www.pipelinepub.com
Volume 19, Issue 2

Understanding Essential Data Center Security Needs

By: Rafael Possamai

Data centers are the core that allow our world to remain connected. The safety, security, and privacy of the information and connections within these facilities must be guarded and protected in several ways. The three main areas of data center security typically focus on physical and cyber security along with best practices data center operators should consider when it comes to overall security.

Physical security leverages remote and on-site monitoring, well-designed buildings, biometric scanning, badged access control, and more. Digitally, the cybersecurity side of any organization must also be robust. Network segregation, restricted access to physical devices, live network monitoring, and regular auditing are just the beginning. To ensure all elements of security are addressed, businesses must also commit to well-defined policies and procedures, often crafted by experts leveraging relevant industry certifications.

This article will address the three essential security realms that data center operators and network engineers should consider when understanding the demand for data security in their facilities.

Why data center physical security is critical

Data center operators should consider physical security as their main area of focus when it comes to guarding and protecting client data. Most companies that are seeking to store their data in a data center usually pay close attention to the security systems that are on site to safeguard critical information.

Most data center operators have man-traps, biometric scanning, armed guards, and more. However, some go the extra mile by providing enhanced security with two-factor authentication (2FA) and badged access with paperwork that needs to be completed for clearance. In addition, some data center operators may require background checks for individuals who will be visiting or engaging with a customer deployment, especially if the type of access being requested is unescorted. This is not uncommon as some data center operators have contracts with government agencies that may require certain levels of security clearance.

Prior to any prospect arriving at a data center site, some facilities utilize gates that require a badge and/or PIN for entry. Armed security guards are common on site and are usually former military or police with experience to handle any situation given the need. These security guards are usually behind the camera scanning the facility and its surrounding areas, as well as patrolling the grounds for any unauthorized visitors outside of employees or clients that are checking on their deployment.

Some may ask why there is a need for such robust security. Beyond protecting sensitive and private customer data, most data center prospects require a deeper layer of security to protect their information.

To meet these requirements, some data center operators may have the option to develop locked cages for customer deployments. While not required, some government agencies or agencies involved in other high-level projects require private cages with locks to ensure that even at the external level, the internal level of security must match what is already provided by the data center operator.

In some cases, data center operators themselves may require additional access to these secure and private cages at the request of the customer after initial deployment has been completed. This provides an extra layer of security to ensure critical data is protected 24/7/365.

Cybersecurity should remain at the forefront

Cybersecurity is another main priority for data center operators who are considering all bases to be covered when it comes to data protection and security.

Facility network operators manage and ensure that network segregation is in place. This means having separate networks for each distinct system, such as security cameras, access control, guest Wi-Fi, internal corporate networks, and more. These are directly managed via VLANs and ACL to minimize exposure to any one network segment in case of a breach.

The need for increased security not only physically but digitally arises from the increased targeting of corporations by cybercriminals. These cybercriminals have a skill set that includes ransomware, network takeovers, and now a new type of threat called system wiping or ‘wipers’.

Typically, ransomware attackers will infect an internal file of an organization and then proceed to lock private and internal data for money. Now, attackers have released the ‘wipers’ to infect systems, and instead of locking files for ransom, they are destroying all internal network data, which includes company data, personal data, client data, and more.

In recent years, the United States Department of Justice released a news notice that cyber attackers were going after the data center industry and MSPs. They target the data center industry to try to gain leverage over the existing customer information of data center organizations. With increased threats and new types of cyberattacks being brought to the forefront, data center organizations must take additional action to

prevent and fully mitigate these cyberattacks. Network engineers and network operators are increasing their awareness of these attacks and are also taking precautionary and proactive measures to get ahead of these issues. Most network operators will restrict physical access to networked devices by means of disabling unused network ports in common areas of a facility.

Conducting regular network infrastructure checks is critical to help mitigate any potential attacks. Monitoring network infrastructure with alerts and alarms also aids in early detection of potential issues.

Having a robust and clear plan with the network team in place can help data center operators stay ahead of the curve with cybersecurity. In addition, having dedicated security and access policies and procedures in place within the organization helps ensure employees and customers alike are aware of security expectations and requirements.

Data center operators and their IT team must work hand in hand to ensure that their employees follow all security protocols, including the use of a company VPN, 2FA login codes on devices, and also remain alert to phishing emails and malicious links or documents.

In addition to a workplace cybersecurity policy, IT teams must do their due diligence by having training sessions on cybersecurity to help employees understand what type of cybercriminals are out there and the attacks they should be on the lookout for.

Best practices for data center security

Given that data center security is a top priority for leadership teams as well as management teams in any given data center facility, common best practices should be applied throughout the organization. These include:

Clean desk policy

Usually, employees have a busy day-to-day schedule while on the job and it can be easy to forget something when in a meeting or on a personal call, so the reaction might be to grab a sticky note or piece of paper and jot something down.

This is not a good idea because it could potentially expose sensitive information to anyone that may be walking nearby or anyone that may not have the required access for that key piece of information. This includes passwords, account numbers, access codes, customer information and more.

Establish cybersecurity training

Ensuring that an organization's employees are fully trained on cybersecurity is essential. Employees who work in other departments that are not technical may not be aware of the cyberattacks criminals employ to gain access to organizational infrastructure.

By mandating cybersecurity training at an organizational level, employees will be educated on cyberattacks to look out for such as ransomware and will be better suited to relay this information to IT teams to investigate.

Reinforce corporate IT policies and procedures

Corporate IT policies and procedures are standard at any organization. By having the IT or network department work alongside their HR team, they should reinforce the IT and cybersecurity policies in place so that there are no hiccups when it comes to what is allowed in the organization.

For example, these may include prohibitions regarding use of personal cell phones or computers on company Wi-Fi networks or against conducting business on hardware that is not authorized by the organization.

Have leadership champion the security cause

The leadership team should champion the cause of security for the entire organization. Most internal teams seek the knowledge and understanding of senior leaders and are more than likely to listen to what they have to say.

Having the leadership team drive the message of security and cybersecurity from the top down will go a long way toward protecting the organization. If senior leaders are fully equipped and trained in cybersecurity, their message will resonate even further with employees.

Conduct consistent network audits

Consistent network audits with intrusion alerts cannot be overstated enough. This is one of the first go-to pieces of critical information to always monitor. By taking precautionary measures, organizations can identify if there are any gaps in their network that need attention.

Understanding the dynamics of physical security and cybersecurity is critical for any data center organization looking to implement additional layers of protection. The more mature your security posture is, the more potential prospects you have when seeking a data center provider.

By remaining aware of current and past types of cyberattacks, an organization will be well prepared to handle any situation.