Physical Security

Best Practices for General User

Digital data are well-secured against malware thanks to firewall, and anti-virus software. However, if a computer is stolen, this kind of prevention will be useless. A physical barrier has also to be created to protect the resources of an organization. All levels of the network have to be protected in order to ensure the best security. In fact, in the OSI layers, the first one is the physical layer. In order to have an entirely secured system, physical security has to be taken into account.

Physical Security Threat

Several situations can constitute a threat to information system. Knowing them is the first step in systems protection. These threats can be caused accidentally, intentionally or by natural disasters.

- **Environmental Threats**

Natural disasters can result in catastrophic losses. Earthquake occurs without warning and can create great damages, even worse than hurricanes. Personnel and equipment are both at risk. Flooding areas can also provoke casualties with long lasting effects. Therefore the location choice of a data center is crucial.

Some environmental conditions can also damage systems and, thereby, data incorporated. Inappropriate temperature and humidity can lead to interruption of services and data damage. For instance, computer systems should normally be kept between 10 and 32 degrees Celsius[1]. High humidity can provoke corrosion whereas too low humidity can modify material shape and dwindle their performance. In fact, humidity should be maintained between 40 and 60%. Moreover, fire is not a threat only from the flame but also from heat, toxic fumes, and water damage linked to fire extinguishers. Finally, dust can block equipment with moving parts, as rotating storage media.

- **Technical Threats**

Electrical devices require uninterrupted utility voltage. In fact, if the voltage received is less important than the required one, (under 20%) the system will be interrupted and the computer will automatically shut down. In the case of an overvoltage, the damage will depend on the intensity and the duration of the surge of voltage. Some components can even be destroyed. Logical errors can be created by noise interference in the electronic device.

Electromagnetic interference can be caused by noise but also by motors, fans or other computers. Space, as well as power lines, can transmit these interferences. Nearby commercial radio station and microwave can also create interferences.

- **Human-caused Threats**

Human-caused threats are harder to manage because they are unpredictable, and are generally designed to pass through prevention measures. Unlike logical threats, which refer to damage done to software and data and are handled by hackers, physical threats can be achieved by people without any computer sciences knowledge. Theft of equipment and illegal copying of data can be realised by an intruder who gains unauthorized access or by an insider. Equipment can also be destructed as well as data and resources can be misused.

Moreover, data can also be recovered from old devices. If hard drive is not correctly sanitized before the sale of a computer, the purchaser can recover all the data and gain access to them. According to a student's analysis of 158 disk drives purchased on eBay[2], 71% contained old data that could be recovered and read, and even if 36% had been formatted, they still contained old data that could be recovered.

Only 9% were properly cleared. Thus, students easily got access to a log file containing credit card numbers, an ATM financial log file, medical records, and personal e-mails.

Student Information Exposure Caused By Laptop Theft[3]

In 2005, a laptop was stolen from a "restricted area" of the University of California Berkeley. The man entered the area while it was unoccupied. This computer contained files with names and Social Security number of over 98.000 students.

When a computer is accessed by someone else, it is not only the device that has been lost but also the valuable information that it contains.

Physical Security Prevention and Mitigation Measures

Physical Security represented a market of $48 billion in 2012 and should reach $125 billion by 2019[4]. To prevent the threats mentioned above, several measures can be taken.

- **Premises Security**

The choice of the site location is important to minimize likelihood of environmental threats. For instance, a data center should not be located on the top floor (for fire consideration), in the basement (for flooding consideration), in the core of a building (to provide protection from natural disasters or bomb attacks) or close to a public area (for security consideration).

Temperature and humidity can be controlled thanks to threshold warnings and air conditioner. The rate of humidity can be monitored thanks to a hygrometer. Fire can be avoided thanks to automatic fire detectors and extinguishers but those not containing water.

