1 Make your systems "crunchy" on the inside, not just the outside

By Robert L. Scheier

If you've been around security for the last few years, you've probably heard the phrase "crunchy on the outside, chewy on the inside."

That means your organisation is well protected with firewalls and/or antivirus tools at the gateways where the network meets the Internet, while the servers, storage and management consoles on the inside are left virtually unprotected.

People have been talking about moving to more "end-to-end" security for some time, but in recent weeks I've heard customers are actually taking action. They're finally making the inside of their IT infrastructures more "crunchy" because of new threats, new regulations and new technology. The tools they're using include encryption, authentication, host-based (as well as network-based) security, and they're separating the data path from the data management path.

If you're not worried about data at rest, then you haven't heard about the theft of computer equipment holding information on about 500,000 military health beneficiaries from a government subcontractor in December. Such physical theft of data will become even less pleasant as regulators start enforcing HIPAA rules protecting patient data and the Sarbanes-Oxley Act, which requires that CEOs and CFOs personally promise their financial statements haven't been cooked. At least one security technology –- encryption -- can actually make it easier for hackers to get to vulnerable servers and disks by hiding the sometimes-malicious nature of packets as they pass through firewalls at the edge. If all that didn't make the middle of your network a scary place, consider the oft-quoted statistic that 70% of all security threats come from inside the organisation.

One security administrator who's seen the light is Jeff Nigriny, chief security officer at Exostar, which provides online collaboration and buying services for aerospace giants such as Boeing, Lockheed Martin and Rolls-Royce. "We typically worry more about what each individual server is doing with the data then we do about (hacks against) the network," he says. Most of the traffic hitting his firewalls is either non-malicious or consists of

unsophisticated attacks, he says. The bigger risk, he says, is the encrypted traffic that "we don't have a good chance to inspect at the border" and is passed through to his servers.

What to do about such threats? Here's a sampling of how security managers are making their systems harder to hack on the inside, as well as the outside.

Encryption

Encryption to protect data at rest on disk drives "is the number one request we hear from our users today," says Nigriny, with the urgency of the request "in direct proportion to the value of the data being protected."

Only 1 to 2% of the data in an organisation is ever in movement across the network, with the rest sitting on a disk drive somewhere and usually unencrypted, says Steve Duplessie, senior analyst at Enterprise Storage Group, a storage research firm.

Encryption is all the more important because of the rise of storage area networks, which offer far more entry points to a hacker than storage "direct-attached" to a server. Some users worry the processor-intensive work of encrypting and decrypting network traffic can slow performance and that managing the encryption keys can be more trouble than its worth. To ease the performance concern, vendors such as Decru Inc. sell standalone appliances that take the encryption load off the server.

Authentication

Authentication helps ensure unauthorised people posing as administrators do not change the configuration of firewalls, storage networks or other network components. "When you talk about configuration, it opens up a whole new area of potential backdoors and loopholes," says Mark Diamond, president and CEO of Contoural Inc. and chair of the Storage Networking Industry Association Customer Advisory Board on Storage Security. "It could be somebody from inside the firewall who could walk up and reconfigure (a storage area network) very easily."

In the storage networking world, emerging standards to watch include the SwitchLink Authentication Protocol (SLAP), which would prove that devices within a storage area network are what they claim to be, and the Encapsulating Security Payload protocol that would prove data has come from a legitimate source and hasn't been tampered with.

Separating data management from data access

Even if you have authentication tools in place, there's always the possibility that a rogue administrator with official access rights could hack into or change your data. An added layer of protection is to create separate logical and physical paths for managing data and for reading it.

"You want IT people to do backups and restores, provisioning, and to replicate the storage onto multiple disaster recovery sites…without being able to read the data," says Decru CEO Dan Avida. Avida argues that standalone appliances such as Decru's make this separation easier than using security functions in storage management tools.

Host-based security

This ranges from simply keeping up with patches (which would have prevented much of the damage caused by the recent SQL Slammer worm) to validating SQL queries to determine if they're real queries or attempted hacks. "It's almost criminal," says Nigriny, for an application service provider to not validate SQL requests to catch common database attacks. Exostar decrypts and inspects requests for application services at the server because only the server can understand the context of, and the validity of, those requests.

Some people say the new security model should be "crunchy all the way through." Others, like Nigriny, argue that Web services call for a "softer on the outside, crunchy on the inside" model where most of the protective measures are applied on the servers. The right model will vary by organisation, but one thing is clear: These days, you need some "crunch" all the way through, and not just on the perimeter of your network.

About the author

Robert L. Scheier writes frequently about security from Boylston, Mass. He can be reached at rscheier@charter.net.