Realtime
publishers

The Shortcut Guide™ To

Business Security Measures Using SSL

sponsored by

Now from Symantec. | VeriSign Authentication Services

Dan Sullivan

Chapter 4: Best Practices for Implementing a Business-Centric Security Management Strategy ... 31

Protecting Critical Servers ... 32

What Constitutes a Critical Server? ... 33

Using Encrypted Communications ... 34

Hardening Server OSs ... 35

Locking Down Databases ... 36

Protect Mobile Devices and Communications ... 36

Encrypt Communications with Mobile Devices ... 38

Authenticate Mobile Devices with Digital Certificates ... 38

Maintain OS Patches ... 39

Keep Antivirus Up to Date ... 39

Use Encryption on Mobile Devices ... 39

Network Defenses ... 40

Deploying and Configuring Network Perimeter Devices ... 40

Firewalls ... 41

IPSs ... 41

Network Access Controls ... 42

Filtering Content on the Network ... 42

Monitoring and Auditing Network Activity ... 43

Security Awareness ... 43

Security Awareness Topics ... 44

Effective Security Awareness Training ... 44

Checklist of Practices and Technologies ... 45

Copyright Statement

© 2009 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers or its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

This sponsored eBook is valid until July 12, 2012.

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. VeriSign, VeriSign Trust and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. Other names may be trademarks of their respective owners.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library for IT Professionals. All leading technology eBooks and guides from Realtime Publishers can be found at http://nexus.realtimepublishers.com.]

Chapter 4: Best Practices for Implementing a Business-Centric Security Management Strategy

A business-centric security management strategy is multifaceted and takes into account both the technical and organizational aspects of information security. Throughout this guide, we have seen how security threats and vulnerabilities can undermine business operations and integrity, and we have discussed methods for developing a security strategy. In this, the final chapter of the guide, we turn our attention to examining best practices for implementing a business-centric security management strategy.

So how is business-centric any different from other approach to information security? The starting point is the business strategy. What are the goals and objectives of the business (or other organization) and how are they implemented? The answers to those questions start to frame the security discussion because we can assess risks to particular business processes and assets. Part of that assessment process is determining a relative value for an asset or process that is being protected. For example, we wouldn't invest more than the value of car in an anti-theft device for the vehicle. The same logic applies in information security. We mitigate risks to business information assets according to the value of those assets and the priority we assign to them.

Once we understand threats, vulnerabilities, and the risks and costs associated with them, we can then formulate a security strategy for protecting the business. This chapter examines specific methods for mitigating information security risks. As we shall see, one security control, or measure, can help reduce multiple risks, and every risk is ideally mitigated by more than one control. Of course, the reality of business is that we cannot always have our best case scenario, but we strive to get as close as possible.

The fundamental areas of a business-centric security management strategy span a number of areas and include:

- Protecting critical servers
- Protecting mobile devices and communications
- Deploying sufficient network defenses
- Providing end user training

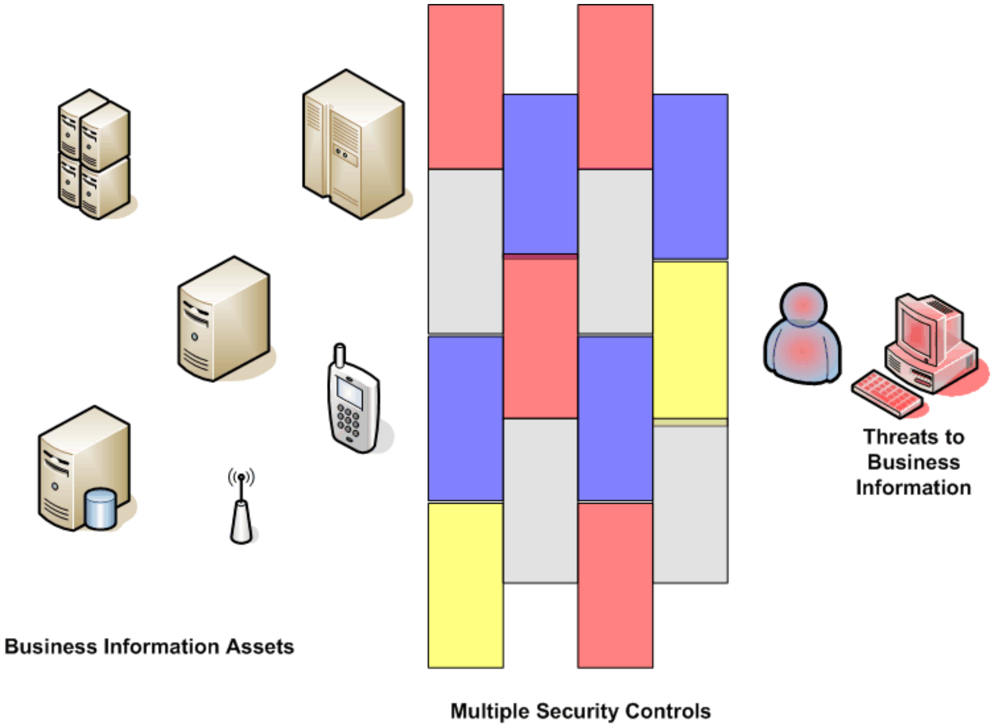
Business Information Assets
Multiple Security Controls
Threats to Business Information

