



MESSAGING SECURITY

DEFENSE IN DEPTH (AND BREADTH)

MESSAGING AND WEB SECURITY ESSENTIALS SERIES

Realtime
publishers
"Leading the Conversation"

➤ Messaging Security: Defense in Depth (and Breadth) By Dan Sullivan

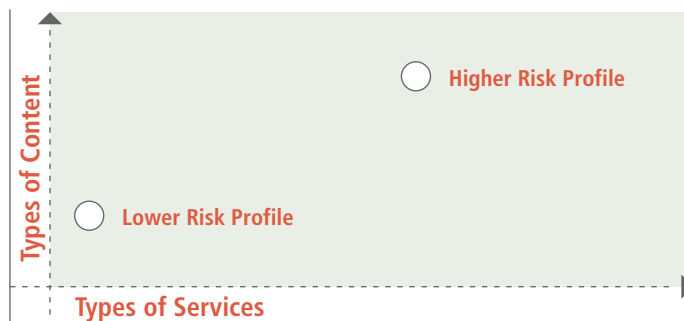
DEFENSE IN DEPTH IS A PHRASE YOU OFTEN HEAR WHEN DISCUSSING INFORMATION SECURITY. THE PRINCIPLE BEHIND IT IS SOUND: DO NOT DEPEND UPON ONE MECHANISM OR PRACTICE TO SECURE A SYSTEM. IT IS ALSO INSUFFICIENT FOR PROTECTING THE INTEGRITY OF MESSAGING SECURITY. IN ADDITION TO THE DEPTH OF DEFENSES, YOU MUST THINK IN TERMS OF THE BREADTH OF DEFENSES.

Consider a simple example that justifies the need for defense in depth: A firewall has been put in place, so there is no need to worry about an attack that depends on a protocol that uses one of the blocked ports, right? Not exactly—tunneling through an allowed protocol, such as HTTP, on an open port, such as port 80, can be an entry point to the network. With a defense-in-depth strategy, you assume that any one countermeasure maybe compromised and therefore multiple countermeasures are required to mitigate security risks. So far so good, however, you do not want to be too limited in how you think of threats.

As more services are provided on the Internet, from email and instant messaging to IP telephony and Web video conferencing, you are creating more potential vulnerabilities that can be exploited by attackers. A heap overflow vulnerability has been discovered and fixed in the Skype Internet phone client (Source: <http://www.skype.com/security/skype-sb-2005-03.html>). Frankly, there is nothing unusual about this; buffer overflows are a common security vulnerability. It, along with the other 4,279 vulnerabilities found this year (according to the National Vulnerability Database at <http://nvd.nist.gov/>), does demonstrate that the breadth of the vulnerabilities in your systems is correlated with the number of services you provide.

Vulnerabilities are also associated with the type of content that moves through a network. Leaked trade secrets can compromise competitiveness. A database security breach can result in the disclosure of personal financial or protected healthcare information resulting in regulatory violations. Offensive material brought into the office can create a hostile work environment leading to civil actions against an employer. Content type is another dimension that comes into play when you consider the breadth of security requirements.

➤ **FIGURE 1:** The risk profile associated with messaging security is determined by both the breadth of network services provided and the breadth of content distributed.



Clearly, when the subject of security turns to messaging security, you must think in terms of breadth as well as depth. The first step in a defense in depth and breadth approach is to prioritize information assets. Which applications, if they were unavailable, would severely disrupt operations? What data, if disclosed, would compromise competitive advantages or leave the organization liable for violating regulations? At the same time, consider threats to maintaining an appropriate work environment. Having a clear understanding of what is to be protected, you can apply countermeasures to protect those assets. Technology alone will not mitigate security risks—well-defined and implemented policies and procedures are required, too.

Technologies for Messaging Defense in Depth and Breadth

If you had to summarize messaging security in its most basic form, it would have to be keeping the bad stuff out and keeping the confidential stuff in. There is plenty of malicious content to get in, including viruses, worms, Trojan horses, keyloggers, screen scrappers, root kits, and behavior-tracking adware. Add to that list offensive material that could create a hostile work environment, peer-to-peer file sharing services that consume storage as well as network bandwidth, and the use of non-work-related sites that can raise productivity concerns. Then there is the material that needs to stay within an organization's network, such as customer account information, healthcare data, and other confidential and proprietary information. Protecting these assets is done with several technologies: anti-malware, anti-spyware, firewalls, intrusion prevention systems (IPSs), and content filters.

Anti-malware applications are commonly called antivirus, but that is a bit of a misnomer. They certainly can detect and eliminate viruses, but anti-malware programs can effectively detect worms, Trojan horses, and other malware as well. Anti-malware should be deployed both on the network and on individual devices. There are several reasons for this. From the defense-in-depth strategy, a network-based anti-malware program may have vulnerabilities not present in desktop versions and vice versa. When the two anti-malware deployments use programs from different vendors, there is a chance that malware not detected by one will be identified by the other. It is also better to eliminate a threat earlier rather than later. The human body can fight off many pathogens but, as a rule, you are better off if they do not infiltrate the body to begin with. Similarly, malware is better stopped at the perimeter than at the desktop. Once inside, the malware may be able to exploit vulnerabilities in the operating system (OS), network services, or applications.

