANIA
tel: (40) 21 3178-787,
fax: (40) 21 3179-797
office@datanets.ro
www.datanets.ro

believe in more