Realtime
publishers
"Leading the Conversation"

The Shortcut Guide™ To

Protecting Business Internet Usage

sponsored by

SurfControl®

Dan Sullivan

Copyright Statement

Chapter 3: The Life Cycle of Internet Access Protection Systems

Protecting information assets is a multifaceted challenge. To begin, there are many kinds of threats to information assets, ranging from external attackers to natural disasters. There are correspondingly many defensive measures and risk mitigation strategies to reduce the potential impact of these threats. Once in place, security measures must be managed and maintained—particularly with an eye to keeping up with changing security conditions. And if there were a security breach, security and information management teams would have to respond to control the damage and recover as quickly as possible. This chapter will examine several key parts of the life cycle of Internet access protection systems:

- Assessing threats and appropriate prevention strategies
- Developing and maintaining policies
- Implementing multipoint solutions
- Maintaining and monitoring countermeasures
- Auditing
- Implementing incident response

Although the term “life cycle” is being used, it is worth noting that the relationship between these elements is not a strict cycle in which one element always follows another. For example, a forensic analysis of a security breach can depend heavily on information gathered during threat monitoring. Let’s begin the discussion of the life cycle with the core problem—threats to information assets and how to counter them.

Assessing Threats and Appropriate Prevention Strategies

The goal of information security is to preserve the confidentiality, integrity, and availability of information. To realize that goal, security professionals must contend with a wide variety of threats:

- Malware
- Network-based attacks
- Information theft and cryptographic attacks
- Attacks targeted to specific applications
- Social engineering
- Threats to physical security

This section of the chapter is organized into two parts. First, it will examine examples of threats and describe suitable prevention measures to each. The second section turns attention to guidelines for determining which of these measures to deploy and how to select them based on a cost-benefit analysis framework.

Categories of Threats and Defensive Measures

A comprehensive information security program will address many types of threats. Just as there is no single motive that drives all attackers, there is no single preventative measure that will protect assets against them. Some of the most common and well-known types of threats and suitable defenses are described in the following sections.

Malware: The Ever-Evolving Threat

Malicious software, or malware as it is commonly known, is a relatively dynamic category of threats. The techniques used to destroy data, disrupt services, and steal information have evolved to adapt to changes in security practices and countermeasures. For example, antivirus defensive measures can detect many viruses and worms by searching for patterns in the binary code that appear in the virus but not in other programs. These patterns are essentially digital fingerprints that are used to identify the threatening software. In response, virus writers developed stealth techniques to mask their malicious code (see Figure 3.1).

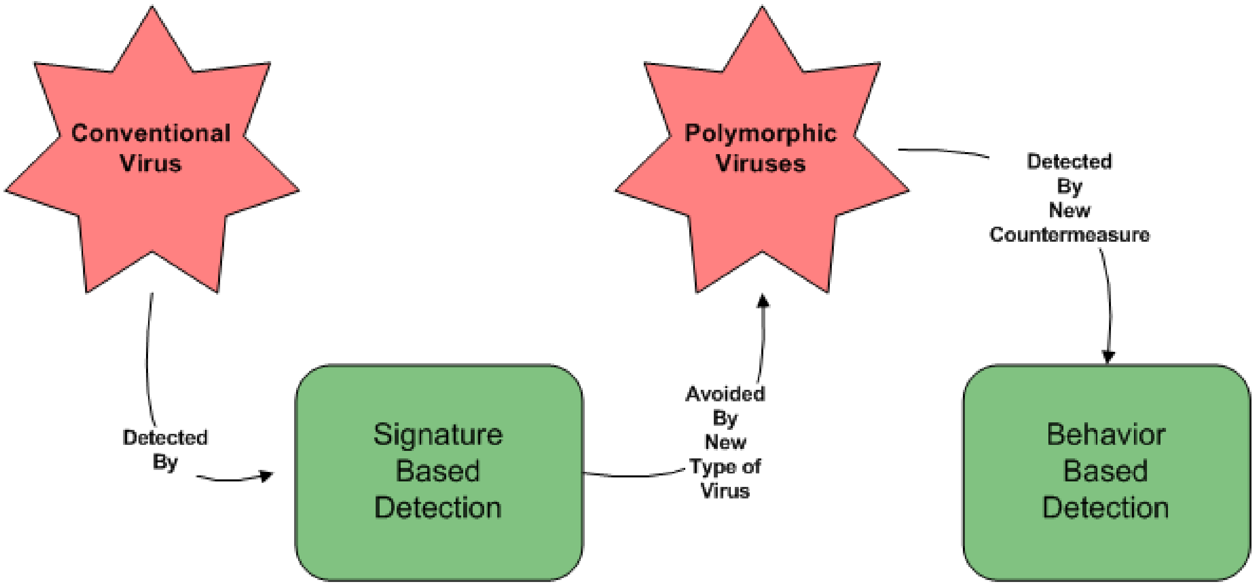
Conventional Virus
Polymorphic Viruses
Detected By New Countermeasure
Detected By
Signature Based Detection
Avoided By New Type of Virus
Behavior Based Detection

Figure 3.1: Malware and defensive measures change in response to each other.