Anti-spyware may detect some of the same threats as anti-malware, especially programs such as keyloggers. If adware is missed by anti-malware, anti-spyware can detect and eliminate the potentially unwanted program (PUP).

Firewalls are the first line of defense for messaging security. Again, following the principle of detect and block early, firewalls prevent potential threats from entering the network. Packet-filtering firewalls work well to prevent basic threats. For example, someone may unknowingly install an ftp server while

setting up an ad hoc development server. (In the ideal world, this would never happen and policies and procedures would be followed; reality is a different story). A firewall can effectively block traffic to the file transfer server known for security vulnerabilities. Application proxy and circuit proxy firewalls operate at higher levels of the network stack and more effectively control traffic based on content.

Like anti-malware, firewalls belong both on the network and on servers and client devices. The need for multiple layers of firewall protection is obvious for mobile devices: if they are disconnected from the network, they are vulnerable unless local countermeasures are deployed. Even stationary devices, such as servers and workstations, should be protected with personal firewalls. If a client device were compromised by a Trojan horse that included botnet software for emailing spam, a properly configured personal firewall could block SMTP traffic and prevent the spam from reaching its recipients.

IPSs can also help to improve the security of messaging. The assumption behind the use of an IPS is that other countermeasures have failed and there has been a security breach. IPSs work at the network and host levels. Network-based IPSs may detect unusual traffic patterns; for example, large volumes of SMTP traffic from a workstation that has been compromised and included in a botnet. (A personal firewall should block this, but in case that fails, the IPS could detect and block the problem; this is another example of defense in depth.)

So far, the technologies described have an important element in common: they operate to protect different types of content. Anti-malware can be configured to filter HTTP as well as SMTP traffic; firewalls can block thousands of ports; and IPSs can detect many types of anomalous patterns. Together they can provide both depth and breadth in security measures. Another technology that provides for a finely targeted breadth of coverage is content filtering.

Content filtering is essentially a traffic-scanning process that detects patterns of banned content. For example, employees of a company may not be allowed to use company resources to peruse gambling, entertainment, or music and video download sites. The other technologies listed cannot reasonably detect and block access to those sites without also potentially blocking access to legitimate use site. Content filters, however, can. They also provide breadth of protection by blocking offensive material, such as adult, hate speech, and similar sites.

One of the better aspects of content filtering is that it can work on traffic going out of as well as into an enterprise. The technology can therefore provide a measure of protection against information leaks.

If technical solutions alone were enough to reduce security risks to an acceptable level, you could stop here. They don't—which brings us to the other dimension of defense in depth and breadth: security management practices.

Security Management Practices for Messaging Security

Technical solutions are necessary but not sufficient to obtaining reasonable levels of messaging security. You also need four security management practices: patching, policy development, auditing, and training.

All software past a somewhat minimal level of complexity is likely to have bugs. Some of those bugs will present security vulnerabilities. Probably one of the best remembered is the flaw in SQL Server that was exploited by the SQL Slammer worm so effectively and rapidly that traffic on major segments of the Internet was effectively shutdown. What is less well recalled is that a patch for that vulnerability was released by Microsoft months before the attack. Vulnerabilities exist in OSs, network services, databases, Web servers, Web browsers, enterprise resource planning systems (ERPs), email servers, and just about any other major category of software. (Peruse the vulnerability database at <http://www.securityfocus.com/vulnerabilities> for specifics.) Protecting the integrity of messaging systems requires that you protect the integrity of shared infrastructure, and patching is a key element of that process.

Policy development is essential to establishing the goals and objectives of messaging security. Policies define what is to be protected as well as the measures used to protect those assets. Without adequate policies, managers and systems administrators are left to make decisions that may or may not align with broader enterprise objectives.

Auditing is another key practice that can help to maintain the integrity and confidentiality of messaging systems. This practice enables you to know what has actually happened within the infrastructure. Policy development defines what should be done, implementation and maintenance procedures execute those policies, and auditing verifies that they are effective.

The final key practice is training. You cannot underestimate the human dimension of messaging security. Users may not need to know the intricate details of IP protocols, OS vulnerabilities, or the inner workings of polymorphic viruses. What is important is an appreciation for the threats to information assets and users' role in protecting them. Simple acts—such as not downloading a file-sharing client, contacting the service desk when the personal firewall displays an unfamiliar message, or reporting phishing messages—can contribute to the overall effort to protect messaging and its underlying infrastructure.

There are many threats to messaging services. The common practice of defense in depth works as well here as in other areas of information security, but it works best when the full breadth of network services is accommodated within that framework.

Dan Sullivan is the resident editor at the Realtime Messaging and Web Security Community. Please contact Dan with your comments at: dan_sullivan@realtimepublishers.net

For more Messaging Security information please visit The Realtime Messaging and Web Security Community, sponsored by McAfee, at: www.realtime-emailsecurity.com.

www.realtime-emailsecurity.com