

PROCESSOR.

Tech & Trends

General Information

November 30, 2007 • Vol.29 Issue 48

Make It Difficult For Intruders Slow Them Down & Sniff Them Out

Enterprises make every effort to deal with increasing threats, but attackers are relentless. "At some point, an intruder will access the network," says Randy Abrams, director of technical education at ESET (www.eset.com), a security software vendor.

No security is foolproof. But with tools and tips from these experts, enterprises can improve their defenses and make intruders' jobs more difficult and less rewarding.

■ Strong Passwords

To stall intruders' efforts, companies should use strong passwords, which are hard to figure out because of their length, complexity, or both. When passwords are too complex, employees often write them down and paste them on their monitors to remember them, according to Dan Simon, senior application security specialist at Halock Security Labs (www.halock.com), a full-service security risk consulting firm. Posting passwords in plain sight, however, can reveal them to intruders who enter from within.

A 20-character password with all lowercase letters is stronger than an eight-character password with letters, numbers, and other characters in both uppercase and lowercase, according to Abrams. "Use long, easy-to-remember passwords made of sentences," says Abrams, a former security expert with Microsoft. This facilitates passwords that are hard to guess but easy for employees to remember.

Passwords should also be set to expire periodically so that old passwords become useless by the time talented intruders figure them out. Administrators can set things up so that once the current password has expired, employees must change passwords before they can log in again, according to Tom Turner, vice president of marketing at Q1 Labs (www.q1labs.com).

■ Authentication Procedures

Authentication helps to prove that a user is genuine. Today, there is two-factor authentication, which requires two forms of identification, generally something you know and something you have. This makes it more difficult for an intruder to falsify an identity and get on the network.

Forms of identification include secure IDs on USB sticks or smart cards and passwords, for example. "Users have to have their passwords and the hardware token, too, to log in," says Steve Tate, security expert and computer science department head at the University of North Carolina at Greensboro. Strong two-factor authentication is available from multiple vendors, according to Simon. Examples include RSA's SecurID (www.rsa.com) and Aladdin's eToken PRO Smartcard (www.aladdin.com).

■ Minimization & Permissions

The enterprise should architect the network to minimize losses, according to Gene Spafford, executive director at the Purdue University CERIAS (Center for Education and Research in Information Assurance and Security). Minimization involves setting the network up so that if someone does get in, risk and damage are limited.

Permissions are part of minimization. Administrators can grant user access permissions or limit access to all the different resources on a network. "Active Directory is one of the most prevalent tools used to set permissions. There are a plethora of other third-party tools available," says Abrams.

According to Simon, users should only have access to the resources they need to fulfill their roles. The enterprise can set policies around company roles so that a user ID associated with a role has certain access rights and limitations automatically. By using permissions, the enterprise can limit the potential for an intruder to use a single, compromised identity or system to get to the whole network.

One way to use permissions is to limit network access for customer service people whose roles include reading outside email, according to Spafford. If a customer service employee opens an attachment designed to help an intruder gain access and the customer service representative's ID has permission to access the rest of the network, the intruder will immediately gain the same access rights automatically.

To strengthen the use of permissions, partition the internal network into separate domains that don't have common authorizations or access, according to Spafford. By using separate domains, the same users won't automatically have access rights to the shipping department they work in, for example, and, say, the accounting department.

Other examples of minimization include encryption and database access. The enterprise can encrypt "data at rest" (data that is not moving around like network traffic) without storing the security keys on the system, according to Spafford. The intruder may find the encrypted data, but the security key to open it won't be sitting right next to it. Enterprises should keep sensitive or critical databases offline to prevent their exposure to intruders. "In a networked environment, don't have them connected to anything that is on the Internet," says Spafford.

Important tools that are increasingly available to small and midsized enterprises include DLP (data leak/loss prevention) software and NAC hardware and software.

DLP software detects sensitive information leaving the network. When it does, it can set off an alarm or drop the connection, according to Spafford. "Some of those products are available at modest prices, and the performance is reasonable," he says.

Enterprises use NAC technology to protect the network against infections and intruder access that pass through company endpoint hardware, such as laptops. For example, NAC can check a laptop to make sure its security software and patches are up-to-date before allowing it to connect to the network. NAC hardware is available today in the \$800

to \$2,000 price range per appliance, according to Abrams. Security software vendors are adding NAC software to their security suites, as well.

■ Tracking

It's hard to track an educated intruder. "One of the first steps an attacker will take after compromising a system is to cover their tracks—removing all logs and other traces of an attack," says Simon. Hardware, such as servers and firewalls, keep access and activity logs.

Good first steps to counter an intruder's stealthy behavior include having multiple points for logging and auditing system behavior across the network, according to Simon. Enterprises should keep log files on secure, remote storage on separate systems where possible to keep them safe from removal, Simon adds.

IDSes are another good means of tracking intruders. IDSes analyze security-related data from around the network to determine whether there might be a system or network compromise. A standalone IDS can be expensive. However, some firewalls come with IDS capabilities, according to Tate.

■ A Complete Plan Of Action

Discouraging intruders is a matter of planning and know-how, as well as an investment in a combination of affordable security products. Plan security-related purchases and intruder prevention measures in concert with each other and in advance. ■

by David Geer