FULL-TIME SECURITY TO DEFEND OUR DATA

Cyber attacks are frequent. Every day, or every second, rather, there's a hacker somewhere in the world targeting other people's computers and when it comes to costs, they can be huge, both in terms of recovering the damaged system and the loss of information.

This phenomenon is now the major push for outsourcing data to external structures, rather than keeping them in-house.

While the theme of so-called cyber security, or the management of software attacks, is widely discussed, in this case we want to focus more on the physical security of the machines. Few talk about it, but often thefts of hardware and equipment occur by intrusion into the data center or offices. Cases are numerous, and famous, such as that of a few years ago at the Financial Times, at Watford's servers in northern London, which blocked the normal editorial work and publication for several days.

In many cases, the sole targets of the burglaries are hardware and networking devices within the data center. Thieves steal from web farms where there are machines of specific interest. Other times, however, these thefts are planned to find the data contained in the machines, and in this case, the damages are not only not cheap but also risky for corporate or public security.

We talked about this with Luca Beltramino, Managing Director of SUPERNAP Italia, and by now a data center veteran. "The latest hacker attacks have increased the need to migrate data to security- and redundancy-optimized infrastructures. They realized that it makes no sense to invest money to refresh the data center in-house because they cannot keep up with new technologies and new certifications. So, the focus is on points where security is highest. "

Beltramino continued, "In recent years we talk about cyber security, but it is equally important to focus on physical security. Experience teaches us that you can equip yourself with the most sophisticated software, but if you are neglecting your physical security, trouble is just around the corner. There are numerous things to do are. First, it is essential to ensure that your facility has specific rules for access to data halls; second, it would be useful to have anti-intrusion systems, preferably with professional personnel; and finally, in the case of sensitive data, encrypt it."

Data centers should therefore be physically built to safely guard the information contained therein and keep unauthorized people far away. How does SUPERNAP Italy operate? "For us at SUPERNAP Italia, physical security is paramount. Our facilities are equipped with a team of armed guards, hired and managed directly, working 7 days a week, 24 hours a day, and regularly visiting Las Vegas for specific training. Specific authorization is required to enter the data center, visitors are always accompanied within the data halls, and only after crossing multiple layers of protection that include both structural measures, such as walls and doors, and technological solutions, such as biometric scanners, all under video surveillance."

It's important also to think about other aspects, as Beltramino points out. "Structures that use Switch technology, such as SUPERNAP Italia, have been conceived and built to accommodate a data center, not re-adaptations of existing buildings, so they have all the features necessary to ensure the security of the data contained, even against natural phenomena. The decision to build in Siziano, in the Province of Pavia, was made not by chance, but after careful geophysical studies that allowed us to verify that there are very low seismic and flood risks. It is also a no-fly zone, and given the proximity to Linate Airport, a factor that prevents fly-overs thus eliminates the risk of such accidents."

In sum, physical security is clearly a major concern for the industry, but better options exist to manage it.