Physical Security and Information Systems

The first difference that appears when reinforcing the security of a personal computer and reinforcing the security of a data center's server is **location**. In fact, with a personal computer, it's not necessary to set a physical security system to restrain machines' access to "normal employees". In big data-centers, before starting thinking about a **Software-level security system**, the System Administrator has to make sure that accessing the server is not as easy as getting to the office's coffee machine. In some data centers, sysadmins and everyone else appointed for server's maintenance have relevant credentials to pass an **electronic security system** such as encoded Ids, fingerprints scans, passcodes and so on. A **three-factor authentification (3FA)** system is one of the best security system when it comes to protect servers from unwanted reaches and **social engineering**. The system simply rotate around 3 main point: **something you know**, **something you have**, and **something you are**. For instance, a person can firstly be prompted to input a code, then show an Id and finally scan her/his iris in order to be granted access to a certain area. When it comes to protecting **sensitive data** on a large scale, barriers should be installed so that machines are protected from unauthorized intrusions of all kinds. At the end of the day, it's primordial to understand that risks will always be present, however computer security specialists must keep a sharp eye on their physical and digital security systems.

Another difference that appears when reinforcing the security of a personal computer and reinforcing the security of a data-center's server is that **patch management** and **updates** must be strictly followed in data-centers. Technology evolves at the 'speed of light'; nowadays, new **breaches**, patches, and bugs pop-up on a daily basis. Data-centers must have a strict process for

software and hardware updates but also a group of professional following **Information Security news** in order to reduce the risk of potential cyber attack. IT professionals have to make sure that updates and patches systems are **up-to-date** and not only that; they have to constantly check that the system is **running periodically and normally** (at an enterprise scale for instance, many use tools like Ninite). If a problem 'stays' in the system for too long, damages may be huge.

Thirdly, another security aspect that put personal computers and data-centers' servers apart is that data-centers, because of what they are (a source sensible information), are victims of all kind of traits and attacks. A personal computer is less likely to be as famous and as publicly vulnerable as a data center. Investing in a reliable security software with insurance and having enough IT professionals to monitors the data-center's network irregularities is a must for big data-centers. Data-centers' servers must have additional layers of security and most importantly knowledgeable and reliable people taking care of it.

Resources

http://www.serverhardening.com/

Google

Class'slides on OS Hardenning