Security Tools and Measures

Instructor: Many layers of security controls make up a robust defense-in-depth strategy.

Starting at the network perimeter, firewalls and other network security controls block or allow network traffic based on the needs and security posture of the organization. Firewalls, routers, and other network devices might enforce these rules at the network, host, port, or protocol level. Decisions can even be made based on the direction the traffic is flowing, the type of traffic being sent, and the connection status.

The network intrusion detection system, or IDS, watches the traffic for suspicious or anomalous behavior and sends alerts to security staff. Network traffic logging or captures provide records of all traffic and events for later correlation and investigation.

Access controls direct which data is available to which job roles, functions, or network areas within the organization. For instance, the finance department doesn't need access to the HR database, and the HR department probably doesn't need access to customer invoice records.

Antivirus software or host-based intrusion detection systems should be run on individual hosts and operating

systems. Host-based IDS and antivirus work hand-in-hand to detect malicious software and prevent it from running. This combination of tools can prevent a compromise or alert security staff to respond to a compromise.

Local system logs provide a record during a compromise and a method for auditing login attempts, new or deleted accounts, password changes, software installation, and remote access histories.

Encryption can also safeguard data within each system. Where access controls help segregate data availability by function or privilege, encryption protects the confidentiality of data from compromise. Even if encrypted data were accidentally leaked or stolen, it might not be readable in its encrypted form. Data can also be encrypted while in transit within or across the network to avoid sniffing or man-in-the-middle attacks.

Most systems and applications require some form of authentication to prove that you are who you say you are. Authentication can be achieved with a standard username and password pair, or something you know. When combined with biometrics or the use of smart cards, however, you increase the security of the authentication method by requiring the user to also provide something they are (in the case of biometrics) or something they have (in the case of a smart card).

Beyond these technical measures, simple door locks, security guards, and lack of physical access further diminish an attacker's ability to directly compromise a system, network, or data.

Lastly, users should periodically train on topics such as phishing awareness, what to do in the event of a suspected compromise, and personnel and device security. They should also be familiar with their organization's Responsible Use Agreement.

When combined to form defense in depth, each security mechanism is backed up by another so that no single failure leads to a catastrophic event. While the user is still typically the weakest link, proper training and multiple security measures help reduce the likelihood that small mistakes lead to larger incidents.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098