A Five-Layer View of Data Center Systems Security

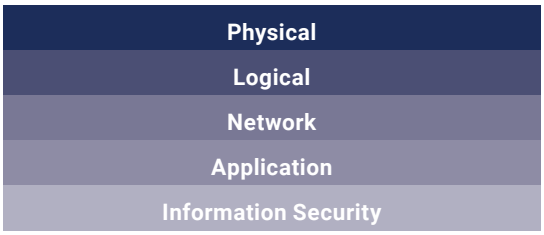
The data center is the central nervous system for any organization. As the hub of servers that host business-critical data, the data center needs special attention. There are some basic checks required for keeping IT systems safe in the data center. It is imperative for IT systems auditors and system maintenance teams to understand these checkpoints.

In addition to checking information security practices and defensive mechanisms, it is equally important to assess backup procedures and practices to strengthen the organization's resilience following a security attack. The rule of thumb is that information security audits should assess the confidentiality, integrity and availability (CIA) triad.

There are five layers of data center systems security (**figure 1**), and there are checks required in each of the layers.

FIGURE 1

The Five Layers of Data Center Systems Security



The Physical Layer

The perimeter layer meant for protecting the systems hosted inside the data center is the physical layer. Practices of protection at the physical layer include access controls for data center rooms, racks, servers and entry processes. Protections also ensure checks for availability of data copies at different physical locations.

- **Data center physical access controls**—It is important to set up multifactor authentication (MFA) for accessing data centers and to maintain surveillance controls at entry and exit points and inside data centers. Data centers are not like typical workspaces that allow frequent access and casual visits. These first-level checks and controls are essential for data security.
- **Locking controls for server racks**—It is necessary to prohibit external device access to servers and guard against potential data leakage through unauthorized cable connections. Locking controls help prevent data theft and physical disruptions.
- **Checks for security breaches at the hardware level**—For remote monitoring of hardware, the usual practice is to connect base hardware to

RAVI SHANKAR VEMURI

Is an IT infrastructure manager with ACT Fibernet, an India-based Internet service provider. He has had multiple opportunities to implement state-of-the-art compute, storage and network systems. Vemuri has helped deploy highly efficient disaster recovery solutions and identity management and enterprise backup solutions for safeguarding critical data, managed multiple operating system (OS) environments, and participated in complex application and storage migrations. Prior to ACT Fibernet, he worked in the banking and telecom industries, primarily in IT and telecom infrastructure management roles. In his 19 years of experience, Vemuri has managed diverse environments in IT infrastructure, IT development, telecom operations and project management roles.

"Because not much outgoing traffic is expected from the virtualization layer, Internet access can be restricted for the most part."

the network. However, revalidation of the connectivity requirements is necessary for proper access control.

- **Firmware upgrades**—Original equipment manufacturers (OEMs) are the best judges to advise on firmware upgrades. Infrastructure teams should take manufacturers' recommendations to upgrade firmware to safer and more stable versions.
- **Process checks for exiting employees**—Removing physical access must be included in the exit formalities for all employees leaving the organization. Human resources (HR) and IT teams must coordinate to regularly reconcile the access list.
- **Access to external agencies**—Temporary access to hardware vendor support teams must be closed immediately after the support ends. In the case of the cloud, there is a higher scope for such measures given the scale of operations and client audits.
- **Disaster recovery strategies, off site backup procedures and business continuity plans**—Building resilience is important to counter disruptions such as earthquakes, fire accidents or other catastrophic events. Factors such as degree of criticality of data, recovery point objective/recovery time objective (RPO/RTO) and regulatory compliance requirements are important elements of disaster recovery (DR) design strategies. These strategies should include such considerations as location of the DR site, scope of applications, size of hardware, bandwidth requirements between the data center and DR sites, data replication methods, and frequency of DR failover/failback activities. The main focus here is on physical availability of a data copy in a cross-location site. In the case of a natural disaster, the goal is to be adequately equipped to recover critical data.

Logical Layer

The logical layer refers to the operating system (OS) environment. Protecting the logical layer addresses security of the virtualization layer, optimization of the OS footprint, use of traditional and next-generation defensive mechanisms to secure OS instances, and adoption of best practices and processes related to the work OS footprint.

- **Virtualization layer security**—This layer is easy to handle. Version updates, port hardening and Internet blocking usually require only a few services running on top of the virtualization layer to control ingress traffic. Simple Network Management Protocol (SNMP) and some limited specific services are required for monitoring. Therefore, it is easy to implement restrictions on ingress loads. Because not much outgoing traffic is expected from the virtualization layer, Internet access can be restricted for the most part. Organizations should keep virtualization software updated to avoid security bugs common in older versions.
- **Regular patching and removal of old and unsupported operating systems**—As a security defense mechanism, patching is a nonnegotiable, regular operating activity for data center teams. For example, Microsoft releases security patches for Windows operating systems on the second Tuesday of every month. Operations teams must complete these patches in a timely manner, as they fix all known bugs. Many leading OS manufacturers sunset older versions and stop releasing security patches for them. Thus, organizations need to be ready to move away from older OS versions. This requires advanced planning and execution.
- **OS installation**—It is always better to start with safe installation practices. This approach helps to avoid both vulnerabilities and downtime once the instance is put into production. Some of the key practices are changing default security settings and passwords, avoiding unnecessary packages, secure shell (SSH) hardening, and server hardening practices. The principle of least privileges should be adopted when providing user access. This means that only appropriate privileges are given to users based on the requirement. A casual and liberal approach to this process is not safe.
- **Secured login through PAM tools, two-factor authentication**—Logical access controls primarily help to counter brute-force attacks and guard against unauthorized access. Privileged Access Management (PAM) tools are useful to establish single sign-on requirements, and they offer strong password management features. These tools make it easy to maintain access logs and help ensure audit compliance requirements.