- **Technical Threats Prevention**

In case of power fail, alternate power sources should be available. Each critical room should be protected by an Uninterruptible Power Supply (UPS)[5]. It is a battery that will provide power to the equipment for a short period. This additional time should be used to shut down properly all servers in order not to lose data or to switch to a generator, which may take few minutes. In fact, when power runs out, all data contained in the RAM will be erased. For longer electrical issues, generators should be employed. If it is often supplied with fuel, the generator will be able to work indefinitely. Filters and shielding can prevent some electromagnetic interference.

- **Cloud Computing**

Cloud computing will reduce the number of physical systems and thus of physical access. All data stored in the cloud will not be physically threatened.

- **Human Threats Prevention**

In order to restrict access, several options are available. Restricting access to a building in which sensitive data are stocked will finally restrict access to these data. Lockers are the cheapest and easiest way to control access.

In order to prevent laptops and other portable hardware (as hard drives) from being stolen, security cables will fix hardware to the wall or to desks. Another option is to put a tracking device on movable resources to prevent it from being taken out of a predefined area. Also recognizable laptop bags should be avoided as well as using in public such devices.

Some simple precautions should also be applied to ensure minimal security. Writing down the manufacturer name, model and serial number of a laptop can help to find it more easily. A careless moment even very short is enough to rob a small device. Valuables should not be left in common areas or vehicles.

If a drive needs to be sanitized, the best way to guarantee it is to destroy it physically. However some less invasive methods exist. For instant, overwriting the drive's data will lead to the impossibility of recovering them. Simply delete or erase data will not remove them from the drive. Consumers need to be better educated to know how to erase properly data stored on computer hard drive.

- **Personnel Training**

In order to ensure physical security, users have to be aware. In fact, the foundation of security starts with individuals. Basic behaviour has to be respected. Any suspicious act should be identified and reported; employees should know how to react in the case of an incident, therefore comprehensive security awareness should be provided to employee. Sensitive physical documents and equipment should not be easily detectable.

Moreover, up-to-date list of personnel and their access right has to be provided to the security staff to ensure that only authorised people can gain access.

Physical Access Control System

There are several factors to authenticate a person. It can be done with something he knows as a password, something he owns as a token, something he is as finger print, something he does as voice recognition. Combining these factors increases security level.

- **Biometrics**

Biometric refers to the analysis and measurement of human body characteristics, thanks to technological tools, in order to authenticate people[6]. Generally, it consits of a reader or scanning device, a software to convert the information in digital data and to compare the matching points, and a database to store the data for comparison.

Iris and retinal recognition is based on the eye pattern. It is considered as being a secure form of biometric authentication because it is harder to duplicate. Iris recognition has a promising future and will be more and more present in daily life. The main challenge remains its high cost. Retinal recognition analyses the layer of blood vessels at the bottom of the eye. The process is 10 to 15 seconds long. To date, it remains mainly used for high-risk security. However, as iris scanning, it is promised to a bright future.

Fingerprint scanning is now widely used (even on the iPhone). However, it remains vulnerable. Thanks to gelatinous materials, fingerprints can easily be copied. In order to prevent it, manufacturers have added other components which take also into account the vein structure.

Figure 1: Fingerprint scanner[7]

Facial recognition is used both to authenticate and to identify. In fact, it can even be used to find someone in the crowd. It remains vulnerable since covering his head with a hat or wearing sun glasses is enough to disable the recognition as well as using a picture of someone else face. Voice recognition as face recognition can easily be reproduced thanks to sound recordings.

Speed, accuracy, user-friendliness, low-cost, public acceptability, reliability , resistance to counterfeiting and fast enrollment times are characteristics to take into account before choosing a biometric system.

- **Badges / RFID**

RFID badge contains the site code and the badge ID. Its operation is simple, employees have just to swipe their card in close proximity to a scanner[9]. Thanks to that, it is possible to determine the identity and passing time at a precise location of

each user. However, RFID has some drawbacks. Badges are easily cloned, and RFID is vulnerable to brute force attack. In fact, unlike smart applications which are able to lock out if too many failed attempt have been done, RFID system will let user try billion of times and as badge ID numbers are generally incremental the system will be easily cracked.

