NETWORK SECURITY: RISKS AND

While you can't see the threats, you know they are there and must be dealt with.

Today's corporation is under constant attack. According to the Internet Crime Complaint Center, a partnership effort between the FBI and the nonprofit National White Collar Crime Center, U.S. hacking incidents in 2009 accounted for $560 million in losses — more than double the losses the previous year.

And that's just the value of data lost, and only for reported incidents. When you add in the expense of data recovery along with lost business caused by downtime and fraudulent use of stolen data, the cost of cybercrime to American businesses increases dramatically. A 2007 Government Accountability Office study estimates total losses to U.S. businesses at a staggering $115 billion a year.

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.

Reasons for Risk

There are several reasons for such a dramatic increase in information security breaches. The most obvious: Criminals looking to trade information for cash have replaced youthful hackers joyriding the Internet. Today, cybercrime has gone mainstream. It's big business, with highly organized professionals targeting high-value data for profit.

Another factor is the increasing raggedness of the corporate perimeter. Business networks today incorporate remote employees working from home; global partners; mobile workers using unknown networks from the field; customers and clients accessing resources via the web; virtual servers, storage and applications both on and offsite; and a host of cloud-based services that handle data and data security in different ways.

And the weakest link is not technological at all, but human: a company's staff itself. Despite huge advances in networking technology and increasingly virulent attacks on the network, most employees have little understanding of security basics.

Meanwhile, a changing business world demands they engage more and more with social media and networking sites, web-based information and remote partners, increasing the chance that a less-than-tech-savvy worker will open a link, visit a site or download a file carrying a payload that will compromise your network's security. Even unwittingly, staffers might give out private information, such as network passwords, prelaunch product information or client data.

But the situation needn't be direly grim. Businesses have become quite good at defending their network perimeters, and companies such as Cisco Systems, VMware, WatchGuard and others have introduced powerful new tools to deal with the changing nature of networks and of attacks.

Protecting the network today requires a shift in thinking away from the perimeter and toward, on one hand, a more granular approach to specific applications and, on the other, a more holistic view that encompasses the corporate culture and human behavior. That shift must take place against a backdrop of the traditional security technologies that IT has relied on.

New Threat Landscape

The network today looks different than it did a decade or even a few years ago. There are more ways than ever for an attacker to gain access to corporate information and network resources.

"Mobile devices are one new vector for attack," says Jeff Wilson, principal analyst for network security at Infonetics Research. "There are a lot of new devices — notebook PCs, mobile phones, netbooks, tablets — that IT professionals must deal with. There are also new threats from virtual devices,

social networks and even established websites. In fact, legitimate web traffic is the most likely source of attacks these days."

One issue is the increasingly permeable nature of the corporate network. "There's this huge change going on in networks," says Bill McGee, manager of security solutions marketing at Cisco. "We're seeing a major erosion of the perimeter, with a huge proliferation of endpoint devices, often consumer-based IP-enabled devices, attached to the corporate network."

41%

Business leaders surveyed who identify business continuity and disaster recovery as the top driver of security initiatives[1]

Virtualization presents another challenge. Although in most ways, virtual machines (VMs) are secured in much the same way as physical ones, the technology remains new enough that significant unknowns exist about their security. According to a recent report from the tech analyst firm Gartner, 60 percent of virtual servers are insecure, largely because of the failure of businesses to involve information security teams during planning and implementation.

"In virtual environments, you don't have the visibility you had before," Wilson says. To manage network connections, virtual servers generate virtualized switches and other ways of handling traffic that are invisible to the existing network security tools outside of the VM.

"For instance, even though you have a firewall in front of the server, viruses can move between applications and from virtual machine to virtual machine," Wilson points out. "And they can do this without going through the firewall."

Gartner predicts that more sophisticated tools for securing virtualized systems will emerge by 2015, and already vendors are crafting tools to deal with these issues. VMware has developed VMsafe, for example, to provide an application protocol interface that security tools can use to effectively "reach into" a VM and provide the same protections allowed on physical servers.

At the other end of the network from the data center, end users' everyday web use can open a company up to attack. SQL injection and cross-site scripting (XSS) attacks are becoming especially virulent, with attackers taking advantage of holes in the way content is delivered over the web to insert malicious code just about anywhere.

Likewise, the exchange of images, videos and links that is the currency of social networking opens up new avenues for malware to get into the system. For example, portable document format (PDF) files have emerged as the No. 1 source of malware in recent years, due to widely known and easily exploited security holes. The widespread use of URL shorteners, too, makes it easy to direct users to look-alike phishing sites and sites containing malware.