Today's viruses are much more complex than the early boot-sector viruses that brought malware to the attention of IT users; they are also just one of several types of malware that now pose threats to information assets. Other common forms of malware include:

- Worms—Exploit vulnerabilities in operating systems (OSs), network services, and applications to propagate and cause damage
- Keyloggers—Capture keystrokes and transmit them to the attacker
- Video frame grabbers—Copy the contents of what appears on a computer display and transmit it to the attacker
- Rootkits—Hide the presence of themselves and other malware
- Trojan horses—Appear to be legitimate but in fact contain malware such as keyloggers and spyware

The countermeasures developed for detecting viruses can often detect other forms of malware as well. Deploying antivirus programs on client devices and scanning network traffic as it enters the network are appropriate defenses for combating malware. In addition, locking down client devices—for example, denying most users the privileges needed to install software or update the Windows registry—can prevent the installation of malware that manages to avoid detection.

Another effective, but easily overlooked, defensive measure is security awareness training. It is common knowledge now that you should not open an email attachment sent from someone you do not know. Less well known are tips such as avoiding sites that may harbor malware, such as peer-to-peer file sharing sites, and not downloading browser plug-ins that may be Trojan horses. Keeping users aware of the changing tricks and techniques used by malware developers and cyber-attackers is an effective complement to the technical countermeasures that are essential to preserving information assets.

📖 For more information about malware and related in-bound threats, see Chapter 2.

Network-Based Attacks

Network-based attacks are threats that are launched and controlled from a device or devices other than those under attack. Denial of Service (DoS) attacks and Distributed DoS (DDoS) attacks are examples of network-based attacks. These attacks use one or more devices to overwhelm the targeted server with so much network traffic or demands for services that the target cannot respond to legitimate requests.

Firewalls and intrusion prevention systems (IPSs) offer excellent defenses to these types of attacks. They use a few different techniques to detect and inhibit attacks. Some work by detecting patterns in network traffic indicative of an attack. These are analogous to using virus signatures in antivirus software; a large number of TCP connection requests, for example, can indicate an attack known as SYN Flooding, a crude but sometimes effective DoS attack.

IPSs can also use statistical techniques to analyze typical patterns of system use on a server or a network. These patterns are then used as a baseline for comparing with ongoing system use; any significant deviation for the baseline could indicate an attack. Complementing statistical technique are rule-based approaches that use heuristics, or rules of thumb, for detecting anomalies in system activity.

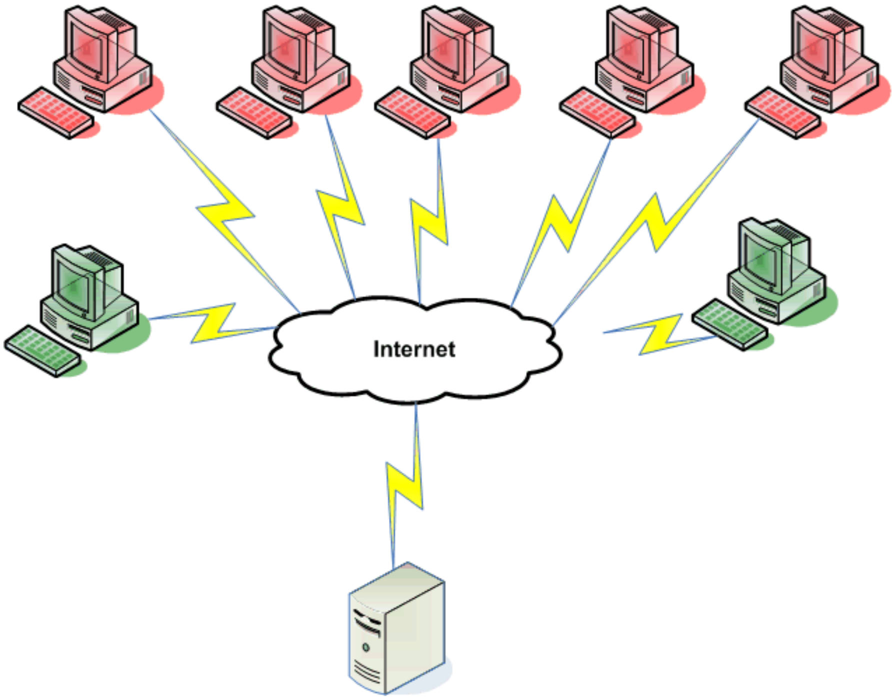

Figure 3.2: In a DDoS attack, multiple devices (red) flood a server with requests, overwhelming the server and blocking legitimate users (green).

