Introduction to Physical Security and Security of Services

Jennifer Vesperman

jenn@linuxchix.org

2002−02−24

Revision History

Revision 0.1	2002−02−17	Revised by: MEG
Converted from text file. Modified wording.		
Revision 0.2	2002−02−24	Revised by: MEG
Conforming to LDP standards. Added abstract.		

How does an individual or organisation assure their Internet services such as websites are available? This article discusses techniques for assuring physical security of hardware and methods of making sure the servers run and have Internet access.

Table of Contents

1. Introduction

1.1. Copyright Information

1.2. Overview

If an intruder gets physical access to a computer, they can easily gain access to the information stored on the computer. Methods range from simply tucking the computer under their arm and walking off with it to collect the data at leisure, to using a 'rescue disk' or some other method of starting the computer with no passwords, to removing the hard drive and starting it on their own computer, with full access to the information stored on the drive.

Most operating systems have some method of starting the computer with no passwords − this is intentional, because most organisations will lose or forget a critical password at some time. This can only be done when physically at the computer, however − the operating system designers rely on the user being aware of this fact, and securing the computer room.

There are methods, in most operating systems, of disabling the 'no password' start − if you choose to implement them, be extremely careful and document the passwords well. But secure the copy of the passwords.

1.3. Physically Securing the hardware

Keep any computers which have sensitive information away from the general public. Use common sense − locked doors, locked windows and security systems are all readily available. Your local police department is likely to have up−to−date advice on realistic security for your area.

There are specialist devices available for attaching computers to desks, or for locking computer cases closed. If you (or your local police department) feel that that is warranted for your system, buy them and apply them. Just remember that you also need to prevent an intruder from actually reaching the computer in the first place − information can be stolen without moving the computer itself.

---

2. Physical security of networks

Networks can be easier to secure − if there is a single computer (or a small group of computers) which hold the sensitive information, those are the computers which must be physically secured. Other computers can be left less secure, provided the network itself is secure and the unsecured computers don't have sensitive information on them − such as network passwords.

In 'big business' the computers which store the sensitive information are often kept in a special computer room, in a secured building. In small business or home environments, keep these separate − don't use them as regular computers. Make certain they're behind the scenes somewhere, away from customers.

3. Power

There are two issues with power supply. One is the matter of power smoothing, preventing sudden surges or drops in supply, and the other is supply itself. Blackouts and brownouts can cause the computers to shut down suddenly, losing any information stored only in short−term memory (RAM). Sudden surges or drops in supply can cause physical damage to computer components, if they are bad enough.

Power smoothing is only needed in some areas. Local computer experts will be able to tell you if your area's supply is prone to surges and dips, and can offer advice on whether you need surge protectors or power smoothers. However, if you buy a UPS (uninterruptible power supply), most have power smoothing built in.

A UPS (uninterruptible power supply) is used to protect against sudden loss of power. It's somewhat of a misnomer, as it doesn't itself provide power − it is essentially a large battery that charges itself from the power main. The computers are plugged into the UPS, and if the mains power cuts out, the UPS provides enough power for the computers to shut themselves down and save all their information.

Most UPSes will signal the computer when the main power cuts out. Get your local computer expert to ensure that yours does (preferably before you buy it), and ensure that your computer is set up to respond to that signal.

If you want a truly uninterruptible supply, there are companies in existence which would be happy to sell you a power generator that cuts in automatically when mains power cuts out, and a UPS−like device to handle the cutover to the generator.

---

4. Network Access

Network access, such as internet access, tends to be at the mercy of large organisations which run the local internet 'backbones' (the main routes). Even if you buy your connection through a small provider, their own connection is usually with one of the larger organisations.

The reliability of your local providers can be a significant issue to the success of your business − or it might not be, depending on what your business is. If it is important to have reliable access, you might want to either write reliability (and penalties) into your contract with them, or to have two different providers, who themselves, preferably, are connected to two different backbones.

If you have the two providers, you will probably need to have a specialist configure your network so that in the event of one provider failing you, your network automatically cuts over to the other. And that when the first resumes connectivity, the network routing switches back to a dual−route.