- **Password management practices**—Though PAM tools help achieve best password management practices, it may not be possible for all organizations to implement such tools for all instances. Still, every organization should define and implement a password management policy comprised of best practices such as password expiration settings and complex password requirements.
- **OS configuration backups, snapshots**—It is safe to have snapshots enabled on critical legacy systems. In case of any negative incidents or data inconsistency issues, it would be tedious to recreate complex installations. Snapshots and configuration backups can come in handy.
- **OS footprint optimization**—"Less luggage, less risk" is a good principle when it comes to optimization of the OS footprint. Optimization should be an ongoing process that is part of regular operations. To achieve this, infrastructure teams need to work closely with application teams to consolidate and reuse application processes. This approach will not only mitigate risk related to OS and application vulnerabilities, but it also lessens maintenance workloads. It also helps improve the utilization of hardware and software resources.
- **Process checks**—Some process checks may seem obvious, but it is important to ensure that they are foolproof and automated. A typical example is removing logical access for exit employees.
- **Traditional defense mechanisms**—Mechanisms such as antivirus and antimalware protection for servers and patching of operating systems are nonnegotiable. Their use must be ensured 100 percent of the time on all relevant systems. Some built-in OS mechanisms, such as SELinux, can be checked and implemented as appropriate.
- **Next-generation defensive systems**—New tools, such as products from FireEye or Carbon Black by VMware, to counter advanced persistent threats (APT) are being created and organizations should consider implementing them. These tools are smarter when it comes to early detection of attacks based on unusual behaviors and pattern changes.
- **Special focus on endpoints of system administrators**—Laptops of system administrators require special focus. System administrators regularly log in to servers for maintenance activities, and their machines pose a bigger threat if they are not secured properly. Up-to-date patches, antivirus updates and the use of data loss prevention (DLP) tools need to be mandatory basic checks for these systems.
- **Untrusted software**—The entire data center environment will be at stake if untrusted software is introduced to the system. Regular audits on all systems must be mandated for identifying such deviations. Defensive systems such as antivirus programs need to be fine tuned to detect untrusted software.

"Usually a neglected area, restricting outbound traffic is as important as regulating inbound flow."

Network Layer

The network layer comprises elements such as switches, firewalls and routers. These critical gateway elements must be properly configured to safeguard against attacks. Securing the network layer requires placing restrictions on inbound and outbound traffic, optimizing network interfaces, applying microsegmentation, and using safe firewall configuration methods.

- **Optimization of Internet access for OS instances**—Usually a neglected area, restricting outbound traffic is as important as regulating inbound flow. During a ransomware attack, the attacker's central command center tries to establish a connection with the attacked instance. Internet restrictions help to prevent this connection and thwart further development of the attack. As a rule, Internet restrictions need to be applied at the firewall level for all the subnets. "Deny all" should be the first policy, and then exceptions can be applied on a case-by-case basis consistent with the application requirements.
- **Removal of unused network interfaces**—It is important to remove unused paths as a part of regular operational activities. Continual changes and developments will render some network paths redundant. Regular audits and optimization of such paths are recommended. Examples of such cases include:

LOOKING FOR MORE?

- Read *Achieving Data Security and Compliance. www.isaca.org/data-security-and-compliance-2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

"Organizations need to ensure prompt renewal of SSL certificates and change encryption keys periodically."

  - Network interfaces at virtualization and bare-metal OS levels
  - Unused but activated ports on network switches, routers, firewalls and load balancers
  - Redundant policies and routes on firewalls, routers and load balancers
- **Denial of public IP assignment at the OS level**—Avoid assigning public Internet Protocol (IP) at the OS level as far as possible. Though there are firewall features at the OS level, network firewall appliances that are intended for this purpose are better suited to protect at the central level. Preference should be given to Network Address Translation (NAT) and proper restrictions should be applied at the firewall level. It is easier to manage these controls at central devices. There can be exceptions, such as with Domain Name System (DNS) instances, that require applications with built-in advanced security features.
- **Removal of VPN access for exit employees**—A virtual private network (VPN) is the entry point for sensitive internal networks. Controls at the VPN level are simple to apply and very effective. These processes are nonnegotiable and must be carried out religiously.
- **Microsegmentation of networks**—Though complete blocking of cyberattacks is the goal, there would be some situations where just containing the spread is critical. Smart design and microsegmentation of data center networks helps.
- **Conservative approach**— "Deny all" first, and then "allow" only required traffic. This should be the mantra for firewall policy makers.
- **Firmware upgrades on network equipment**—Central network elements, such as firewalls, are critical devices; therefore, infrastructure teams typically hesitate to apply major changes to these boxes. However, it is important to install firmware upgrades promptly to avoid future downtimes and out-of-control situations.
- **Checking IPS signature updates on firewalls**—Due to network or support issues, firewalls may stop getting intrusion prevention signature (IPS) updates. Organizations need to implement monitoring checks on this.
- **Configuration backups of network elements**—Configurations of central elements such as firewalls, load balancers and switches are critical, and there should be a mechanism to extract these backups to a place that network administrators can easily access.
- **Segregation of production and backup data**—It is important to guard against the spread of attacks from production environments to backup instances. Based on business criteria, organizations can resort to older backup methods (e.g., tapes and offsite backups), newer technologies such as airgap solutions or hybrid approaches.