Compared to key, the main advantage is that a card can be disabled and thus, may deny access to premises a day after the end of an employee contract.

With the use of RFID the human part is being lost and unfortunately, scanner does not determine if the one using the card matches with the owner of the card.

Facial Recognition in San Francisco University[8]

On campus, students generally move together and only one person provides his badge for the entire group access. This creates a lack of security. In order to control dormitory access, the University of San Francisco was looking for a passive and non-intrusive way to check people identity. They finally choose the iOmniscient's face recognition system. This system can check many faces at the same time and thus remains operational even during peak hours. Thanks to this system, visitors can be identified by attendant for proper check-in.

- **Key Fobs**

A key fob is a key with an integrated control access to network services and information. This token is a two factor identification because it needs a token (the key) but also a pin known only by the owner. As it is an object, the owner will notice wether it has been stolen, whereas, people generally ignore wether their password has been stolen.

To use it, the user enters his pin and as a response, the token delivers a number to log onto the network.

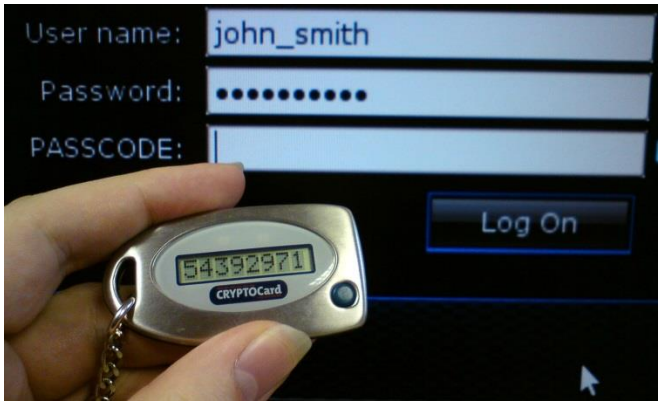

Figure 2: key fobs[10]

- **Security Camera**

Video surveillance has been existing for a long time but it becomes really sophisticated. Facial recognition can even be integrated. Camera definition and quality are constantly improving. The main limitation is due to bandwidth. It remain the largest market of physical security with 72% in 2012 and keeping growing[11].

Video monitoring systems are especially helpful in checking incident and historical analysis. To be used as a real time identification tool, a human has to be monitoring the screen all the time, otherwise security camera will remain confined to a role of gathering data.

Conclusion

Physical security is essential to improve security and is as important as data security. It would be a significant error to underestimate the importance of its implementation. Access should be physically limited only to authorised people. Moreover, education remains the key to avoid security threats. As each university has different needs and budget, each security protocol will be unique. Measures taken should depend on the operating environment.

References

1. "Google books: cyber Security and IT Infrastructure Protection by J. R. Vacca" 2013 Web. 29 July 2015
2. "Remembrance of Data Passed: A Study of Disk Sanitization Practices" S. L. Garfinkel and A. Shelat 2003 pdf.
3. "UC Berkeley police investigating theft of laptop containing grad student ID data" March 2005 Web. 31 July 2015
4. "Uninterruptible Power Supply" April 2015 Web. 30 July2015
5. "Physical Security Market is Expected to Reach USD 125 Billion Globally in 2019" 30 July 2015
6. "Physical Security: A Biometric Approach" SANS Institute Reading Room site 2003 pdf.
7. "Fingerprint scanner" November 2013 Web. 31 July 2015
8. "iOmniscient's Facial Recognition system deployed at the University of San Francisco to enhance security and safety of residence halls" September 2013 Web. 30 July 2015
9. "The 8 most significant ways physical security has evolved" January 2014 Web. 29 July 2015
10. "Crypto card two factors" October 2013 Web. 31 July 2015
11. "Physical Security to mitigate Social Engineering Risks"

Copyright Statement