Information Theft and Cryptographic Attacks

When sensitive information is transmitted outside of trusted systems, it should be encrypted to preserve confidentiality. Few consumers would want their credit card information transmitted through the Internet as plain text. Even when data is stored on an organization’s own devices, it is sometimes encrypted to prevent information theft. Several high-profile laptop thefts have raised awareness about the dangers of storing large quantities of personally identifying information on mobile devices.

Even when encryption is used, threats to confidentiality still exist. Two such threats are cryptographic attacks, or attempts to break the encryption code, and the loss of a private key in a public key cryptography system. The best method for countering cryptographic attacks is to use strong cryptography and properly manage the private key. Strong cryptography is based on sound encryption algorithms and long keys. For example, the Advanced Encryption Standard (AES), adopted as a standard by the U.S. government, can use 256-bit keys. Although in theory, a brute force search of all possible keys could be used to break this encryption, the time required to conduct such a search is so long as to be impractical. Of course, anyone in possession of the private key can decrypt even the most strongly encrypted message. It is imperative that private keys be securely distributed and stored to ensure that security is not compromised.

An important factor in the use of cryptography is that information should be encrypted only as long as that information is useful or not publicly available. Documents detailing a merger negotiation would be kept confidential during the negotiations, but once the deal is finalized and announced, the contents of those documents are far less valuable.

Attacks Targeted to Specific Applications

An emerging threat is the threat of specialized attacks against targeted applications. These attacks are focused on a particular database or application with the objective of gaining access to information or services. Economics is the primary driver of these types of attacks. Well-defined and enforced access controls, secure software development practices, and detailed monitoring of applications are required to combat these specialized attacks.

Social Engineering

Social engineering is the practice of deceiving legitimate users of a system into disclosing information that will aid the attacker in compromising system security. A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares she uses, what her password is.

A successful social engineering act requires the trust of the victim, so user awareness training about the problem is an effective defensive measure. Strict policies about service desk staff never asking for personally identifying information or passwords over the phone or in person can also help potential victims recognize a social engineering attempt.

Threats to Physical Security

Electronic defenses, especially perimeter defenses, can be defeated if attackers gain physical access to IT assets. If an attacker can reach an office, the attacker could:

- Install hardware keyloggers to capture keystrokes, including usernames and passwords
- Pose as a driver from a parcel delivery service and pickup backup tapes and disks
- Engage in social engineering with office staff to learn about security procedures, office policies, and the names of executives and managers in the office
- Use a rogue device to access a poorly secured wireless network

Any one of these ploys might not be enough to compromise a system or result in a disclosure, but they can provide pieces to the security puzzle that attacker is trying to assess. Physical access controls, surveillance, and security awareness training such as ISO 27001 are suitable measures to combat this type of threat.

From increasingly sophisticated malware to social engineering to physical threats, there are many ways to fall victim to information security attacks. With a large set of preventative measures at one’s disposal, the question arises, how to choose among them?

Balancing the Cost and Benefits of Defensive Measures

The task of balancing the cost and benefits of countermeasures is essentially an exercise in risk analysis. The purpose of a risk analysis is to identify assets, threats to those assets, the potential loss to an organization due to threats, and finally, how to respond to that potential loss. The risk analysis process consists of five steps.

First, the organization must assign values to information assets. The value can be based on the replacement cost, if the asset is hardware, or the cost to recreate or recover, if it is a software asset or data. Also consider differences in how assets are used. For example, two laptops might both cost $1000, but one stores only the email of a sales representative, which is less valuable data than the other, which belongs to the CFO and contains undisclosed financial data. Organizations should also take into account the effect of a security breach on customer goodwill and brand value. These, of course, are more difficult to measure, but some consideration should be given to all costs, not just those that are easily quantifiable.

The second step is to estimate the potential loss per risk. This could include:

- The cost to recover from a malware attack, including lost productivity and IT staff time.
- The cost to recover from a DoS attack, including the cost of modifications to firewalls, IPSs, and other network assets to prevent future successful attacks.
- The cost of fines and penalties for violating confidentiality and privacy agreements by allowing the disclosure of sensitive information during a security breach.
- Lost revenues due to unavailable systems that were compromised by an attack

With this information, you can calculate the single loss expectancy, or the cost of recovering from a single incident.

The next step requires an estimate of the likelihood of each type of risk. For example, based on past experience, an organization may estimate that a significant malware attack will occur once per year and information loss due to a security breach will occur twice per year. The cost per year (known as the annual loss expectancy—ALE) of a malware attack is the cost of recovering from one malware incident; the cost per year of information losses is two times the single incident cost.

This is not a recommendation or advisory, merely an example.