Application Layer

Reviewing the processes at the application layer is critical for safekeeping applications and database systems. At this layer, emphasis is placed on secure methods for maintaining application and database instances, segregation of production and test environments, use of robust data encryption methods, and implementation of code and database backup systems.

- **Data encryption mechanisms**— Encryption of data at rest and data in transit is critical to avoid data leakage. Applications and database systems should be designed to ensure compatibility with the latest and most stable Secure Sockets Layer/Transport Layer Security (SSL/TLS) methods. Organizations need to ensure prompt renewal of SSL certificates and change encryption keys periodically.
- **Defense mechanisms such as web application firewalls**—Web application firewalls (WAF) add protection from layer seven attacks, including HTTP flooding and web security vulnerabilities such as Structured Query Language (SQL) injection. Typical network perimeter firewalls are not capable of dealing with such attacks; therefore, additional security must be added through a web application firewall (WAF). Because WAFs are a relatively new technology, their use adds complexity to operations. Security teams need to gain good understanding of this technology and

ensure blocking mode is used for all critical public-facing applications under WAF.

- **Safe coding and database installation practices**—It is always best to do things right in the initial stages of application building.
- **Application code backups and database backup procedures**—Keeping at least two backups is recommended (one in the same location and one cross-location copy).
- **Segregation of production, development and testing environments**—Segregation is important primarily to ensure that the production environments are secured. A similar concept to microsegmentation, this helps avoid the spread of attacks from test setups to production setups. Test setups are more vulnerable given the high scope of experimentation there.
- **Restrictions on production environments**—Access restrictions are required to avoid negative impacts on production environments. In the case of smaller organizations, if it is not possible to have segregated teams, segregation of networks will help prevent mistakes.
- **Process of log capturing for critical application and database changes**—Easy tracking of changes and quick turnarounds are helpful in case any issues arise due to changes in production environments.
- **Password management of application and database users**—Best password management practices should be followed in application and database management, similarly to OS user password management.
- **Secured connectivity for interapplication dependencies**—Infrastructure teams should take all the necessary information from application and database teams and ensure that only required ports are opened for interapplication and database connections.
- **Consolidation of database instances and reduction of database footprint**—The "less luggage, less risk" principle also applies in database consolidation and footprint reduction, similarly to the OS footprint.
- **Special focus on public-facing applications**—Public-facing applications are inherently more vulnerable to attacks. More focus and security are necessary for web, mobile and third-party applications because there is less control over them.

"The five-layer view covers all aspects related to the security of data center systems and it consolidates them all into one comprehensive guide."

Information Security Layer

Security checks on the physical, logical, network and application layers are mostly managed by system administrators and application development teams. Further governance checks come under the responsibility of information security teams. These responsibilities include:

- Reviewing cyberthreat intelligence systems and operations of the organization's security operations center (SOC)
- Reviewing defense mechanism tools such as firewalls, antivirus and WAFs
- Reviewing information security operations, including vulnerability assessment and penetration testing (VAPT) activities and external and internal audits
- Checking the information security awareness quotient of the organization (i.e., reviewing cybersecurity awareness programs, providing information security training to system admins)
- Checking standard operating procedures, change management procedures and documentation
- Reviewing the IT security policy
- Checking data privacy terms and conditions in nondisclosure agreements (NDAs) with vendor partners
- Reviewing agreements with employees to strengthen the privacy of the organization's sensitive data
- Providing a 360-degree view of the robustness of the information security of the organization, including internal controls, system robustness, controls on partners, risk from customers and additional controls for cloud hosting

Conclusion

Basic checks are required for keeping IT systems safe in a data center. These checks can be viewed from five different perspectives: physical, logical, network, application and information security.

At the physical level, the focus should primarily be on process controls rather than technical aspects. At the logical level, the focus should be on security of operating systems. At the network level, the focus should primarily be to optimize and secure inlets and outlets of the data center network.

At the application level, the focus is two-fold: how to secure applications from attacks and how to secure business-critical data. At the information security layer, critical governance checks should be undertaken by information security teams.

The five-layer view covers all aspects related to the security of data center systems and it consolidates them all into one comprehensive guide, making it easier for practitioners to implement effective security.