Testing and Monitoring Access Policy Controls: The Right Controls Can Boost Compliance and Efficiency

Save to myBoK

by Cheryl Traverse

Testing and monitoring access policy controls are critical best practices for all healthcare organizations. By testing and monitoring IT resources, perimeter security systems, and technical user activities, organizations can ensure service delivery, the protection of the resources that deliver those services, and their ability to enforce and validate access controls inside the infrastructure.

Without such assurances, an organization's intranet is vulnerable and susceptible to insider attacks and cannot effectively ensure regulatory compliance in terms of data protection and security.

Closing Visibility Gaps

Testing and monitoring networks, servers, applications, and databases are well-established practices in most healthcare organizations. With security levels heightening, many organizations also routinely test and monitor their perimeter security systems with firewall penetration tests, intrusion detection and prevention, and virus filtering.

But organizations must also address the threats to security and compliance presented by partners, vendors, offshore developers, managed service providers, and other technical or privileged users that have been admitted to the network. They must test and monitor access policy controls for these high-risk technical users that can close visibility gaps and ensure compliance.

For example, a medical treatment facility contains technologies and systems outside the realm of conventional IT infrastructure components, such as CT scanners, patient-monitoring devices, and test equipment that are generally beyond the scope of standard IT security measures. Such a facility may have dozens of pieces of medical equipment from various manufacturers that are supported remotely.

Typically equipment vendors require a virtual private network (VPN) connection to the facility's private network in order to support the equipment. This common practice can introduce unnecessary security risk by exposing sensitive data. Even segregating these network-enabled medical devices from the IT infrastructure network does not eliminate patient data breaches, because many FDA-approved medical devices operate using legacy technology. A compromised scanner, for example, gives unauthorized access to patients' scanned images and data stored on the device's hard drive.

Merging IT Operations, Medical Device Service, and Maintenance Platforms

As more and more medical devices become network enabled, the line dividing IT operations and medical device maintenance is diminishing. Traditionally medical device service has differed from standard IT operations in that medical devices use serial communication as the primary transport and IT operations use the network (TCP/IP) transport.

However, the process of upgrading, troubleshooting, transferring data, and other tasks performed on a medical device are fundamentally the same as those processes for an application server or network infrastructure device. Since most medical devices are now manufactured with built-in network transport capability, servicing a medical device is almost identical to servicing an IT infrastructure component.

Recognizing the benefits of merging the two technology platforms helps healthcare organizations properly plan for the consolidation of these operations within the context of centralizing access, policy enforcement controls, controls testing, and reporting.

Implementing Test and Monitor Guidelines

The following tips for assessing access controls cover the combination of IT operations, medical device services, and maintenance processes. In these tips, technical, privileged, and third-party users refer to any individual or groups of individuals that are authorized to access network resources or medical equipment in an organization's network.

Access by Exception. Healthcare organizations come to expect that vendors require a VPN connection in order to provide maintenance services. With a VPN connection (regardless of whether it is an SSL or IPSEC protocol) the access model typically has a predefined encrypted domain and a default access policy that gives the user full access to all resources inside that encrypted domain.

In order to restrict a particular VPN user's access to authorized resources, exceptions in the form of rules or nested access policies must be created to block the user from all unauthorized resources within the encrypted domain.

Healthcare organizations should consider adopting technology that allows them to adhere to the principle of the least privileged, which is also known as deny all, permit by exception (DAPE). In the DAPE model, each user or group account starts with no access or visibility to anything in the entire infrastructure. In order to grant user access to specific resources on the network, an exception is created to give highly granular resource access permission to an individual user or group of users, allowing visibility to only that explicit resource.

Switching from a VPN model to a DAPE model provides an immediate security improvement. Moreover, the DAPE model simplifies testing and monitoring of access policy control because all privileged users have no access by default and each is granted access to only a short list of specifically authorized resources. This condition is much easier to test and monitor than if these users had full access by default and each had to have a long list of rules blocking out unauthorized resource access.

True Separation through Compartmentalization. Many healthcare organizations are seeing an increased need for sharing data across separate domains. A good example is the domestic sharing of medical information between the US Department of Veterans Affairs and the Department of Defense systems. The biggest challenge here is not how to let users in, but how to ensure they are only given visibility to explicitly authorized resources so that critical information such as patient data and classified information is not compromised. Compartmentalization is key to achieving true segregation of duties as required by many regulations.

Techniques such as port-based access provisioning give very granular control over the information the authorized user can see, hiding everything else. For example, using a port-based access method, the organization can let a vendor in to troubleshoot a database but prevent the vendor from reaching the operating system that the database server runs on.

By eliminating unnecessary exposure of the IT infrastructure and limiting the reach of individual users when they are on the network, the organization is effectively reducing the testing and monitoring scope, which in turn reduces the overall cost of compliance.

Containment to Authorized Access Areas. The biggest exposure for healthcare organizations derives from leapfrogging: the ability of an admitted user on the network to hop from an authorized resource to other unauthorized resources on the same network. The lack of access containment security controls is the biggest vulnerability for any healthcare organization that grants remote access to technical, privileged, or third-party users.

Security policy enforcement technology can effectively contain users to their respective authorized areas by automatically testing and monitoring changing conditions to detect any user attempts to jump to an unauthorized server or device on the network. When a violation is detected, the connection is blocked, the user is warned, and an alert is sent to the specified authorities.

Tracking and Reporting User Activities. Collectively implementing centralization of access, policy enforcement controls, and containment is necessary to automate and simplify the testing and monitoring of access controls. The net result is the assurance that healthcare organizations require to operate efficiently, securely, and compliantly.

Centralized tracking and logging of user activities is essential to passing the audits necessary to achieve regulatory compliance. As such, healthcare organizations should consider implementing session recording for both command-line interfaces and graphical applications. These can provide the forensic details necessary to support the results obtained from routine monitoring and control tests as required by the compliance department or the external auditors for the healthcare organization.

HIPAA regulatory compliance mandates are weighing heavily on virtually all areas of the healthcare industry. While organizations are aware of the criticality of testing and monitoring access policy controls (particularly for third-party privileged users), many are not doing it because the task is daunting, time consuming, and resource intensive. By implementing controls and technology that compartmentalize and contain network users to authorized applications and devices, organizations can secure highly sensitive patient data and ensure regulatory compliance.

Cheryl Traverse (ctraverse@Xceedium.com) is president and chief executive officer of Xceedium in Jersey City, NJ.

Article citation:
Traverse, Cheryl. "Testing and Monitoring Access Policy Controls: The Right Controls Can Boost Compliance and Efficiency" *Journal of AHIMA* 79, no.5 (May 2008): 54-55.