HOW TO SECURE A SERVER ROOM

With all the talk of artificial intelligence, developer strategies, and cloud technologies, the physical pieces that allow your company to function can easily go by the wayside. Hardware like personal computers and mobile devices are essential, of course, but without servers, access to the intranet and internet are simply not possible.

Of course, security plays a vital role in technology, but security should never be limited to software patches and updates. Securing your company – your data, your strategies, and your products – must start with securing your servers.

Servers and server rooms

Enterprise-level computing relies on servers. Typically, these are the physical computer devices that provide functionality for other devices, like individual employee computers or devices, which are known as clients. Depending on the company's size, you may rely on a single server or on a network of servers. Servers can also have specific functions in and of themselves: mail servers, internet servers, database servers, and application servers.

Servers require a lot (a lot!) of resources, such as dedicated power sources, required cooling for these powerful machines, and hundreds to thousands of physical network connections. Highly sensitive machinery, serves are very sensitive: any small change to a server can result in a significant network outage. That change can be a real tech problem or even something as seemingly small as a dip in temperature or a person fidgeting with the server rack.

For these reasons, server rooms are a necessity, no matter the size of your business. Servers need to be stored in dedicated, single-use rooms where the servers can run continuously. Servers and server rooms are best when left to run unattended, save for problems that require an IT administrator.

Server room considerations

Physically, a server room can be as small as a closet or as large as an entire building, depending on your company's size, capabilities, and reach. But you'll need to consider more than just the size of your current server needs. Instead, you'll need to consider a few factors:

- **Location.** Designing a server room isn't as simple as picking an out-of-the-way walk-in closet. You'll need to consider where your server room will be located, especially if you have offices in more than one location. A good rule of thumb: server rooms are not a multi-purpose room or a storage closet; really, server rooms should never be collocated.
- **Environmental controls.** Servers are high-energy, power-hogging machines and they can heat up fast. So, year-round air conditioning is a typical requirement, unless you live near the Arctic Circle. The environment should be conditioned to cool and reduce humidity, but the system should also be automated, so that IT admins can monitor it from afar – something known as a "lights out" server room. Lighting can even have a significant impact, so install motion-detection lights, which also help control the budget. Think of the server room as an oven (but much cooler) – every time the door opens, temperature and humidity can fluctuate, so you need environmental controls that can respond quickly.
- **Safety.** Perhaps no part of your business is as sensitive to emergencies as your server room. A flood, fire, or other act of god can destroy your server room, ruining company data, products, and more. Server rooms should be fitted for fire alarms, extinguishers, suppression systems, and moisture detection systems, at the very least.
- **Future growth.** Your server room may be enough for now, but are you prepared for a successful upcoming product launch? You may want to reserve additional space for adding servers as you scale.

Securing your server room

Designing a secure room is one thing, but securing it is an ongoing process – as soon as you think you're finished "securing" something, a new threat comes along. Unfortunately, securing a server room isn't as easy as installing some secure software. In most server environments, server security starts with physical security.

Think of physical security as who's allowed inside the server room and what those people may touch. Because servers generally run entirely on their own, very few people have any reason to go into a server room. In case of an error or for maintenance purposes, those folks should be limited to very specific IT personnel. Your IT department likely includes system and operational folks, developers, programmers, and engineers, and leadership positions, but most of those employees have no business being in a server room. The more you can limit access to the server room, the safer it will be.

Therefore, restricting access is essential. Start with determining who is responsible for the room:

- Which department owns access?

- Who establishes its rules?
- Who is allowed inside?

Next, you need to control and monitor the access, for both entrances and exits. Locked doors that require a key are not enough – they do not restrict access. Even if only three people have access to the server room, those three people can pass their keys to restricted persons who can then enter the server room.

Consider installing a camera at each door to the server room, because then you can track who is *actually* going in the room and when, as well as all attempts by non-approved persons who try to get into the room. Surveillance may not catch every movement, though, so motion sensors can pick up the slack.

Once the room itself is secure, you're not done. Servers themselves must be physically secured, too. Racks that hold the servers must be locked, both front and back, and their individual cages must be locked. Racks can serve as shocks, absorbing shifts in physical space, so that servers are less likely to move. Racks and cages also prevent people from moving servers around or otherwise tampering with their settings. You'll also want to lock networking and power cables and control that access. (If any cabling isn't collocated with the servers, the same access requirements apply to the "networking room" as to your server room.)

A combination of products, such as keys, fobs, and biometrics, may serve you best. But you don't need to get too complicated: mixing products and combinations can lead to gaps in your security.

Pie-in-the-sky security

Generally, a multi-layer approach to authentication is best. If money is no object, you can consider more advanced security options for server rooms.

A mantrap, also known as airlock control, is a small anteroom, with two doors that separate the hallway access from the server room entrance. These can have different designs:

- **Restricted entry, unrestricted exit:** the authorized person enters the first set of exterior (hallway) doors, which then lock behind the person. Then, the internal doors unlock. If timed in short succession, as is best, you'll prevent tailgating.
- **Restricted entry and restricted exit:** in this version, all hallway and interior doors are locked. The allowed person must authorize to get into the first door, which then locks, and then the person must authorize to get into the second door, which then locks.
- **Two-person authentication:** you need two approved people to open and access the server room, is particularly secure, which the NSA and other intelligence groups reportedly rely on.

Another expensive approach are biometrics, but security experts are divided. Certainly, biometrics is the cutting edge in securing anything these days. But biometrics can often be more of a show than a strong practice – an expensive magic trick. If you do opt to include biometrics, the best strategy is to incorporate it into three-factor authentication: a physical badge, a door code, and an iris scanner.

Securing server rooms is an absolutely necessity. It is not a cheap endeavor (would you want cheap security?), so you'll have to find some custom balance of security, accessibility, and cost. Leadership may be hesitant to invest in server security, but by knowing that something will go wrong, it's just a matter of when, you can choose to be on the offense instead of on the defense.

A good tenet of server room security: the more you control, the more secure your servers will be.