Figure 4.1: A guiding principle of best practices in business-centric security strategy is to apply multiple security controls in an overlapping manner to create a defense-in-depth approach to mitigating risks.

The drivers behind the best practices in each of these areas are the need to maintain the confidentiality of business information, integrity of that data, and the availability of information systems and assets. What follows is a non-exhaustive set of best practices that serve those drivers. Servers that support critical applications, maintain enterprise databases and perform other essential functions are a good place to begin our discussion.

Protecting Critical Servers

A critical server is one that, if it were to go down or otherwise have degraded performance, would have an adverse impact on business operations. Examples include email servers, database servers, and application servers used in production environments. It is important to classify servers in terms of their criticality because, as with data classification, some servers are more important than others; when it comes time to allocate information security resources, it is imperative to know how to prioritize server security spending.

What Constitutes a Critical Server?

How do we distinguish critical servers from non-critical servers? We need to start with business strategy and the business processes put in place to support them. Note that we do not start by asking opinions of users of those servers. Developers, for example, may consider their servers critical because in effect they are "production" servers from their perspective. If developers' database server goes down, they will not be writing much database code; that does not, however, make it a production server and therefore possibly a critical server. Of all the production servers, some of these are critical because business processes depend on them, and if they were to fail, the business process could not be executed or could only be executed at a significantly slower pace.

Clearly this is a gray area where reasonable people can disagree. For example, many of us might consider a Web server hosting a site on corporate charitable giving as a production system but not critical; if it were down for the day, it would be an inconvenience but work could be made up when the system is restored. In general, we can think of server categorization as a subset of all enterprise servers that are most important for business operations. Many, but perhaps not all, production servers may be categorized as critical.

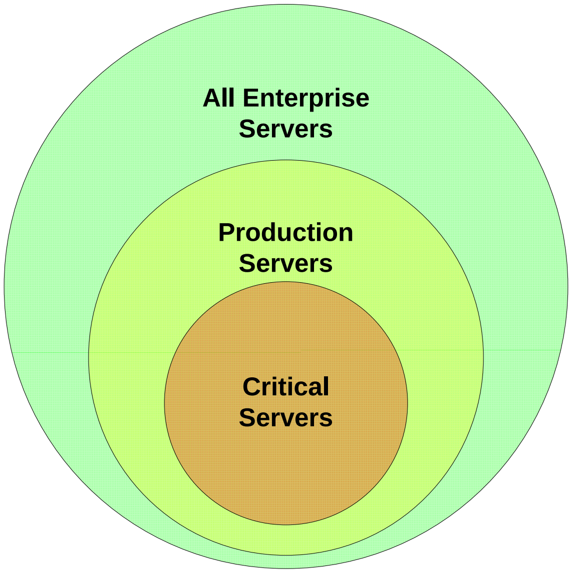

Figure 4.2: Servers can be categorized in terms of criticality to business operations. Critical servers have the highest priority for security measures because their disruption can have significant adverse impact on business operations.

Once critical servers have been identified, we can apply a defense-in-depth strategy to protect them. We should apply these principles to all servers if possible, but we should start with critical servers, then other production servers, and then to all other enterprise servers if there are sufficient resources.

Some of the multiple, overlapping security measures we can use include:

- Encrypted communications
- Hardened operating systems (OSs)
- Locked-down databases running on those servers

These three measures represent the types of controls that can be applied to protect information exchange between servers, reduce the attack surface of the OS, and reduce vulnerabilities in core applications running on these critical servers.