Finally, an increasing reliance on cloud computing could create vulnerabilities. So far, hackers have yet to execute a major attack via a cloud platform. Still, the fact remains that the security of those systems is out of the hands of the company's IT team, making it difficult to know how well data and applications are being protected. And even trusted systems are vulnerable to simple attacks such as an unauthorized person acquiring a password for online sales, payroll or file storage service.

Defense in Depth

Obviously, huge organizations with large, expert IT staffs are falling victims to damaging attacks. So how can a midsize 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.

Every network still needs a firewall — but a firewall is rarely just a firewall anymore. Today's firewalls, such as WatchGuard's XTM Series, Cisco's ASA 5500 Series and Check Point Software Technologies' Software Blades, include spam blocking, content filtering, antivirus, intrusion prevention, reputation checking and virtual private networking (VPN) capabilities.

It's no longer enough to indiscriminately block or allow traffic, says WatchGuard Senior Product Manager Tracy Hillstrom. "You have to defend against specific attacks and shape the way employees use the Internet with filtering. Also, you need visibility: What kind of traffic is coming into your network? How are your resources being used?"

Who is using those networks and on what kind of device is important, too. Identity control provides a framework for identifying who is trying to access the network and what they are allowed to do.

"The idea is to find out who they are, what device they are using and what's running on the device," Infonetics Wilson says. "You also want to know if they are using the latest antivirus definitions, is there malicious code running on their machine and where they are coming from. Network access control takes all this information and synthesizes it to decide what level of access to give."

[1]SOURCE: Trial by Fire: The Global State of Information Security Survey of 7,200 IT decision-makers worldwide, PricewaterhouseCoopers (2010)

Five Steps to Safer Social Networking

The rise over the last few years of social networking and social media tools as key business technologies has companies struggling to keep pace.

Because these technologies encourage a more relaxed approach and genuine personal connections, it can be all too easy for employees to either open themselves up to attack or even to willingly (or possibly unwittingly) divulge corporate information.

Unfortunately, too-strict controls on social media use can backfire; web users have an uncanny ability to detect when corporate voices are inauthentic or constrained. Also, employees who run into barriers they don't understand have a way of ignoring them. "When you make security too complex, users will find a way around it," says Sai Aloazarpu, senior director for security and acceleration at Citrix Systems.

These tips can help you strike a happy medium between heavy-handed censorship and completely open access.

1. **Set clear policies:** The first step, of course, is to issue clear guidelines about what employees can or cannot do online. Don't leave it to your employees to guess whether some behavior is appropriate or not.
2. **Keep an eye out:** Make sure someone in the organization is charged with reviewing employee social media activity on a regular basis.
3. **Scan everything:** Social networks offer great media for the spread of malware and viruses because the comfort levels are higher. If social networking plays a part of your business strategy, make sure to perform deep-packet inspection, content filtering and identity management on all social media traffic. (Vendors have begun to include social media features in their tools to scan things such as Facebook widgets, files sent over Twitter and instant messages.)
4. **Monitor URLs:** The common use of URL shorteners on social networking services makes phishing and malware attacks easier. Make sure they're checked against a blacklist or, better yet, a reputation management service before they can be visited.
5. **Train, train, train:** The intangible nature of security makes it difficult for most people to grasp its importance relative to their actual work. Institute ongoing training about the threats posed by social media and social networking sites and how those risks can be lessened. It may seem like common sense, but it's not. Most people have no idea that they could be putting their company, or themselves, at risk.

Because attackers have largely turned away from attacks against the operating system or network as a whole in favor of attacks against specific applications, being able to monitor and control the activity at the application level becomes increasingly important.

Application firewalls can provide a much more granular level of control than a gateway firewall, adding a layer to protect against outside attacks and to minimize the spread of successful attacks.

To identify problems, network administrators can also monitor the traffic their applications and users generate. Deep-packet inspection analyzes the content of traffic to see what kind of data it contains, which can be important since the firewall does not distinguish between good and bad traffic once an application is approved.

Monitoring the network as a whole can also enhance security. Cisco IOS NetFlow offers a heuristic approach to network traffic, comparing current conditions with typical flow to identify unusual spikes in activity.

Reputation management has emerged as a powerful tool in dealing with web-based attacks without unduly limiting employees' ability to do their jobs. Tools such as Cisco's Security Intelligence Operations (SIO) constantly monitor threats as they emerge.

"What arms our devices is global threat awareness," says Sarah Vanier, manager of security solutions marketing at Cisco. "This is how you stay ahead of what's happening out there." SIO automatically pushes updates out to subscribers every few minutes, detailing new sites that are known to be the source of attacks, recent spam messages that contain malware or phishing attacks, and other threats.

Visibility Plus Control

There are a ridiculous number of threats out there. Even if nobody steals anything, there is a huge amount of loss involved when users are unable to use their computers or the applications they need.

The important thing in any layered protection strategy is to ensure that all 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. ◊