Network security has come a long way since the days of script kiddies and publicity seeking Denial-of-Service (DoS) attacks. Today’s most lethal security threats are frequently the work of organized crime, whose attacks are much more complex, targeted, global and sinister than ever before.

The teenage attacks of yore aimed for widespread chaos, publicity and notoriety. But the attacks of today often hide unnoticed for weeks, months or years on corporate networks. They are designed for stealing customer or employee information that can be sold for a huge profit and used for ID theft and phony credit card purchases.

No longer does the IT department have a monopoly on computer sophistication. Many in the generation brought up on video games and computers now have sufficient technical know-how to take advantage of network weaknesses for purposes of espionage, revenge and plain old making a buck.

To counter, most effective network security today is done in layers. The feeling is if an intrusion is missed at one level, it will be caught in subsequent layers. So whether you are shoring up security at the edge, the core or in between, a network secured in layers offers optimum protection.

**Threats Omnipresent**

The headlines scream about threats just about every week. Thousands of customer or staff records are hacked from large retail chains, hospitals, universities and financial services companies with networks that one would assume were closely guarded.

You can follow the weekly security breaches on the site of the Privacy Rights Clearinghouse—http://www.privacyrights.org/ar/ChronDataBreaches.htm.

The numbers are disturbing. According to the FBI and Computer Security Institute’s 2008 Computer Crime and Security Survey, almost half of all respondent organizations had experienced between one and five security incidents in the previous year.

More than a fourth reported attacks targeted specifically to networks or businesses like theirs. The average loss reported for each incident was $288,618, with the most expensive losses, averaging $500,000, resulting from financial fraud. Insider abuse was reported by 44 percent of respondents.

The perpetrators of these attacks are no longer isolated individuals. They often belong to sophisticated networks and ecosystems of producers, distributors and users who collaborate across global geographies, a phenomenon the FBI/CSI calls the professionalization of computer crime.

Sources of threats have also changed, with the number of threats coming from web surfing now equal or surpassing threats from once familiar e-mail attachments. Blended threats are also on the rise, with spam and phishing e-mails that prompt the user to click on a phony website resembling a well-known, legitimate site.

Victims then provide their personal information unknowingly for identity theft, download malicious software or add their systems to a global botnet of thousands or millions of other PCs bent on spreading spam and malware or penetrating other networks for data theft.

“We’re seeing botnets that are much larger and more sophisticated and stealthy than before,” says Eric Aarrestad, vice president of marketing for WatchGuard. “These botnets are much more targeted, sophisticated and damaging than ever.”

Peer-to-peer, gaming and pornography sites are riddled with malware. Even mainstream legitimate websites such as MSNBC.com have been compromised.
Hackers have even targeted social networking sites such as Facebook and LinkedIn. These sites have become a normal part of many corporate environments. And hackers are using social engineering techniques to trick users into downloading malicious software.

Viruses and worms are still relevant. However, stealthy Trojans and rootkits are now in favor with their ability to hide in systems and continue downloading and spreading malicious software on the LAN and across the Internet for weeks or months at a time.

The upshot: Today’s Internet threats are more dangerous than ever before. Slow networks, hobbled and vandalized websites and compromised employee productivity were big enough problems in their day, but primarily expensive nuisances.

Thanks to organized crime, compromised customer data, theft, extortion and worse, businesses now risk seriously harming their own customers and opening themselves up to crippling lawsuits. In the case of regulated industries like financial services and healthcare, expensive fines and legal action are also possible.

The publicity of an intrusion was damaging enough in the days of DoS attacks. Today such an occurrence can be crushing when the public finds out that its personal information has been compromised.

**Defense in Depth**

Obviously, huge organizations with large, expert IT staffs are falling victims to damaging attacks. So how can a small- or mid-sized business possibly hope to protect itself?

The answer is a strategy of defense in depth. It is one which uses many types and layers of security to catch and deflect security threats before they enter the network and, if they’re missed at the perimeter, after they get in.

Why defense in depth? Simply, the days of the network perimeter are over. Today’s blended and application-level threats can enter your network through e-mail or client web surfing, often bypassing your firewalls with ease.

With widespread mobile computing, smartphones, USB memory devices, wireless LANs, links with partners and suppliers, and even iPods, which are increasingly used as portable hard drives to steal company data, there are simply too many holes a hacker can take advantage of to reach inside the perimeter.

The bottom line is you still have to protect the perimeter today. However, you also have to protect internal servers, desktops, hardware and software.

How do large organizations get tripped up? “We find that companies get hacked through the smallest location not patched,” says Mike Flaum, product marketing manager for Juniper Networks’ SRX Series of gateway unified threat management products.

That often means a branch office, mobile user systems or wireless LANs. “People spend so much money on their front-line defenses that they often neglect the little sites, thinking that nobody will hack through that,” Flaum adds.

“For the most part when a company is hit it’s because of some machine they didn’t know about that didn’t get updated,” says Brian Grayek, vice president at CA. “This could be from their lack of a good systems management approach or computers that were added and not discovered from a merger or new offices.”

In addition to perimeter firewalls, many organizations rely solely on endpoint protection. And many of those neglect non-Windows systems such as those running Linux or the Macintosh OS X operating system.

