WHITE PAPER

Securing Information Infrastructure: Expert Advice on Evaluating the New Risks and Structuring Your Defenses

Biography of Author

John P. Pironti, CISA, CISM, CISSP
Enterprise Solutions Architect/Security Consultant – Unisys Corporation
Technical Advisor – F5 Networks

John P. Pironti is an Enterprise Solutions Architect and Security Consultant at Unisys Corporation and a technical advisor to F5 Networks. He has designed and implemented enterprise wide electronic business solutions, information security programs, and threat and vulnerability management solutions for key customers in a range of industries, including financial services, government, hospitality, aerospace and information technology. Mr. Pironti is a Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP). He is also a published author and a frequent speaker on e-business and security topics at domestic and international industry conferences.

Introduction

Information security is no longer an afterthought in the development of technical solutions to business problems. It has now become the top concern of senior management and technologists alike in the development and operation of those technology solutions. That is because those solutions now represent an integral part of the business process, enabling enterprises to operate more efficiently, effectively, and profitably.

The enterprises implementing the solutions are not the only ones who understand their value. Their adversaries do, too. The adversaries also recognize the value of compromising the business solution for their own gains. Those gains may be political, financial, or social. The challenge in information security is that the adversary only has to be correct once, but the protector has to be right all the time.

One of the key motivators for the new focus on information security is the increase in regulations on a global scale. Sarbanes Oxley, the Gramm-Leach Bliley Act, the European Data Privacy Directive, and the Basel II accord, among other regulations, put a new focus on information security. Each of those regulations has specific requirements surrounding information security that must be addressed in order for an organization to comply with them. These regulations also have defined penalties for non-compliance that can include criminal charges against management teams of organizations. This has quickly turned enterprises' focus to improving their information security capabilities and posture.

Gramm-Leach-Bliley Act - Section III
Development and Implementation of Information Security Program, Section B.

Assess Risk. Each bank shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration,
2. Assess the likelihood and potential damage to these threats, taking into consideration the sensitivity of customer information systems.
3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks

The audit community has also taken note of this new, management focus on the need for more comprehensive security controls and capabilities. Traditionally information system auditors had minimal knowledge of information security concepts and technologies, and relied on checklists and advice from information security subject matter experts to populate their audit reports. With the new regulatory climate and mandates from management they now take more interest in information security. They want quantifiable evidence that the information security controls in place are working as promised to protect the organization's information infrastructure. Without that they are unwilling to provide positive audit reports.

This new focus from management teams has brought about maturity in the way that information security is being addressed. Traditional solutions revolved around a perimeter and network-centric model for protecting the enterprise's information infrastructure. This model included utilizing network firewall, virtual private network (VPN), and intrusion detection and prevention (IDS/IPS) solutions at all network entry points to the information infrastructure. The theory was that if you can protect the borders you can then worry less about the internal elements because the adversary cannot access them. These network centric solutions have proven helpful, but they are incomplete now that the business solutions being put in place require a wider range of access to internal resources by outside systems and users.

Information security solutions are no longer built around a specific technology. The new focus is an information-centric model. This model strives to ensure that the three pillars of information security are met: confidentiality, integrity, and accessibility of the information being protected. In this model the information is analyzed and assessed for its value to the organization. Once that is understood, information is given an appropriate level of protection based on its assessed value. That protection will include process, procedure, and policy elements and will use technology elements as a tool to enforce them.

Emerging Attack Trends and Attack Evolution

The attack methodologies and trends are evolving from a network-based approach to an application-focused approach. Adversaries typically target areas within a solution that they perceive to be the easiest to compromise. Traditionally the easiest area to attack in an information infrastructure solution was the network. While organizations were evolving their network infrastructure to include connectivity to the Internet they often left themselves exposed to attacks. During that period network firewall technologies and network-level protection were considered difficult to install and operate. In addition, they often had weaknesses caused by incorrect configuration of these solutions. That is no longer the case due to the greater understanding of the need for security at the network layer and the ease of use engineered into those technologies by the vendors who develop them.

The adversary community has now been shifting its attention and techniques to attack the applications themselves instead of the network. One of the key reasons for this is that applications, especially web-enabled applications, are often connected to the Internet. Holes can be punched through the network security layers, such as firewalls, to allow unauthorized users to access these systems. When connected to the Internet these applications and web environments can be easily located using everyday activities and technologies such as DNS queries or ping sweeps, or even through the advertising on web pages.