Using Encrypted Communications

Servers can house data from the various data classification categories, such as public, sensitive, private, and confidential.

- Public data can be freely disclosed; sensitive data should not be disclosed but would not cause significant harm to the company if it were disclosed.
- Sensitive data should not be disclosed, but if it were, that would not cause significant harm to the organization. Examples of sensitive data include project schedules and approved vendor lists.
- Private data is data about a third party, such as a customer or patient, that must not be disclosed outside of established procedures.
- Confidential data is company proprietary data, such as trade secrets, that need to be keep tightly controlled to prevent adverse affects on the organization. In theory, we might only be concerned about protecting communications when private and confidential data is involved; however, as servers may share different categories of data, we should apply security to protect the category of data warranting the most control.

Consider a Web application with a product and order database. The product catalog—including product lists, descriptions, and current pricing—is public information. Customer order data, including shipping addresses, billing addresses, and credit information, is private. Rather than risk disclosing private customer data, all communications between the application and the customer should be protected with encrypted communications.

SSL/TLS communication is the industry standard method for secure communications (TLS is also known as SSL version 3). It provides authentication so that we can verify the identity of the server we are working with as well as encryption of data communications between servers or between servers and clients. (Actually, the SSL/TLS standards do not require encryption of data to be compliant with the standards, but SSL/TLS is often used for encryption).

SSL encrypted communications can help mitigate a number of threats:

- Man-in-the-middle attacks in which an attacker intercepts a message between parties and alters the message stream. SSL encryption scrambles the content of messages and related services, such as digital signatures, and provide authentication and non-repudiation functions.
- Eavesdropping on communications. Protecting against this threat is especially important if the communications travel over unencrypted or weakly encrypted wireless networks. An early wireless encryption standard, WEP, is fairly easily cracked and should not be depended on to protect the confidentiality of server-to-server or server-to-client communication. Fortunately, if the server encrypts data using SSL before it is sent over a weakly protected wireless network, attackers will not be able to decipher the message in any reasonable period of time.
- Insider attacks from persons with access to internal communications. An internal attacker who does not have access to an application or database may still be able to capture data from those systems if the data were transmitted in unencrypted form. Even in the case of communications between internal servers, there is often a need for encrypted communications.

Remember, data in motion is not protected by the application and database access controls that help protect that data when it is at rest.

Hardening Server OSs

Hardening an OS reduces the potential vulnerabilities by using several techniques:

- Changing default configurations
- Removing default accounts
- Shutting down services that are not required
- Removing applications not needed in a production environment, such as removing compilers on production servers that run applications developed and compiled on other servers
- Reducing privileges on all accounts to the minimum set needed to perform business operations
- Patching the OS to apply security updates

Resources

For more information about hardening OSs, see the Bastille Hardening program at http://bastille-linux.sourceforge.net/ and Center for Internet Security Benchmarks at http://cisecurity.org/bench.html.

We should also apply the same principles to enterprise applications running on these servers. We'll consider databases as an example.

Locking Down Databases

Databases are a prime target for attackers because databases often store valuable information. Even if the server uses SSL-encrypted communications and the OS is hardened, attackers may be able to steal data by attacking at the application layer.

Locking down a database includes several steps:

- Removing or disabling default accounts and schemas
- Changing default passwords
- Removing unnecessary database options
- Securing the database listener, the process that establishes connections to the database
- Applying access controls to database files and directories
- Implementing strong password policies or other authentication measures to reduce the risk of password-cracking attacks

In addition to securing the database server, developers should be aware of coding techniques for avoiding SQL injection attacks. All the measures previously listed will not block an apparently legitimate query that is sent to the database by an approved application. It is the developers' responsibility to implement application code that is not vulnerable to such attacks.

> **Resource**
>
> See Colin Angus Mackay's *SQL Injection Attacks and Some Tips on How to Prevent Them* for more on this topic.

In addition to protecting servers, businesses should adapt their security measures to protect information when it is stored or used on mobile devices.

