THE AUDITORS CHECKLIST

STORAGE SECURITY

8

questions internal auditors should ask their security and infrastructure teams, to determine whether storage is sufficiently secured and whether data is fully protected.

BACKGROUND

The vast majority of critical data is stored in storage systems. In fact, one storage system is equivalent to about a thousand servers. Attackers can circumvent many existing protection layers, to do great harm: steal data, tamper with sensitive records, and destroy your data and its backups.

External auditors are now paying attention to storage security, and failure to show effective risk controls may lead to severe penalties.

1 Do our security incident-response plans cover storage-centered attacks? If so, does it address the following scenarios:

- Recovery from a complete wipe of a storage array
- Recovery from a complete corruption of the SAN fabric configuration
- Recovery from ransomware

2 Is there a complete inventory of storage devices that includes the current security status for each one?

- All storage arrays (block, file, object), SAN switches, backup, & archive environments?
- Storage software versions and, in particular: patching status, known CVEs, and resolution status?
- What is backed up? Where? How?
- Which storage protocols are allowed? Are all obsolete and insecure protocols disabled?

3 Is there secure event logging and auditing of storage infrastructure?

- Central log services (including redundant and tamper-proof records, and redundant and reliable time service)
- Configuration change audit (e.g. track what changed and when - in device configuration, storage mapping, and access control)

4 **Do you have an established security baseline process for storage infrastructure?**

- Security baseline and configuration baseline implementation document set
- Process for regularly validating adherence to baseline and post changes
- Process for updating the baseline according to best practices and to deal with emerging threats

5 **Is there a well-documented, and enforced separation of duties for critical storage services?**

- Separate admins for storage
- Separate admins for backup
- Separate admins for disaster recover

6 **Are all storage administrative-access mechanisms documented?**

- Separate admins for storage
- Separate admins for backup
- Separate admins for disaster recover

7 **Are existing mechanisms for ransomware protection, air-gapping, and copy-locking used? Is there an audit process to verify they are correctly deployed at all times?**

8 **Is the security of storage systems regularly audited? Does this audit process include:**
SAN communication devices, storage arrays (block, file, object), server-based SAN, and backup?

FOR EACH OF THE ABOVE QUESTIONS:
how easy is it to prove? Can it be done automatically? If not, what would be the cost – in time and money – to produce?

BOOK YOUR STORAGE RISK ASSESSMENT

See how secure your storage systems are with this one-time assessment. Get recommendations on resolving any risks that are identified

CONTINUITY