These costs should provide an upper bound on the amount spent on countermeasures to prevent these threats from materializing. Countermeasures that cost less than the ALE should be deployed to mitigate the risk in cases in which the organization wants to reduce risks. There might be situations in which organizations are willing to accept the risk, either because the likelihood is so low or the cost of mitigating the risk so high. Alternatively, an organization could shift the risk by purchasing insurance.

So much depends on accurate valuations of assets and intangibles—such as customer goodwill, that it is essential to have accurate estimates or you risk skewing security resources to the wrong assets. Assessing threats and developing appropriate defenses is a key component of the asset protection life cycle. By understanding the risks associated with each asset, the value of each asset, and the cost of protecting the asset, organizations can make rational and efficient choices with regard to security practices. After the objectives for information asset protection are in place and choices are made about appropriate countermeasures, policies and procedures should be defined to put those decisions into practice.

Developing and Maintaining Policies

The terms “policies and procedures” sound bureaucratic and, to many, is out of place in the dynamic world of information technology. IT departments are constantly tasked with adapting to new requirements, responding to changing business environments, and meeting aggressive project schedules. It is not uncommon to hear complaints about formal policies and procedures slowing things down—and sometimes they do, but that is not necessarily a bad thing. Policies and procedures define standards and methods for accomplishing specific tasks. In contrast, ad hoc methods tend to “re-invent the wheel,” depend upon undocumented practices, and often leave systems more difficult to maintain than they should be.

Policies are statements of objectives and direction that guide implementations. For example, an organization might have a policy that all sensitive data that leaves the internal network should be strongly encrypted. Procedures are step-by-step instructions for implementing a policy. In the example just mentioned, a procedure for encrypting sensitive information on mobile devices might include the installation of a program that automatically encrypts all data stored on the devices long-term storage mechanism.

From an information asset protection perspective, several policies should be defined, including those that define:

- Acceptable use—Who is allowed to use the organization's information systems? For what purpose? Under what conditions?
- Access control standards—How are users authenticated to systems? What are password standards? How are users assigned to security roles? Who has authority to change access privileges?
- Anti-malware practices—What anti-malware software should be used? How frequently should full scans be performed? How frequently should devices check for updates? Who is responsible for responding if a malware attack is detected?
- Audit and vulnerability assessment procedures—What topics should be examined in an information security audit? How frequently should they be conducted? How should vulnerability assessments be performed? How should detected problems be remediated?
- Client device security—What security programs must run on client devices? What specialized restrictions apply to notebooks, PDAs, smart phones, and other mobile devices? What privileges are users granted to modify their local machines? Is the use of USB memory devices allowed?
- Email use and retention policies—What is the acceptable use of email systems? How should incoming and outgoing email be scanned? What are quarantine procedures for potentially malicious code or inappropriate content?
- Encryption use—When should encryption be used? What algorithms and key lengths should be used? How should keys be stored and distributed?
- Information privacy—What information is considered private, confidential, or sensitive? What are the rules for disclosing such information? In what situations should personally identifying information, such as Social Security numbers, be collected? What regulations and corporate governance policies apply to privacy protections in information systems?
- Risk analysis—How should information assets be valued? What are the organization's levels of risk tolerance?
- Server security—How should servers be locked down? What OS services should be allowed to execute? What restrictions are applied to servers that are accessible directly from the Internet, for example, those in a DMZ?
- Wireless security—Under what conditions are wireless access points deployed? Which wireless security protocols will be used? How will rogue devices be detected?

It might be difficult o develop polices for all of these areas immediately. Start with the acceptable use policy, access control standards, anti-malware, and information privacy area. If wireless devices are used in your organization, develop a wireless security policy as soon as possible. As with any aspect of security, you must prioritize based on the needs of your organization. There are other areas that warrant formal policies—for example, when virtual private networks (VPNs) are used, when third parties are granted access to key applications, and when procuring IT assets. Policies serve a unifying purpose by describing what is to be accomplished; this is especially important when multipoint solutions are deployed.

Implementing Multipoint Solutions

Multipoint solutions are redundant and complementary preventative measures that are deployed throughout an IT infrastructure.

Redundant Defensive Measures

Redundant solutions, commonly referred to as defense-in-depth solutions, perform the same logical function. For example, antivirus software may be deployed on individual client devices and on a network appliance scanning all incoming and outgoing traffic. With redundant solutions, there is no single point of failure for a particular service; if one countermeasure is down, the service is still available from the other countermeasure(s). Also, a vulnerability in one implementation of a countermeasure might not exist in other implementations (see Figure 3.3).

