



Getting security savvy

Security software vendors used to sell their products by spreading fear, uncertainty and doubt about the faceless hackers that might be trying to penetrate your company's network at this very moment. Now the threat is much more in our faces, and businesses are being forced to wise up. By David Braue

These days, the biggest threat to corporate security is email-borne viruses, which are proving remarkably effective at spreading across the globe like the proverbial wildfire. And despite every effort to educate users in the very simple ways to avoid catching such viruses, every group of employees has users that just don't play it safe. Denial of service—and a potential impact on crucial business applications—is the inevitable result as torrents of virus-laden emails scour the globe for their next target.

"We've seen advancements in propagation techniques over the past two years," says Kevin Houle, a senior member of the technical staff with security specialist Computer Emergency Response Team (CERT). "Someone with malicious intent can now get control of several

hundred thousand computers in a matter of 24 hours. The question then becomes 'what do I do with these computers?'"

Your crucial information systems, bent to the twisted whim of a nameless hacker. It sounds like the plot of some twisted movie, but it's effectively the scenario that awaits those who don't put the right security controls in place. Fortunately, there is no lack of options: firewalls, intrusion detection systems (IDSes), honeypots, virtual private networks, digital signature technologies, and a myriad of other security tools can now help overwhelmed companies retain some semblance of control in the face of an attack.

Despite their many precautions, however, companies that have invested heavily in security technologies now face another problem: the sheer increase in information volumes has made it virtually impossible for IT staff to keep up.

Email viruses can flood a network so fast there's little time to react before service has been interrupted. IDSes have gotten better at detecting spurious activity that suggests an outside hack attack, but on the flip side they're so sensitive that customers are finding themselves absolutely swamped with IDS logs running into the tens or hundreds of thousands of events a day. And while managers might value up-to-date sales reports produced by an enterprise reporting system, the provision of up-to-date security logs is of little use to anybody unless they can be acted upon—and quickly.

Getting smarter about security

While security issues are naturally kept close to any company's chest, there are signs that many firms have become willing to bring in third parties in ways that they

“Someone with malicious intent can now get control of several hundred thousand computers in a matter of 24 hours.”

KEVIN HOULE, COMPUTER EMERGENCY RESPONSE TEAM

never did before. A growing number of managed security service providers (MSSPs), for example, are finding customers more than willing to outsource the monitoring of, and reaction to, security alarms triggered by in-house systems.

Andrew Walls, principal consultant with security consulting firm Betrusted, sees the rise of the MSSP as an indication that companies have become more mature about their security infrastructures. “The client base has become more intelligent about the consumption of products and services,” he says. “Security, in terms of products, has become a commoditised item; what is important to clients out there is the provision of services that are underlaid by the consulting operations.”

Yet even MSSPs can struggle to make sense of security systems that are generating tens or hundreds of thousands of alarms a day. Security vendors privately concede that many customers have simply turned off their IDSes after several weeks of struggling to keep up with voluminous event logs. After all, if detailed security logs are so large that they can’t be analysed for days, they’re not going to do much to help catch intruders in the act.

Enter the latest phase in the security industry’s evolution: reconciliation. Having accepted that an assemblage of point security solutions leaves significant potential holes and a serious management burden for customers, security vendors have recently begun turning their sights to providing correlation engines that can do the dirty work on customers’ behalf. Solutions like Tier-3 Huntsman and Symantec Enterprise Security Manager, for example, are designed to read the voluminous logs from a variety of different security systems and correlate events to weed out massive numbers of false positives.

Increasing data volumes due to the beginning of a nightly backup, for example, might easily be confused for a flood of virus-generated emails and reported to the IT manager as such. If a correlation engine can spend a few weeks monitoring the network for a baseline of activity, however, it will recognise that backup data is supposed to cause a bandwidth flood on certain TCP/IP ports at a certain time every night. This presumption might be confirmed by analysing backup logs, which would reveal that a backup did indeed start at a particular time.

By applying such common sense rules, correlation engines promise to take much of the pain out of security

technology. Workflow rules can be created so that the second a workstation begins transmitting a flood of emails, the workstation’s connection is cut and the relevant people are automatically notified so action can be taken. Over time, tighter integration between previously disparate security solutions will improve communication between various modules.

Looking deeper into the data

By looking at security in terms of anomaly detection rather than as a way of catching unknown intruders, correlation tools will become critical in helping companies keep on top of what is a dramatically changing security landscape. Yet while some vendors try to make better sense of the myriad technologies out there, still others are trying other new approaches to information security.

The latest new approach is ‘deep packet inspection’, in which security tools delve deeper and deeper into the OSI model to pick out particular types of potentially malicious network activity. Young gun Fortinet recently took this approach even further by launching a security appliance capable of scanning any type of data stream for intrusion or virus signatures. Rather than simply watching for suspicious traffic flows, Fortinet-developed chips are able to scan data streams in real time ñ at a full 2Gbps throughput ñ to detect suspicious data at any point in the network.

This approach means the box could easily be deployed not just at the edges of the network—like most firewall and content scanning systems—but as a sentry anywhere that critical data is passing. For example, hooking it onto a storage area network feed could add another layer of protection by ensuring that there are no viruses in any data stream being written to the storage array. This is something conventional security solutions could easily miss if a virus was introduced inside the firewall.

“A lot of people still see these things as important for a perimeter-based approach to security,” says Fortinet country manager Pete Sandilands. “There is definitely room for deploying midscale boxes like this throughout a network to get rid of the risk of, for example, people plugging in notebooks with viruses on them.”

Another security tool finding renewed currency is the Data Diode, a product from Tenix Datagate that allows companies to segregate secure parts of their network by ensuring that traffic only flows in one direction. This way, it’s possible to prevent back-door attacks carefully control access to sensitive information.

Just getting new weapons in the security arsenal won’t guarantee results, however, without the usual attention to business policy, security, and the interrelationship of IT and business security objectives. Consultants have pushed this point for years, but with security’s profile continuing to rise—and customers getting smarter than ever about the solutions they’re implementing ñ it seems that effective information security is becoming less and less arcane as time goes by. However, threats change continuously and hackers are always waiting outside the door. Constant vigilance remains the price we pay for life in the information age. ■■■■