When considering the attacks that adversaries are using it is more important to understand their goals and motivations to properly protect an environment from them. The adversary understands that there is value in an organization's information almost as well as the organization themselves. Adversaries also have come to understand that they can cause as much if not more damage to an organization if they compromise the integrity of the information stored or accessed in a solution.

For example, if an adversary is able to invalidate the data in a financial institution's account database or a medical institution's patient record management system, they can do more damage to the organization than if they deleted those databases. In the case of data deletion an organization can determine when the last valid backup of the databases occurred and use it to restore the databases to that point in time.

If the adversary is successful in invalidating the database in a non-uniform fashion over a period of time, they then can cause significant damage to an organization's capabilities and to the confidence of its customers. This type of attack is significantly more difficult to recover from because the organization cannot simply restore backups, because it must determine which data has been invalidated and for how long. This can be a long and arduous process that can have a devastating impact on the operational capabilities of the organization.

One current trend in application attacks is to reverse-engineer vendor patches. The concept is based upon the idea of using the recognized deficiencies in the vendors' products to work against them. An adversary can quickly isolate files a patch has modified and identify how they have been modified, using widely available hash tools and code analysis engines. Once they have identified the files that have been modified they can investigate them for deficiencies. This analysis, along with the vendor-provided descriptions of the problem the patches are designed to solve, allows the adversary to quickly develop exploits. The adversary can then launch attacks using these newly developed exploits across a wide range of systems in a very short period of time.

Most mature patch management programs require a period of time to test and evaluate patches before they are deployed into the information infrastructure. The time required for evaluation and deployment can be days and even weeks for some organizations. The intelligent adversary is aware of this and will often use this to their advantage. They will attempt to reverse-engineer the patches as quickly as possible and exploit as many vulnerable systems as possible prior to patch deployment.

Another emerging attack type is the targeted assault on the applications themselves. The adversary will study the way that an application reacts to different input strings and data flows. If they can profile the way an application will behave with different requests and activities, they will have a greater chance at launching a successful attack. They will then attempt to tamper with input strings to try and gain access to restricted information they are not authorized to access.

One of the other attack techniques plaguing information infrastructure today is that involving attacks through trusted connections. Trusted connections can include virtual private network links, leased line connectivity, and closed networks (i.e., ATM or Frame Relay network clouds). Adversaries understand that the larger organizations that they may want to attack have considerable resources and capabilities to protect their borders and the Internet-facing information infrastructure. They also know in this age of outsourcing that large organizations tend to do business with other organizations, including smaller ones who do not have the same information security capabilities as the targeted one. These smaller organizations also have trusted connections to the information infrastructure of the larger ones.

An adversary who has that knowledge in hand will exploit the fact that the smaller organizations that do business with the larger ones do not have robust information security capabilities. The adversary will exploit this infrastructure and utilize the trusted connections to attack the larger organization.

Most organizations do not invest the same level of resource or capability in securing their borders where they have trusted links to other networks. They tend to believe that since the link is trusted, the traffic flowing through it should be trusted as well. These connections tend to create links to the back-office infrastructure of organizations where the most critical and sensitive business activities take place. That is a fatal flaw in many information infrastructures today.

Remote access entry points are another key area that organizations tend to overlook when securing their information infrastructure. Use of virtual private networking solutions has enabled a remote work force. This capability has tremendous business benefits to an organization but also creates new risks to the organization. Adversaries seek out remote access-enabled terminals in the same way they look for smaller organizations with trusted connections to larger ones.

The problem of remote access points into information infrastructure is an even greater threat to the organization with the introduction of unknown endpoints out of their control. Those endpoints can be personal computers, kiosks, public access terminals, and other systems with access privileges. Recent worm outbreaks have proven this on more than one occasion and in more than one organization. An organization can take what it believes are appropriate measures to protect its infrastructure from being the victim of worm attacks but can fall victim to attack if a rogue or system out of its control introduces the worm into the information infrastructure. This often happens when a consultant or home user enters the environment without having the system they use appropriately protected or in compliance with the security policy of the organization.

The problem is also not only restricted to systems directly interfacing to the information infrastructure through internal or secure network connections. The prevalent use of web enabled capabilities to provide remote access to the information infrastructure also introduces a new level of risk. The widespread access by potentially unknown users with unknown intentions requires a more acute focus on web access points.

