



Compumatics – IT Security Capabilities

Information is the currency of the digital economy. Whether an online storefront or sophisticated Internet-based commodity exchange, e-commerce is critically dependent on the secure flow of information to make the online magic work. These transparent online supply chains can lead to streamlined business operations and new market opportunities. Or, if poorly protected, they can quickly lead to an expensive premature obsolescence.

At its core, information security closely resembles security in the physical world. Brick-and-mortar organizations use burglar alarms, fire alarms and security guards to protect facilities from theft and misuse. The online world has exactly the same need, but the immense economic pressure to get online and grow quickly often tempts organizations to sacrifice security as a non-essential luxury.

This perspective is understandable, albeit shortsighted. Information security specialists are in high demand and short supply. Security itself can be complex in design and implementation, and requires 24x7 attention to be effective. And yet, security is critically important for e-business success. A single break-in at a warehouse carries a finite amount of loss. A single break-in that successfully compromises a key e-commerce server, however, can leave an e-business “out of business” for hours, embarrass that company in the national media and expose the organization to significant stakeholder liability.

Through its subsidiary company Presidium Systems, we understand the needs and challenges facing any organization looking to use the Internet to expand its business opportunities. Our best-of-breed information security solutions and managed security services deliver effective, cost-efficient and comprehensive protection for any e-business. By ensuring the availability, integrity and privacy of mission-critical business information, Presidium eases the information security burden and helps our clients concentrate on what they do best – innovate, profit and grow.

Presidium helps companies safely grow their businesses by providing complete security policy and infrastructure solutions that address security from a people, policy and technology perspective. Unlike any other vendor, Presidium helps to educate the people within an organization to comply with information security policies and integrates each policy using best of breed security technology -- all designed to ensure maximum protection of information assets throughout a corporate enterprise.

People

Our people have current security clearances (some up to Life Style Poly) when required for working in secure environments. Further, they are trained on the latest technologies and products that address the area of IT Security.

Services

Security Auditing

In a security audit we are your defender, not your attacker. You show us your system (firewall, web-based system, corporate network, database solution etc.) - what it does, how it works - and we take it under an in-depth security analysis. The more insight into the system you can provide, the more exhaustive our analysis can be. Throughout the audit, we employ our "attacker's point of view" mode that we sharpen in our penetration tests, continuously asking ourselves the same question: "How could *this* feature be useful for the attacker?" Additionally, we use our collection of probing tools to automatically scan the evaluated system and detect its potentially vulnerable points.

Penetration Testing

If your system hasn't been intruded yet, don't feel too comfortable (by the way, how can you be so sure about it?). Chances are it will become a target some day. By your competitor, an intelligence agency, a disgruntled employee, or maybe just a bored kid who got lucky and found a hole in your mail server. In any event, the damage to your business can be very serious, sometimes lethal. Unfortunately, many times an incident like this is the only way for making the right people in your organization focus on security problems that always get preempted by "more important issues". Fortunately, on the other hand, there is an alternative.

Penetration test is a controlled and managed simulation of an actual system intrusion. It gives you a realistic experience of an attempted (usually successful) break-in into your information system - whether from an outside intruder or from your employee or business partner. During a penetration test, your security mechanisms as well as your intrusion detection and response capabilities are put to the test against a skilled, motivated attacker - only this time you have a complete insight in his thoughts and actions. This is a unique opportunity to get to know your enemy, without the damage you would normally sustain in a real attack.

Periodic penetration testing is a very effective method for keeping your security capabilities on a desired level (they usually slide down to the original level after the penetration test is over). This way, you get yourself a "friendly attacker", constantly trying to subvert your security mechanisms. You know it and your people know it so there's an ever-present awareness of an attacker's existence (as it should be), keeping your security sharp. Every attack is known to you - but not your employees - in advance and documented in details, or you might even suggest where and when to attack to test particular points that you believe could be weak. A detailed statistics is being maintained about the attacks so that you can easily locate weak spots in your security and later watch how they gain in their strength.