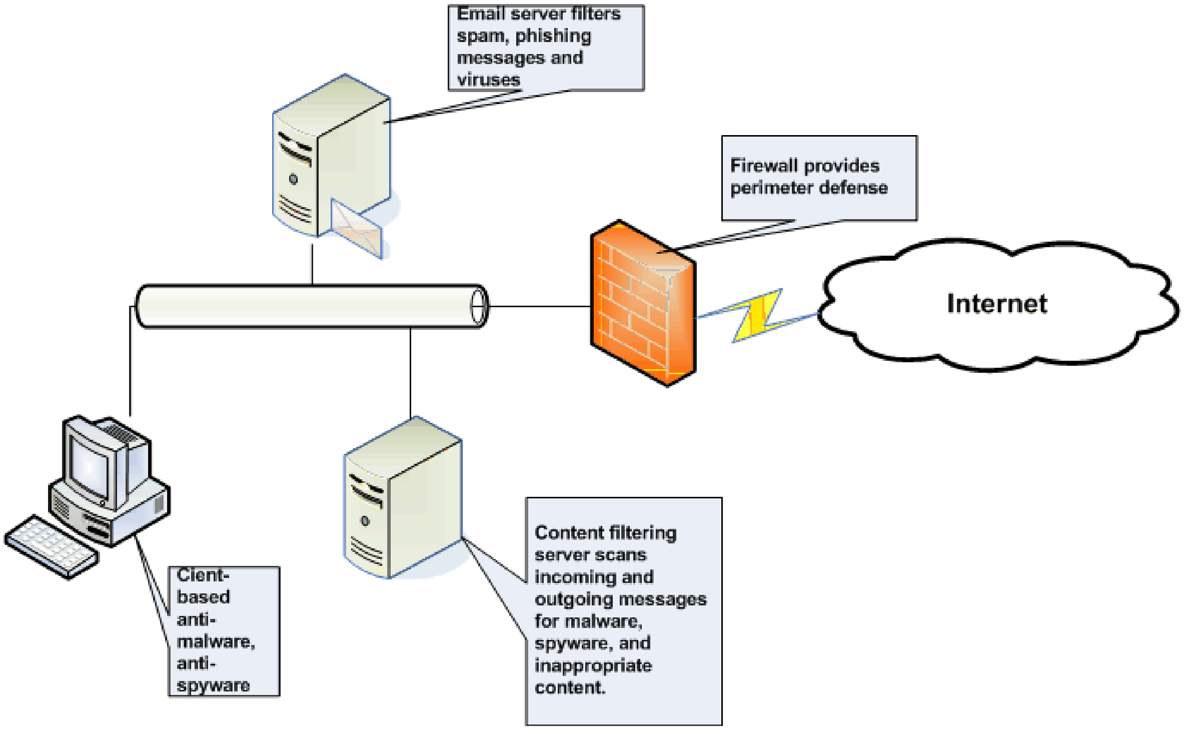
Email server filters spam, phishing messages and viruses
Firewall provides perimeter defense
Internet
Clent-based anti-malware, anti-spyware
Content filtering server scans incoming and outgoing messages for malware, spyware, and inappropriate content.

Figure 3.3: Multipoint solutions deploy redundant defensive measures at different points in the network.

An attacker may be able to use a buffer overflow attack to disable a desktop implementation of antivirus software from vendor A, but the network appliance-based antivirus solution from vendor B does not have the same vulnerability and thus is not compromised by the attack.

Complementary Solutions

Complementary solutions are combinations of defense mechanisms that compensate for weaknesses in each other. Consider database applications. Modern database management systems use listeners—applications that wait for requests for services on particular (usually TCP) ports. A single instance of a database might use several ports for a series of services. For example, one port might listen for query requests and another might listen for service discovery messages. Each of these ports might have different rules for legitimate use, and no single defense can prevent compromises to the database.

The service listening for query requests may accept requests from any IP address, but service discovery messages are accepted only from devices on the same network segment. In this case, a firewall on the network segment might block all incoming traffic on the port used by the service discovery program but allow traffic to the query listener. This setup prevents unauthorized use of the discovery service of the database while still allowing legitimate queries through.

Queries are usually well-formed requests for data, but they are also venues for database attacks. A SQL injection attack, for example, is a specially crafted query that takes advantage of weaknesses in a database application to allow an unverified and unsanitized query to execute. A database function designed to return a single application username and password can be exploited to return all usernames and passwords established in the application. A countermeasure to SQL injection attacks is to verify and sanitize all text strings before passing them on to the query processor to ensure only legitimate code is executed. By using both firewalls—to block unauthorized traffic—and verification routines within database applications—to validate authorized traffic—the two defense mechanisms provide more protection for the database than either can offer alone.

Challenges with Multipoint Solutions

With the additional protection that comes with multipoint solutions come additional challenges (see Figure 3.4):

- Synchronizing the activities of multipoint solutions
- Leveraging data from multiple countermeasures
- Ensuring graceful degradation of performance

As these three challenges demonstrate, there are costs associated with the improved security that comes with multipoint solutions.