Protect Mobile Devices and Communications

Mobile devices are now commonplace. Smartphones, netbooks, laptops, and other mobile devices are de facto parts of the IT infrastructure. We do not generally consider mobile devices as part of the IT asset base, which includes servers, network hardware, desktop devices, and so on. This must change. Employees, business partners, contractors, consultants, and customers are using mobile devices to conduct business. Businesses with large consumer customer bases, such as banks, are creating mobile versions of their online services, such as online banking. Mobile devices are an established and widely adapted platform that we need to consider in a business-centric security strategy.

There is a significant difference between many mobile devices used for business and other IT hardware: the mobile devices are often not owned by the business. Obviously, this means that a business is not in full control of the device, thus,

- There is no standard platform for all mobile devices used for the business
- IT probably does not have an inventory of mobile devices
- These devices are not managed within a business' asset management program

There are, however, ways businesses can control what business data and business operations are allowed on non-business-owned mobile devices. This is done through a series of security policies that define security controls that should be in place before business is conducted with an employee-owned mobile device. These policies assert a business need to protect information assets while recognizing that the mobile device is ultimately owned and controlled by someone else. To distinguish these different types of devices, we will refer to employee or other third-party owned devices as semi-managed devices.

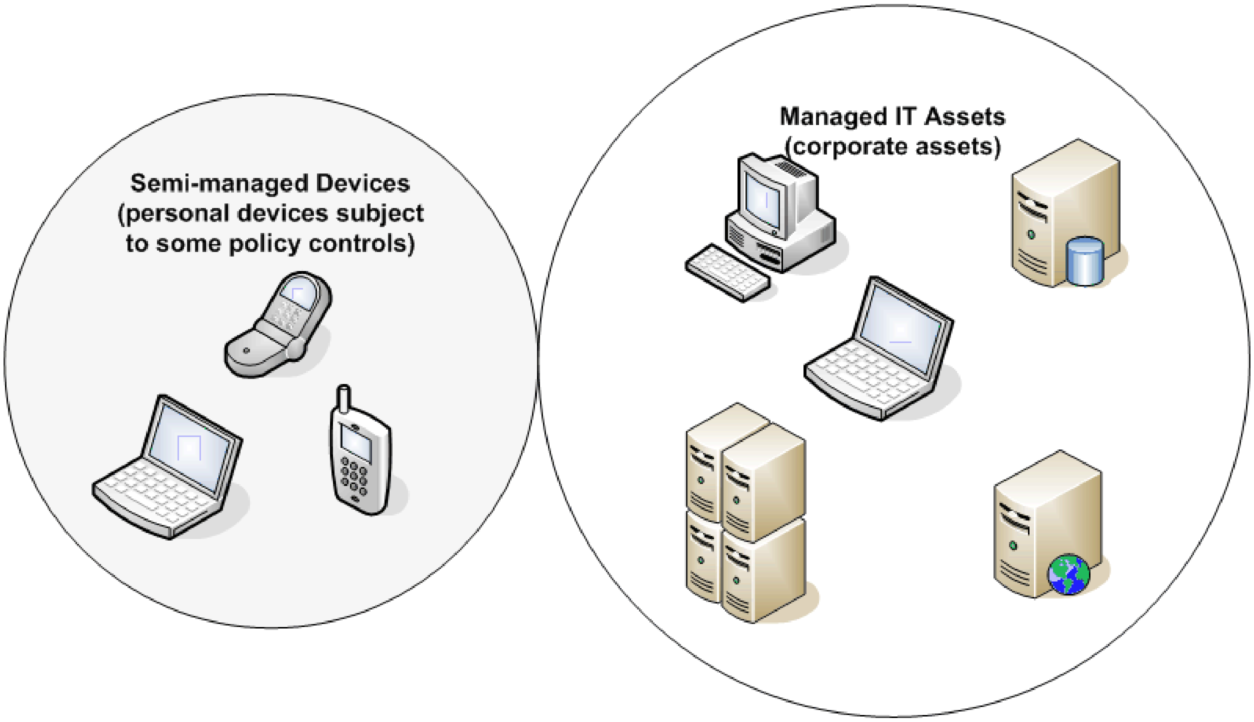

Figure 4.3: Mobile devices owned by employees are only semi-managed; however, they may be subject to policies governing conditions under which business data may be stored or transmitted to those devices.

For both managed and semi-managed mobile devices, businesses can use several policy and technical measures to reduce risks to data related to mobile devices:

- Encrypting communications with mobile devices
- Authenticating mobile devices with digital certificates
- Maintaining OS patches
- Keeping antivirus software up to date

As with server security, we use multiple measures in to implement our defense-in-depth strategy. That strategy enables us to mitigate multiple risks with a single security control and to apply multiple controls to individual risks.

