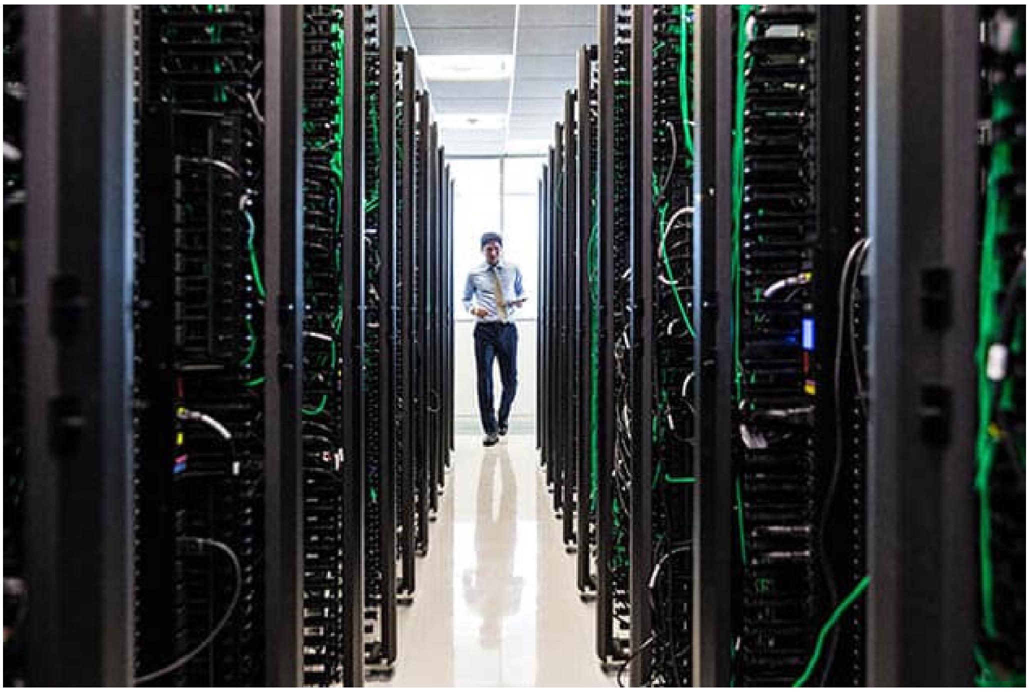
Building Secure Data Center Networks

stl.tech/blog/building-secure-data-center-networks/

Nitin Abbey, Marketing Manager, Sterlite Technologies

November 28, 2022



How to build secure data center

Data center security is transforming all the time. The need for fully equipped data center security solutions results from constantly changing regulatory requirements. Also, cloud migration and the increased frequency of cyberattacks are pushing the envelope for building a more secure data center network. The cyber-attacks globally have increased by 28% in the 3rd quarter of 2022 when compared to 2021 during the same period. The average number of cyberattacks per week has reached 1130 plus per company worldwide. As most companies use data centers for managing IT operations and data storage, making them robust in terms of security is imperative to prevent cyber-attacks and security breaches. Here are 7 steps to build a strong and secured data center.

Common Cyberattacks affecting Data centers

- Ransomware
- Distributed denial of service (DDoS)
- Malware
- Phishing
- External attacks
- Brute-force attacks

7 Steps to Build Secured Data Center Networks

1. **Secure the physical location of the data center**

The on-premise environment for a data center includes the geographic location, ground, underground, building space, and utilities that power it. Here are some tips.

- Choose an ideal location that is not prone to floods, earthquakes, storms, or other natural disasters.
- Select a place to deploy a data center with alternative power sources like solar, wind, etc.
- The place must have good water source availability for cooling the equipment
- Choose an area that has good network connectivity
- Provide limited access to the data center to simplify physical defenses
- Create proper measures to combat emergencies like a fire, water logging, pests, etc.

2. Review, Monitor, and limit physical & remote access

Secure access is imperative to protect a data center. To provide safe access, develop multiple layers of protection that control the permission levels of each individual. Some of the steps for securing data center access are:

- Maintain 24/7 vigilance using CCTV and on-premise security officials
- Provide layered access to every section of the data center facility
- Use facial recognition, biometrics, smart cards, etc., to provide secure access
- Use cloud security solutions like SASE (service edge), XDR, etc., for employees working remotely

3. **Secure your network & data**

Securing your data center includes safeguarding both stored and moving data in and around the networks. Some of the steps include:

- Deploy a zero-trust security model that presumes every inch of network traffic is potentially dangerous
- Use state-of-the-art tools & services to protect data and networks like firewalls, IP address monitoring, DDoS protection, etc.
- Constantly review and upgrade data center security policies.

4. **Provide security awareness training to every employee**

To provide effective training to your workforce on security awareness, avoid the long lecturing session and hundreds of pages of reading materials. Use Continuous but short awareness video bites & analytics.

5. Upgrade and maintain your data center

Regularly updating the data center’s hardware and software is essential to provide foolproof security. Some of the steps include:

- Replace the existing hardware of the data center every 2-6 years

- Always patch the design center software with the latest security fixes

6. **Setup a data backup**

Run frequent data backup sessions for your data center so that in case there is a natural disaster or cyberattack, you can easily retrieve backup data.

7. **Segment your network**

Segment the data center’s network to limit the impact of a data breach only to a few areas rather than the entire network.

Conclusion

Securing your data center involves considerable planning and effort in monitoring and protecting the facility both physically & virtually. The above 7 steps offer the best chance of creating a secure environment for your data center network and minimizing the chances of encountering data breaches and cyberattacks.