Web Environment Security Considerations

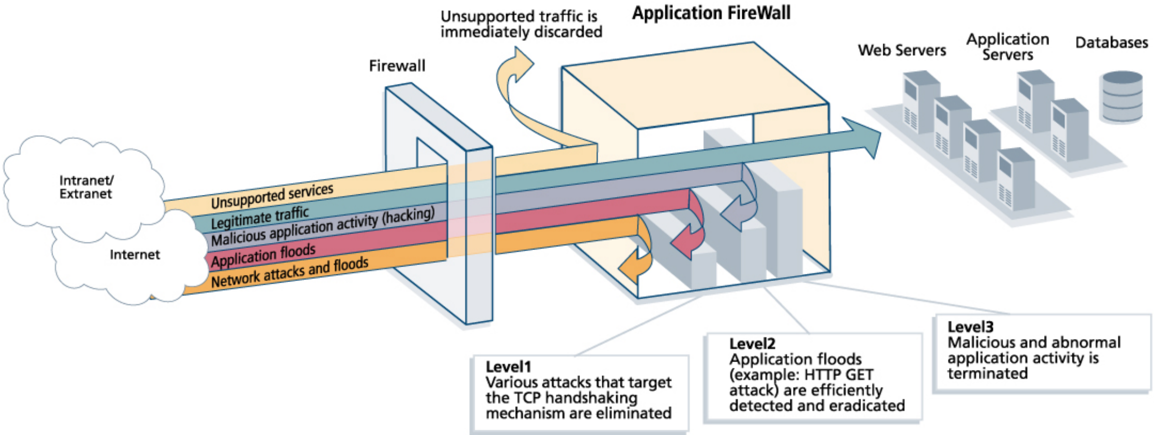
The World Wide Web is no longer an emerging business tool. It has become essential for almost every business today. The ability to provide solutions such as customer self-service and electronic commerce has enabled businesses to be more successful and to enjoy a high degree of customer satisfaction. Unfortunately, only recently have organizations come to realize the intricate and numerous security considerations they must address in order to deploy and operate these solutions securely.

One security solution often implemented in web environments is stateful inspection based firewall technologies. These technologies rely on analysis of the headers of TCP/IP data packets for data points that they then compare to policies, which have been defined for the environment they are protecting. Among other things, the header information will tell the firewall device the source and destination IP addresses, the port or service the packet would like to access, and whether or not the packet is fragmented in any way. It does not, however, investigate the packet payload to examine whether or not the traffic is appropriate for the environment it is attempting to access.

While stateful inspection firewalls are very effective in protecting the corporate network infrastructure, they may not be as effective in protecting Internet facing web environments. If you consider that most of those do not have a known source pool of addresses that should be accessing the environment, and that most traffic will be addressed to port 80 (HTTP) or port 443 (SSL), the abilities of the stateful inspection firewall are limited. That is because most of the current attacks against web-enabled solutions utilize these ports as their entry points into the solution. The use of application firewalls is emerging as the leading practice for protecting web-enabled environments, especially those that are Internet-facing and open to access by the general populace

Application firewalls can provide not only stateful inspection capabilities, but also packet payload inspection mapped to workflow activities for appropriate actions by users within the web environments they are protecting. By providing this level of capabilities, application firewalls can also help reduce the pressure for bug-free code and real-time patch capabilities for web-enabled environments.

Application firewalls can provide this capability because they can create a shield around the solution they are protecting, which in turn can provide some breathing room for the information security, development, and operations organizations to properly assess new risks and exploits as they are identified. Having the application firewall in place allows for a structured and measurable response to code development, enhancement and patch management.


Unsupported traffic is immediately discarded
Application FireWall
Web Servers
Application Servers
Databases
Firewall
Intranet/ Extranet
Internet
Unsupported services
Legitimate traffic
Malicious application activity (hacking)
Application floods
Network attacks and floods
Level1
Various attacks that target the TCP handshaking mechanism are eliminated
Level2
Application floods (example: HTTP GET attack) are efficiently detected and eradicated
Level3
Malicious and abnormal application activity is terminated

One of the business benefits also afforded by the use of application firewalls is the ability to meet the constant demands of customers and the marketplace for new features and capabilities. The current trend for completely secure and bug-free solutions is admirable but not realistic in many organizations. By implementing application firewall technologies as a shield around a solution, an organization can offset the risks of imperfect development. This will allow the organization to continue focusing on its core competencies and development of business-driven features and capabilities instead of having to focus solely on security as its top priority. This allows the organization to balance security against the business' need for continued growth and success.