Encrypt Communications with Mobile Devices

Data that is transmitted to and received from mobile devices may be sent over wireless communication providers' private cell phone networks as well as the Internet. This may not be a concern for many types of communications, but when dealing with private and confidential data, especially when there is a regulatory responsibility to protect this data, encrypting communications to mobile devices may be necessary.

Unlike some of the other security controls we can dictate for mobile devices, this one is well within the control of the business. Private and confidential data is sent only over an SSL-encrypted communication channel. Part of the SSL protocol defines a handshaking procedure between the server and client, so we can be sure that the client will receive the data only after establishing a secure connection. Of course, without sufficiently strong authentication, we run the risk of transmitting data to a spoofed device.

Authenticate Mobile Devices with Digital Certificates

Digital certificates are a key part of ensuring we are communicating with the mobile device we believe we are communicating with. This allows parties in a communication session to authenticate the identity of the devices with which they are dealing. Let's take a look at digital certificate capabilities on a couple of mobile device platforms.

When using the Windows Mobile 6 OS, it is relatively easy to install digital certificates. Windows Mobile is preconfigured to manage three types of certificates:

- Personal certificates maintained in the MY store
- Intermediate Certification Authority (CA) certificates, which are stored in the CA store
- Root CAs, which are stored in the ROOT store

These certificates are used by applications communicating with the device. For example, Microsoft Exchange ActiveSync verifies the trustworthiness of a device by examining its digital certificate. Windows Mobile also provides a cryptography application programming interface (API) for working with digital signatures and digital certificates.

The popular Blackberry smartphone also supports digital certificate-based authentication. These mobile devices support the Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) for mutual authentication and the use of client digital certificates.

Mobile device vendors and software developers are providing some of the tools needed to secure mobile device communication and provide for digital certificate-based authentication. It is business' role to create policies defining when this functionality should be used.

Maintain OS Patches

Mobile devices are like other devices on the corporate network: they run with complex OSs that occasionally need to be patched. Not all patches are security patches, but when a patch is released to correct a vulnerability, the patch should be installed in order to reduce risks.

Many smartphones are personally owned, so businesses cannot force device owners to patch. There may be legitimate reasons for not patching. For example, if a patch to correct one problem introduces another, the user may conclude from their perspective that they would rather live with the security vulnerability. This may not be in the best interest of the business.

In general, there are two methods for ensuring devices are properly patched and configured. Network access control servers can query a device trying to connect to the network and determine whether the device's configuration meets minimum requirements. This works well when a conventional laptop running Windows connects to the network, but may not be sufficient for all the smartphone platforms that could try to establish a connection. An alternative method, and one that should be in place even if network access controls are in place, is a policy that dictates the configuration and security expectations for using a corporate network. This obviously does not have the same enforceability that technical controls have, but it at least puts users on notice that there are minimum security requirements for using a smartphone within the business network environment.

Keep Antivirus Up to Date

In a similar manner, mobile devices should maintain up-to-date antivirus and other anti-malware applications. Applications running on smartphones can open infected documents and inadvertently download malicious content as easily as they can on laptops, so comparable protections should be in place on both platforms.

Use Encryption on Mobile Devices

It would be unfortunate if the data communicated over an SSL-encrypted channel were leaked once it arrived at the mobile device because of unencrypted storage. SSL encryption only protects data in motion; once it lands on the device and is decrypted during the last steps of the SSL communications protocol, it is up the platform OS and applications to protect the data. Device encryption is one part of the solution to the problem. When selecting an encryption program for a mobile device, be sure to consider the need to encrypt data on permanent and removable media, such as SD cards.

Protecting mobile devices and communications requires multiple layers in accordance with a defense-in-depth strategy. These layers include encrypting data during communication with SSL technologies, authenticating devices with digital certificates, maintaining OS patches, keeping anti-malware up to data, and mitigating the risk of a data leak by using device encryption for both permanent and removable storage devices.