Still, Macintosh PCs are penetrating enterprises in increasing numbers. And the Mac has become a target, with more malware written for Macintoshes in 2008 than previous years.

Macintosh users often run Windows software in a virtual machine, which may not be known to IT. Furthermore, sometimes the OS X platform can serve as a network entry point for Windows malware.

By the time end-point protection is involved, it can already be too late to fully address a network that has been penetrated via an unprotected system. That’s why networks are advised to invest in gateway and server security as well.
Firewall Protection
The longest standing gateway protection category is the firewall, offered by Check Point, Cisco, Juniper, Symantec, SonicWALL, WatchGuard and others. Firewalls still examine network and application flows as they did in the past, but now take advantage of deep inspection technologies that move further up the network stack than ever before to deflect threats.

“Now that a lot of threats come in through the web you have to use deeper packet inspection and granular access control, as well as external security intelligence such as reputation to make better decisions,” says Calvin Chai, senior manager, Security Solutions at Cisco.

“If my employee is being redirected to a web server, say, in Russia, and I know that the reputation of that server is not high based on information from a large security intelligence community, then I can enforce a policy decision that doesn’t allow my corporate asset to reach that system,” Chai adds.

Firewalls are also being upgraded to address newer application protocols. These include Session Initiation Protocol (SIP) along with Hypertext Transfer Protocol Secure (HTTPS).

Given the complex threats that exist today coupled with shrinking IT staffs, there is a trend toward additional, Unified Threat Management (UTM) appliances. These are often from the same vendor and combine firewalls with virtual private networking, web filtering, intrusion detection and prevention, antispam and even antivirus and antispyware in a single gateway protection device.

The performance of these devices has gone up tremendously. At the same time, the pricing has come down to the point that there are UTM units affordable for the small business and branch office, in addition to the central office network.

Antispam has become one of the most valuable security categories, not just to eliminate nuisance e-mails, but blended threats and phishing as well. “Just by blocking spam e-mails at the gateway, you can block a huge percentage of malware destined for your network,” says CA’s Grayek.

The advantages of unified threat management include lower price point for multiple types of protection, a single point of management, a single maintenance contract and a single “throat to choke” if something goes wrong.

Many of these devices use signatures, which are profiles of known attacks, to detect and eliminate threats. However, signatures are helpless against brand new threats, also known as zero-day attacks. That’s why it’s important for these products to be able to monitor general network behavior and alert you to anything unusual that might indicate an intrusion.

Many of these devices also allow you to partition the network to provide separate sets of policies and access controls. These can be for, say wireless LANs, which have their own set of security issues, than for other parts of the network.

Server Protection
At the server level, antivirus and host-based intrusion prevention software can protect your mission-critical applications from common application threats. Specialized messaging protection devices also exist to do e-mail content filtering, antivirus and spam prevention.

Content filtering protects against data leakage. It does this by scanning all e-mails for confidential content that you would not want sent outside of your organization.

Finally, Network Access Control (NAC) can be implemented at either the network gateway or at the server level. Here it is often referred to as Network Access Protection (NAP).

Every time a computer connects to the network, either directly or remotely, or to a particular mission-critical server, network access control software will scan the system to make sure that it is completely up to date with security software and updates. If it isn’t, NAC can actually implement relevant updates before the system connects to corporate applications.

For smaller businesses and branch offices, another category to check out are Integrated Services Routers, available from Cisco. Similar products are offered by Juniper’s SRX Series, which build security components such as firewalls, content filtering, VPNs and intrusion prevention directly into network routers.
These devices may not be suitable for the largest and busiest networks. However, they can be an economical solution for protecting smaller installations.

The important thing in any layered protection strategy is to ensure that all your systems are covered. You can’t invest all security dollars to protect the corporate data center and then neglect a small branch office, a small wireless LAN or a Macintosh PC, assuming that they are unlikely targets.

Hackers will look for any conceivable way to get inside your LAN and frequently the best way is through one of these back doors. By taking a comprehensive, layered approach to network security, you can keep your network and business protected for years to come.

Network Protection Categories

**Firewalls** — inspect all computer traffic at the gateway or on a computer to permit or deny access based on a set of rules and policies.

**Virtual Private Networking (VPN)** — provides secure remote access to the corporate network over the Internet for telecommuters, partners and mobile warriors.

**Web Filtering** — lets organizations monitor and control access to the web according to corporate policy, so that unsafe or inappropriate employee web surfing can be kept under control.

**E-mail Filtering** — monitors incoming and outgoing e-mail for malware and confidential information to make sure that the use of e-mail complies with corporate policies.

**Intrusion Prevention** — monitors network traffic for signs of malicious behavior and blocks attacks that might make it past a firewall.

**Antivirus/Antispyware** — inspects e-mails and other traffic for malware, including viruses, spyware, worms, rootkits, and Trojans, and eliminates or quarantines malware to prevent its spread.

**Antispam** — monitors e-mails for signs of spam and can either block it or send it to a special spam directory.

**WORKING WITH YOUR ACCOUNT MANAGER, A CDW TECHNOLOGY SPECIALIST CAN CUSTOMIZE A SECURITY SOLUTION FOR YOUR BUSINESS. CALL 800.800.4CDW TO TALK TO A SPECIALIST TODAY.**

090715