Remote Access Security Considerations

Remote access has quickly evolved in the last couple of years to include a much wider range of users than just road warriors and telecommuting workers who need access to e-mail. The availability of wireless and cable modem/DSL capabilities for the user population has created a vast remote user population. This population is no longer just accessing e-mail remotely, but is now actively exploiting the organization's complete information infrastructure.

Organizations should take a few key steps to accommodate the needs of those users while ensuring the security and integrity of the environments they are accessing. The first is to ensure that strong authentication techniques are used to ensure the identity of the users accessing the environment. These techniques can take the form of client-side digital certificates or multi-factor authentication methods such as tokens or biometrics.

One of the most important security solutions to introduce in this kind of environment is the enterprise quarantine solution. This is the concept of isolating and assessing a user's security posture prior to allowing them access to the information infrastructure. A user will authenticate themselves to the environment, and then have the accessing system analyzed to ensure that it meets the appropriate security levels defined by the environment's security policy. If they do not meet the appropriate security requirements they should be given the ability to update their systems appropriately, but not allowed to enter the environment until they have done so. Until this requirement is in place the user should be quarantined to both physically and logically separated networks. That will help significantly reduce the risk of a remote user introducing security problems into the organization's information infrastructure.

Considerations and Risks Concerning Mobile Data Devices

An inexorable trend today is use of wireless-enabled personal data assistants and smart phones. This means that the remote-access workforce has begun to transport sensitive and valuable information outside the physical boundaries of the organization on a regular basis. These devices thus pose a greater risk to the organization because they can store sensitive and valuable information in a small form factor that is easily misplaced or stolen and have the potential to be compromised from a distance.

Adversaries have already begun to understand the benefits of compromising those devices. In the cases of personal data assistants and smart phones the risk comes from the amount of data typically and often unknowingly stored in these devices. Most users synchronize these devices to their desktop or laptop systems and assume in many cases that their contact databases and calendars are the only items transferred to their mobile devices. This information can be dangerous, but the risks can also measured and understood. What users often do not realize is that other data, such as meeting notes, password reminders, is often also transferred to these devices during the synchronization process. In addition, an adversary can compromise the data on wireless-enabled devices without physically accessing them.

Wireless-enabled devices represent such a significant business benefit to most organizations that forbidding their use because of security considerations is not an option. They can, however, be governed by policies, processes, procedures, and tools that can help mitigate the risks they can pose to an organization. Beyond password protection and encryption tools, education is the best current risk mitigation strategy for these devices. Users need to be aware of the risks that the devices pose as well as the techniques they can use to mitigate the risks. The combination of technology tools and education can help ensure that those tools continue to benefit the business goals of the organization without putting its valuable information resources at risk.

Emerging Security Solutions

The solutions to securing information infrastructure are evolving as quickly as the attack methodologies. Three key concepts being introduced significantly increase the security posture of the information infrastructure. These are:

- A programmatic approach to information security
- Threat and vulnerability management programs
- Defense-In-Depth

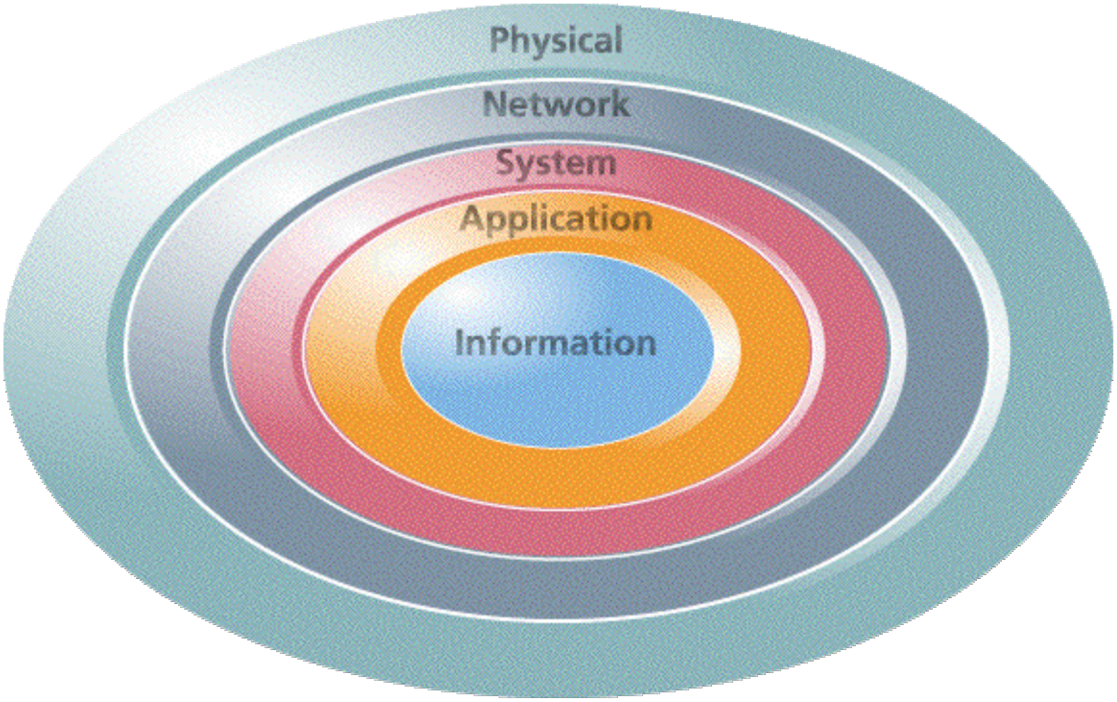
The introduction of these concepts represents a fundamental shift from technology-focused, incident-driven reaction to a business-focused, proactive approach to information security.