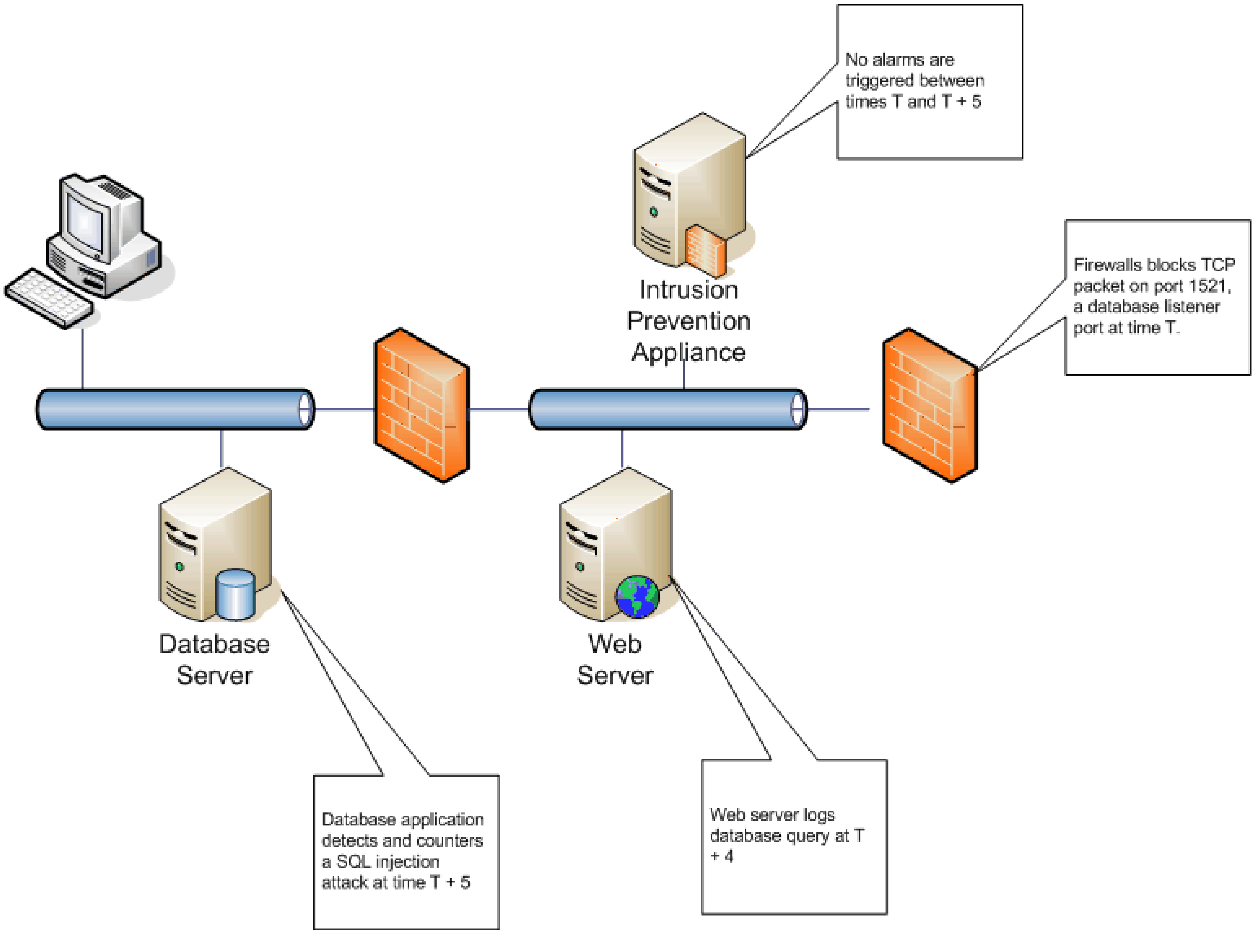
No alarms are triggered between times T and T + 5
Intrusion Prevention Appliance
Firewalls blocks TCP packet on port 1521, a database listener port at time T.
Database Server
Web Server
Database application detects and counters a SQL injection attack at time T + 5
Web server logs database query at T + 4

Figure 3.4: Events recorded by multiple security devices and servers may be related, but correlating events can be challenging; in some cases, a security device will not register an event that other devices log.

Synchronizing the Activities of Multipoint Solutions

Individual components of multipoint solutions should be coordinated for maximum effectiveness. To begin, each redundant component should be configured to address similar threats. For example, both network-based content filtering and client-side antivirus solutions should be configured to respond the same way when potentially malicious content is detected. A notebook user should not have one response to malware when connected to the corporate network and another when not on the corporate network.