Security Probing

Normally, organizations have a good inside view of their security. They know what security mechanisms are employed and what they are protecting them against. On the other hand, they rarely know exactly how their security looks from the outside. And yet, *this* is the view that's available to their attackers. Shouldn't you know what your enemy probably already knows about you?

Security probing is an automated process during which we scan your perimeter security, systematically looking for points of potential intrusion. We collect information about your routers, firewalls, public servers, modem dial-in points etc. In a nutshell, we examine your organization's "electronic walls" for possible entry points, which is exactly what your attacker will do. A detailed report is generated including exact times and targets.

Periodic security probing is the best method for assuring your outside security view remains unchanged in the course of time. There are many reasons why your outside security view might change; for example: the administrator might have "temporarily" opened a port in the firewall and forgot to close it, a web server had to be upgraded and dangerous sample scripts were unwittingly installed with it, or one of your employees installed a modem in his PC so that he could access the Internet from his home. Periodic security probing can be done annually, monthly, weekly, daily, hourly or even every few minutes, depending on how quickly you want to detect the changes.

Security Policy Services

Information security policy is without a doubt the foundation stone of your organization's security. It defines the organization's direction and management support for information security. However, defining, testing, enforcing and updating security policy is never an easy job - it requires changes in business processes and people's behavior and furthermore, it is a project that never ends.

We can augment your internal resources to implement this project from the inception to completion, or you can outsource the functionality and we will handle it all. We analyze your business processes, review your existing policies and corporate documentation to avoid conflicts and possibly suggest their improvements. In close interaction with your management the lifecycle of your security policy is started - with the resulting documents. We can suggest technical solutions for policy support (availability, enforcement, maintenance) and periodically review the policy as well as your compliance with it. We'll help you accept your security policy and recognize it as a powerful tool for protection of your vital business information.

Security Solutions

By combining our superior products and skills, we can provide security solutions that are robust, effective and provide maximum protection for your information assets.

Our solutions include:

- Security Policy Development
- Network Design & Installation
- Firewall Installation & Configuration
- Intrusion Detection Systems Installation & Configuration
- Server Installation, Configuration & Hardening
- Managed System Administration Security
- PKI Integration
- Virtual Private Networks (VPN's)

Security Audits

Our security audit service is ideal for organizations wanting an independent audit of their information systems security.

Our service includes an assessment of critical assets and high-risk information, policy and procedures, security standards and training, hardware and software, and security roles and responsibilities.

We will inspect your site, review your physical security, interview your staff, review your network architecture, perform penetration testing, analyze your access controls and study your security policy.

Results of the assessment will be documented in a report that will detail findings, analysis and recommendations for improving security in your organization.

Incident Response

Are you the victim of a computer security incident?

Our expert security consultants can assist you in the aftermath. We will contain and investigate the incident, find and eliminate backdoors left behind by an intruder, determine what information has been compromised and if needed, gather evidence for a prosecution by performing forensic analysis.

We will also propose and implement corrective action to prevent further attacks, recover any lost data and restore the system.

We will also coordinate with other sites and deal with law enforcement.

Computer Investigations

Our computer investigation services can assist your organization in investigations where computers have been used in the commission of offences, intellectual property matters, fraud, and civil matters.

Our investigative services include:

- Forensic analysis of computer disk drives.
- Data recovery to retrieve deleted, hidden or encrypted material.
- Internet tracing.
- Network Monitoring.
- Keystroke logging & recording.
- Providing expert evidence at court for all investigative matters.

Proposed Detailed Service Offerings

1. Internet exposed server security auditing from the external networks/Internet (web/mail/ftp)

2. Mail server vulnerability from external networks/Internet
3. Corporate Anti-Virus policy
4. Restricted Web Surfing
5. Sub-netting and Non-routable IP segments to restrict unauthorized external connections
6. VPNs/SSH and Remote Connections
7. Online Conferencing Capability
8. Internal network security audits
9. Sub-netting/segmenting internal to the network to separate classified and non-classified info
10. User rights and policies
11. Wireless network security