A programmatic approach to information security is a structured, measurable, business-driven process for securing information within an organization. This approach uses controls and key performance indicators to ensure that appropriate measures are in place to properly secure the organization's information infrastructure. The programmatic approach also ensures alignment to the business and compliance goals of the organization. It accomplishes that by introducing formal communications channels between the information security and business elements of the organization.

Threat and vulnerability management solutions approach information security from a proactive perspective by using threat analysis and threat management concepts. Threat analysis involves using a consistent methodology to evaluate and prioritize the threats to which an individual solution or an entire organization may be vulnerable. This analysis will employ intelligence, asset information, and other data points to determine the likelihood, severity, and possible business impact of potential threats. Once they have obtained this information, those in charge of security can assign a threat level or threat designation to specific solutions and the organization as a whole. That allows security investment decisions to be based on educated assessments instead of fear, uncertainty, and doubt.

Using the information supplied by threat analysis, the vulnerability management element creates attack and event-response plans in advance against identified vulnerabilities. These response plans include prescriptive guidance on how to identify and appropriately respond to an attack or event. Those responsible for these identification and response plans can then forward them to the operations organization, which can use the information to implement identification and remediation steps within automated monitoring and incident response systems.

The implementation of new methodologies and a structured approach to information security are all elements of a concept known as Defense-In-Depth. Defense-In-Depth represents the concept of a layered security model. In this model, multiple layers of independent security capabilities and functions are implemented to safeguard access to information assets. By implementing multiple independent layers of security, an organization significantly improves it security posture: an adversary would have to penetrate these layers undetected at any point in order to succeed in gaining information access.   An organization that implements Defense-In-Depth properly can have a high level of assurance that it is adequately protecting its information assets from both malicious adversaries and user error.



Business-Enabling Security Solutions

The emerging landscape of information security is being defined by business impact rather than technology-driven security models. Traditional defenses based on individual security devices are being replaced by models based on threat assessment. Those models use technology as a tool to implement the policies, procedures, and guidelines defined by the business to remediate the identified threats to the information infrastructure elements that are at risk.

This new class of information-security solutions is business-enabling not least because the solutions are transparent to the user. Security solutions considered roadblocks to success by the user base they are intended to protect (e.g., long and diluted passwords, blocked firewall ports) are not only business-debilitating, users also tend to circumvent them. Solutions such as Secure Socket Layer (SSL)-based VPNs, which allow remote users to access the corporate information infrastructure from any web-enabled facility, and workflow based security solutions such as application firewalls provide high levels of security without presenting roadblocks to appropriate work activities.

Conclusion

Emerging information security solutions are driven by the expanding business value of the assets they are protecting. The expanding regulatory climate is also forcing organizations to rethink how they are approaching information security. They are increasingly moving from a reactive, event-driven model to a proactive, threat-driven one. The current threat models and attack profiles have shown that the adversary community is becoming more intelligent and focused in its attack methods. The traditional “spray and pray” network attack is being replaced with well-planned and targeted application attacks. It is important that organizations understand this well as they implement protection for the information infrastructure.

By investing in a proactive, programmatic strategy for information security and adopting the defense-in-depth methodology, an organization can ensure that it is doing everything that it can to protect its information infrastructure. That will also ensure that the information security solution is not an unintended obstacle to success, but a true business enabler.