Network Defenses

Network security was at one time practically synonymous with information security. We've moved well beyond those days as we see from the demands for mobile device and communication security. Network security is still an essential element in information security, of course, and no description of business-centric security management, no matter how brief, would be complete without it. The following discussion is not exhaustive but does highlight the controls that can be used to mitigate threats to the network and to devices on the network. These include:

- Deploying and configuring network perimeter devices
- Filtering content on the network
- Monitoring and auditing network activity

Deploying and Configuring Network Perimeter Devices

The purpose of network perimeter devices is to keep malicious attackers, content, and software off the network while preventing valuable data from leaking. This goal is easily stated but the implementation is somewhat more complex. For starters, the types of material that should be blocked range from malicious software to content that is offensive or inappropriate for the business environment. Preventing data leaks is challenging because it requires policies and rules that define the type of content that should not be sent unencrypted outside the network as well as how to identify that type of content. (One of the additional benefits of using SSL encryption is there is significantly less risk of the content that legitimately leaves the network being compromised by data thieves).

Blocking malicious content and unauthorized access requires a number of security controls:

- Firewalls
- Intrusion prevention systems (IPSs)
- Network access controls

These controls complement each other by addressing different types of threats.

Firewalls

Firewalls are still a staple of network security although architectural changes have made the perimeter more porous than it has been in the past. Firewalls have evolved from stateless devices that could block or not block a port or filter out a particular type of network traffic to systems that can inspect deep into the contents of the packet, use information about the state of a session, and apply application-specific rules to identify and block unwanted content.

Network firewalls can still act as gateways between network segments and should be deployed where clear lines of separation are needed. Application firewalls should also be used when there is a need to filter content to critical applications. For example, an application firewall may be used to scan input to a Web application in order to block user input designed to conduct a SQL injection attack. This type of application firewall would provide one line of defense against SQL injection attacks. Developers who write code that cleanses user input, use stored bind variables, and other techniques for avoiding SQL injection vulnerabilities constitute another line of defense. Both are needed when practicing defense in depth. As more programmatic services depend on HTTP to send and receive data, the traditional role of the port-blocking firewall is changing. Blocking most ports but allowing HTTP data still allows a great deal of traffic into the network. Application firewalls and other means of deep packet inspection are required to detect threats tunneling in on HTTP traffic.

IPSs

IPSs should be deployed to monitor the state of the network and hosts. IPSs can use signature patterns, behavioral analysis, or both to detect anomalies on the network, such as:

- Large volumes of traffic from a server that normally has low traffic activity at that time of the day
- Attempts at password cracking
- Known OS vulnerability attacks
- Denial of Service (DoS) attacks
- Web application exploits

Unlike firewalls, IPSs are not about just blocking content by packet type or port but analyzing content and its impact on devices. This functionality is important because not all malicious content can be blocked by gateway devices. Some malicious content is not apparent until it enters the network and begins to interact with devices on the network; that is when an IPS can provide additional measures to detect and block that kind of activity.

Network Access Controls

Network access controls are gatekeepers for allowing and blocking access to network resources. Whereas firewalls operate at the packet level to block content, network access controls determine who and what devices will be allowed to establish a connection to a corporate network. Ideally, a deployed network access control will enforce established policies, such as:

- Who is allowed to access the network based on their identity
- User roles to determine what resources users may access once they have established connections to the network
- Ensure devices connecting to the network meet minimum configuration requirements
- Vary access privileges based on the type of device; for example, allowing only limited access to network resources from unmanaged devices

Network access controls are recommended when remote users regularly connect to the network, especially when unmanaged devices are used to work with corporate assets.

Filtering Content on the Network

Content filtering is a network-based method for scanning content as it enters or leaves the network to prevent unwanted material such as:

- Viruses, worms, Trojans, and other malware
- Spam and phishing emails
- Spyware and adware
- Content that is offensive or inappropriate for a business environment

Most endpoint devices today, such as desktop workstations and laptops, run a full suite of anti-virus, anti-spam, and anti-spyware applications but network protection is also advised. The combination of endpoint-based security measures and network-based measures provide defense in depth against these threats.

Network content filters have an added benefit of keeping employees and others from downloading content from or surfing to inappropriate sites while on the job. For an additional layer of defense, businesses can use third-party Web content-filtering services, such as the free OpenDNS service (http://www.opendns.com/). This service provides domain name services but also allows users to block access to specific types of sites, such as adult, gambling, shopping, and other user selectable categories.

