morsewatchmans.com

Improve Your Facility's Network Security with Key Control

Fernando Pires

4-5 minutes

Data centers have long been the choice of organizations to house their servers and sensitive data. However, now many small, medium, and large business are choosing to house their data onsite to keep critical data in-house.

Those businesses that employ on-site servers and that store sensitive data in-house need to recognize that they are at risk of a cyberattack, given the fact that hackers are increasingly sophisticated and aggressive. Security breaches are always a

possibility, so making sure that your servers are protected against both cyber-intruders is critical.

Once sensitive data falls into the wrong hands, it can be difficult for a company to recover. The cost of a data breach has risen 12% over the past 5 years and now costs $3.92 million on average, according to the annual Cost of a Data Breach Report by IBM and the Ponemon Institute. The study found that data breaches that originated from a malicious cyberattack were not only the most common root cause of a data breach, but also the most expensive. However, inadvertent breaches from human error and system glitches were still the cause for nearly half (49%) of the data breaches in the report, costing companies $3.50 and $3.24 million, respectively.

In addition to having multiple and strong cybersecurity practices in place, such as turning on encryption, changing passwords from the default setting, educating employees, and more, businesses need to protect physical access to the network, meaning the server rooms, individual servers and other areas that house the sensitive data.

Another highly effective way to control physical access to your network is to control the use of the server room's physical keys with an electronic key management system. Keys secured in the tamper-proof key cabinet can be accessed by authorized individuals who have presented identification, such as a code, badge or other biometric identification, and been approved by the system. If a key is not returned to the key cabinet as scheduled, an alert is sent via email or SMS text to management so that immediate action may be taken.

All access activity is automatically recorded and from that data, management has a complete history of who removed and returned which key and when. The data gathered from the automatic recording of access activity can be used to analyze trends, in addition to use in an investigation. Trends that could take weeks or months to detect manually can be seen almost instantly.

A security team can query the system for specific details, such as a list of all transactions between certain times. Immediately following an incident such as an unauthorized person entering the server room, a report can be generated, showing who last accessed the particular key used to enter the area.

Organizations around the world are continuing to focus time and effort to secure their facility’s networks and to find ways to eliminate security weaknesses, and if they are not, they should be. By focusing on the physical security of a network and by working to controlling physical access to your servers, you can improve your company’s network security.