Leveraging Data from Multiple Defensive Measures

It can be difficult to aggregate log data from multiple countermeasures. They might record information at different levels of granularity, event timestamps are often not synchronized, and it is not always obvious whether two events are related. In addition, some data that might be of use in a security breach, such as the source of a SQL injection attack, may be found in a Web server log file not in a security device's log. Consider automating the task of aggregating log data from multiple defensive measures. There are numerous tools available, including many IDS packages that accomplish this task.

Ensuring Graceful Degradation

Multipoint solutions can support graceful, rather than drastic, degradation in a service. For example, when an appliance running content filtering software for a network shuts down, client-based antivirus software can provide protection against malware threats. However, other content-based threats, such as leaking confidential information or the distribution of harassing emails, could still get through. When developing procedures based on multipoint solutions, consider how the failure of one or more components will affect the security service; relevant questions include:

- Will other components be able to compensate?
- What is the performance impact?
- What exposures are created?
- How will the component be brought back online?

Multipoint solutions are becoming standard approaches to implementing defense-in-depth security strategies. When deploying these solutions, it is important to understand which components complement each other and which are redundant. Redundant components can provide failover services and reduce the likelihood that a vulnerability in one instance of a countermeasure will render it ineffectual. Complementary solutions provide a similar property but use different techniques to combat the same threat. Security countermeasures are like any other IT resource; they must be maintained and monitored to ensure they continue to meet their objectives.

Maintaining and Monitoring Defensive Measures

Maintaining and monitoring countermeasures are neither the most interesting nor the most high-profile activities that come with a role in systems and security management. These, unfortunately, are often the tasks that are recognized only when they are *not* done and something goes wrong. The following check lists provide a starting point for defining procedures related to both maintaining and monitoring countermeasures.

Maintenance Tasks

The following list highlights tasks that must be performed to maintain a variety of countermeasures:

- Review countermeasure policies and procedures at least once every 6months; more frequently if there are major changes, such as the introduction of new enterprise applications or organizational restructurings.
- Enforce change control procedures on all security devices. Do not change firewall configurations, content filtering parameters, or upgrade software on these devices without following change management procedures. One exception is updating antivirus and intrusion prevention attack signatures. These are changes to the applications' libraries, not the code itself. Critical patches to the same software might warrant an immediate update with change control in some circumstances as well.
- Review vendor support sites, RSS feeds, and other sources of information on deployed security devices and applications.
- Review user accounts, group, and privilege assignments.
- Participate in release management reviews of new and upgraded applications.
- Test backup and recovery procedures.
- Regularly schedule and conduct vulnerability assessments and penetration tests, perhaps on the same schedule policies and procedures are reviewed.
- Cross-train security and systems management staff and rotate duties
- On an annual basis:
    - Review physical security measures
    - Review business continuity plans

> ✎ This list is illustrative, not exhaustive. There are other common tasks as well as organization-specific tasks that could be included.

Monitoring Tasks

As with the maintenance tasks, the following list provides examples of the types of activities that should be conducted (sometimes automatically) on a regular basis:

- Review event and error logs on all security devices
- Monitor quarantine areas used by content filtering devices
- Review statistics on spam filtered, malware detected, and other content filtering events
- Review performance monitoring statistics on CPU, disk storage, and network traffic of security devices to ensure adequate performance
- Review OS logs for system-level events, such as changes to a registry or OS directory
- Review access control logs and user accounts
- Check configurations of client devices to ensure anti-malware, anti-spyware, and personal firewalls are in use and properly configured (ideally, this would be done automatically with a client management tool)

These maintenance and monitoring tasks are performed to keep security devices functioning properly and to detect any significant security events. Organizations should also conduct audits to ensure policies are adequate and effectively implemented.

> 🕮 The International Organization for Standardization (ISO) has established an information security management standard that is defined in two parts, ISO-17999 and ISO-27001. For more information about this security management standard, see http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter.

Auditing

Auditing IT operations is becoming more commonplace with the advent of laws such as the Sarbanes-Oxley Act and other government regulations. An IT audit examines the controls related to general operations and specific applications to ensure policies are enforced and the basic principles of data integrity, confidentiality, and availability are enforced. Audits can examine several functions:

- Data center operations, ranging from backup and recovery operations to staff training to physical access controls to data center facilities
- Application development methodologies and practices—Audits might examine how projects are planned, how risks are analyzed, how software is developed to ensure quality and security, and how change control and release management are implemented
- Network operations—Including the deployment and configuration of security devices, the use of VPNs, and the architecture of trusted DMZs and untrusted network zones
- Business continuity planning and preparedness

Auditing is a complex topic. For small organizations with limited IT resources and little custom software development, an audit can be relatively quick and superficial. For large, and even some small and midsized companies that are highly dependent on IT operations, auditing and review of controls can be much more involved. It is recommended that organizations leverage well-developed and well-documented best practices for audit procedures.