Monitoring and Auditing Network Activity

An unintended consequence of deploying various network security devices is that these devices can generate a great deal of log data. This presents a set of all-too-common problems:

- Each type of device generates log data specific to the device
- The data is distributed across different systems
- There is so much data that it is sometimes difficult to cull out useful information

One way to help improve the management efficiency of network monitoring is to use a log aggregation tool. These can collect data from multiple devices using common protocols, such as Simple Network Management Protocol (SNMP), and perform basic data transformations, such as normalizing timestamps. The advantage of these log aggregation tools is that a network manager can retrieve multiple types of log data from a single application, and basic integration has already been performed. The quality of integration and the ability to detect and highlight important events will likely improve in the future, but these tools can still reduce the burden on network management today.

Network security measures are like common goods, all parts of the infrastructure and business processes benefit from their use. If we start with a business-centric view of network security, we would want many of the standard network security controls, such as firewalls, IPSs, and network access controls. Also, monitoring network activity can become time consuming without tools that can help managers keep up with the volume of log data that these other security measures generate.

The collection of technical controls we have discussed, from measures to protect critical servers and securing communications to protecting mobile devices and network assets, are just one part of a business-centric security strategy. Another part is a focus on end user training on information security.

Security Awareness

The old adage says a chain is only as strong as its weakest link—the same goes for information security. Too often, it is the users, and not technical controls, that fail us. A business-centric security strategy needs to consider security awareness topics and training delivery methods to mitigate threats due to human error and poor judgments.

Security Awareness Topics

The range of security awareness topics that could be covered in training is as broad as the threats, vulnerabilities, and countermeasures that security professionals deal with on a day-to-day basis. We do not need to turn all users into security professionals, and it is sufficient to focus on several fundamental topics that together can help mitigate threats:

- Training on security policies within the organization
- Types of threats to the devices commonly used in business, including mobile devices
- The need to protect data in motion with SSL-encrypted communications
- Threats from spoofing and mistaken identity and how to prevent it with the use of digital certificates
- Threats of data breaches from lost or stolen mobile devices and the need for encrypting stored data
- Phishing and other forms of social engineering attacks
- Malware, infected documents, malicious Web sites, and drive-by downloads

Admittedly, some of these topics can be a bit dry (only some of us care to delve into the details of things like SSL/TLS handshake protocols). How we present security awareness training is as important as what we present.

Effective Security Awareness Training

Effective security awareness training is delivered in a business context, not a technical context. Business users do not need to know the intricacies of asymmetric encryption, but they do need to understand that their business data is threatened if they lose their laptops or someone intercepts their wireless communications while emailing from a coffee shop. Another important aspect of context is the security policies that a business establishes. Those policies are formulated for a reason that must be conveyed to the users. In general, security awareness training should focus on business fundamentals, such as protecting the confidentiality, integrity, and availability of systems. With those as framing principles, the training can then move on to examine high-level threats, including malware, phishing and social engineering attacks, and data breaches. Next, we can focus on solutions, such as SSL encryption, digital certificates, safe browsing practices, and clues to watch for in phishing scams. Not everyone finds information security an engaging topic, and they shouldn't have to in order to understand the impact of security risks to the business.

Checklist of Practices and Technologies

We have covered quite a few topics in this chapter; to recap, the following quick checklist of practices and technologies can be incorporated into your business-centric security strategy:

- Secure communications with SSL—Data in motion does not have the advantage of the access controls in place with data at rest; encryption provides added protection against a number of threats
- Use digital certificates to authenticate devices from servers to mobile devices—Rather than assume we can trust the device to which we are about to send confidential data, verify the device's identity first
- Protect against malicious content with anti-malware and content filtering on the network and on endpoint devices
- Use network security controls such as firewalls, IPSs, and network access controls
- Develop a patch management plan to ensure OSs and critical applications, such as databases, are patched against security vulnerabilities
- Monitor network and host activity—The volume of log data from devices can be substantial; data collection and reporting tools can help
- Train end users by focusing on delivering information from a business-centric, not a technical, perspective
- Think in terms of defense in depth and use multiple security controls to protect against a single threat—Fortunately, many security controls protect against multiple threats as well

To summarize, a business-centric security strategy starts with the requirements of business, assesses the threats and vulnerabilities to the business, and formulates a combination of organizational and technical controls to mitigate risks. Several technologies, such as SSL-based encryption, digital certificates, anti-malware, and network security controls, as well as organizational controls, including polices and end user training, can be used collectively in a defense-in-depth manner to improve the security of the enterprise.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.