COMPUTERWORLD

HOW-TO

Network security primer: Access control

By Michael Cooney FOLLOW

Network World | Nov 17, 2015 11:05 AM PT

During its testimony on security weaknesses among federal agencies this week, the Government Accountability Office detailed a number of critical elements that make up effective protection systems.

Among the systems the watchdog agency detailed was the key components in access control which is typically the technology an enterprise uses to regulate who has access to what resources.

+ More on Network World: Watchdogs detail Federal security tribulations +

The GAO offered a look at what it considers to be the six critical elements in an access control system:

Boundary protection: Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from devices that are connected to a network. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection and prevention technologies can be deployed to defend against attacks from the Internet.

User identification and authentication: A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns a unique user account to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication.

Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric). The combination of identification and authentication provides the basis for establishing accountability and for controlling access to the system.

Authorization: Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. For example, operating systems have some built-in authorization features such as permissions for files and folders. Network devices, such as routers, may have access control lists that can be used to authorize users who can access and perform certain actions on the device.

+More on network World: The 7 most common challenges to cloud computing +

Authorization controls help implement the principle of "least privilege, "which the National Institute of Standards and Technology describes as allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Cryptography: Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. Examples of cryptographic services are encryption, authentication, digital signature, and key management. Cryptographic tools help control access to information by making it unintelligible to unauthorized users and by protecting the integrity of transmitted or stored information.

Auditing and Monitoring: To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is necessary to determine what, when, and by whom specific actions have been taken on a system. Agencies do so by implementing software that provides an audit trail, or logs of system activity, that they can use to determine the source of a

transaction or attempted transaction and to monitor users' activities.

+More on network World: The 10 most common mobile security problems and how you can fight them

Physical security: Physical security controls help protect computer facilities and resources from espionage, sabotage, damage, and theft. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, locks, and procedures for granting or denying individuals physical access to computing resources.

Physical controls also include environmental controls such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies. Considerations for perimeter security include controlling vehicular and pedestrian traffic. In addition, visitors' access to sensitive areas is to be managed appropriately.

This story, "Network security primer: Access control" was originally published by Network World.

Michael Cooney — *Online News Editor*

Cooney is an Online News Editor and the author of the Layer 8 blog, Network World's daily home for the not-just-networking news. He has been working with Network World since 1992. You can reach him at mcooney@nww.com.

Rip and replace: When it pays to make a total systems change

View Comments

YOU MIGHT LIKE

How a Moustache Helps Men’s Mental Health

Movember