📖 Information Systems Audit and Control Association (ISACA) has developed an extensive framework for IT governance known as COBIT. For details, see the ISACA Web site at https://www.isaca.org/.

There may be times—regardless of well-formulated policies and procedures, carefully deployed countermeasures, comprehensive maintenance and monitoring, and audit verified controls—that a security breach can occur. At those times, you should exercise a predefined plan for incident response.

Incident Response

Incidents are events that disrupt the availability of systems, threaten the integrity or confidentiality of data, or violate or threaten to violate appropriate use standards of information systems. Incident response is the method with which an organization controls a security breach or an attack. Computer forensics might be part of an incident response when legal proceedings may ensue.

Like natural disasters, many of us do not expect security incidents to happen to us; the result is that when security incidents occur, the response is formulated on the fly. Planning is required to respond to incidents in a controlled and effective manner. The basic steps in incident response are:

- Planning
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident analysis

The objectives of these steps is to isolate the impact of a security incident as quickly as possible to limit damage, determine the exact nature of the incident and stop it, restore systems to operational state, and learn from the event.

Planning for Incidents

By planning for security incidents, you can employ policies and procedures that are already in place when they are needed. Employees will know what to do when an attack is suspected. Incident response plans should include:

- Definitions and examples of incidents so that employees can readily identify security events
- Roles and responsibilities for responding to incidents as well as established reporting structures
- Initial responses to be carried out in the event of particular types of incidents—for example, a notebook that has been infected with a virus should be immediately disconnected from the network
- Severity rankings of incidents and escalation procedures for responding—for example, a single client device infected with a virus should be reported to a service desk line manager; when multiple servers are infected with a virus, higher-level IT managers are notified

Plans should describe the roles of non-technical staff as well, especially legal, media relations, and executive management in cases of significant breaches that violate regulations or require notification of third parties.

Detection and Analysis

The goal of the detection and analysis phase is to determine the type of attack under way so that it can be stopped. There are many types of attacks, but the general categories were described earlier. Training an incident response team in each type of attack enables the team to be able to assess the nature of an attack.

Indications of an attack are not always as obvious as an antivirus program issuing an alert that it has detected a worm on a server. Relatively unusual events, such as a Web server crash, can indicate an attack; however the same event could indicate a flaw in software that should be patched. IPSs commonly generate false alarms, so even security device warnings must be investigated to determine the cause of the alarm. Multiple indicators, such as a Web server crashing, unusual network traffic patterns, and a slow down in server response times, are evidence of a possible attack.

When indicators are present, analysis is done to determine whether there is a security incident or some other cause of the problem. Analysis is done by checking for variations from normal operating patterns, changes in file system integrity monitors, and events logged to multiple countermeasures or systems that may be correlated. If a network attack, such as a DoS attack, is under way, packet sniffers can be used to gather additional data.

Containment, Eradication, and Recovery

Once an incident has been confirmed, the next step is to contain the impact. What exactly should be done will vary, but options include:

- Shutting down affected devices
- Disconnecting devices from the network
- Stopping services
- Closing ports on firewalls
- Allowing an attack to continue but recording all network traffic for analysis or evidence

The appropriate response depends on several factors such as whether you intend to legally prosecute the attacker, the impact on service delivery, the time and resources required to implement and then recover from the action, and the length of time the action will have be continued. Eradiation requires eliminating the attack. In the case of malware, eradication requires removing the malicious code from infected machines. A DoS attack is eradicated when the flood of spurious traffic stops, such as by contacting an ISP to block traffic from the attacking source. After the incident has ceased, the next step is to recover services. This may be relatively simple, in the case of DoS attacks, or more complex in the case of a malware attack that damages data and leaves malicious programs such as keyloggers.

Post-Incident Analysis

Post-incident analysis is an opportunity to learn from a security incident. Questions will naturally arise about why the incident occurred. Were countermeasures in place and properly configured? Were OSs and applications properly patched? Was a vulnerability missed during a vulnerability scan? It might also be the case that the organization was the victim of a zero-day attack (an attack that exploits a previously unknown vulnerability and for which no patch exists) or that the threat was anticipated by risk analysis and it was determined that the cost of remediation was too high or the likelihood too low to warrant additional countermeasures. Incident response is the one element of the information protection life cycle you would rather not have to address but should be ready for nonetheless.

Summary

The life cycle of protecting Internet information assets is complex. The process ranges from assessing threats and determining appropriate countermeasures to responding to security incidents when those countermeasures are not enough. The life cycle does not follow a fixed progression from Step A to Step B; rather the findings of one stage can trigger the activities in another. Audits and post-incident analysis can prompt changes in policies and procedures. During the course of monitoring countermeasures, new threats can be discovered triggering a re-assessment of risk tolerances. By practicing sound management of each stage of the life cycle, organizations can help to protect their information assets regardless of the order in which those stages are encountered.