GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Janet E. McIntosh

Laptop Theft

Laptop theft has been on the rise in recent years. A FBI report reported 39,900 laptops were stolen in 1999. Some of the reasons for this increase are that laptops are plentiful, small, easy to steal and they are worth lots of money. This paper will examine the numbers of methods and scams that are used to steal laptops, what criminals do with stolen laptops and finally some prevention tips for protecting your laptop.

Many scams have been used to steal laptops. One common scam is targeting victims at airports. One of every 10 laptop is stolen at airports. One method thieves use involves two criminals who position themselves between the victim at the metal detector. One of the criminals distracts the security personnel, by intentionally placing many objects in their pocket. While the first criminal is emptying his pocket, his buddy steals the victim's laptop as it comes off the conveyer belt. He graps the laptop and disappears into the crowd.

Another airport method used by thieves is similar to the old pick pocket scam. This one also requires two buddies working together. Victims carrying laptop on top of a luggage cart is vulnerable to this scam. Once the thieves ID their victim, one gets in front of the victim and abruptly stop causing the victim to drop his luggage on the floor. While the first thief is apologizing and helping the victim pick up his luggage, his buddy comes by and steals the laptop.

Finally, any unattended laptop is an easy steal for thieves. They look for people carrying cases that are obvious laptops. Hotels, conferences and airports are the prime areas thieves target laptop victims. Once the victim leaves the laptop unattended, the thief walks away with the equipment.

Laptop theft is also on the rise inside the office. A survey of IT and IS professionals of Fortune 1000 companies reported two out of five companies reported laptop theft in the office. Many individuals are being misled by a false

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

sense of security. They are relying on building security for laptop protection. Therefore many are leaving their machines unattended without taking proper security precautions such as locking the system down.

What use is a stolen laptop to a thief? Many thieves try to sell their stolen merchandise. First thieves sell stolen laptops to pawn shops where they could receive up to half its value in cash. Many use false identification so the stolen equipment can't be traced back to them. Computer swap meets are also another place thieves get rid of stolen laptops. Most swap meets are not checked by law enforcement for stolen goods and neither do the sellers report their sales or purchases to law enforcement. Again, another way to get rid of the merchandise without being traced.

Even though thieves can sell laptops for money, the data stored on the system can be more valuable than the hardware. Thieves are targeting certain laptops because of the data that is stored on them. Many employees have all kind of company information stored on their laptops such as financial data, proposals, business plans, and product designs. If this kind of information gets into the wrong hands, it can be sold to competitors, the media or use for blackmailing someone. A lot of personal data is also stored on laptops such as social security numbers, credit card numbers, addresses, and etc. Theft of this data can also be damaging to a company especially if the personal data is client information. Stolen laptops are often used to gain access to a company's network because laptop owners fail to protect their systems with strong passwords. With access to a company's network a thief can cause unlimited amount of damage such as install malicious code, steal sensitive data, delete files and corrupt valuable data.

Precautions must be taken to protect your laptop from theft, whether travelling or working in your office. The following tips should be considered for laptop users:

- Disguise your laptop by carrying it in an ordinary briefcase instead of a computer case. People carrying computer cases are an easy target for theft.

- Keep your laptop with you at all times. When going through the metal detectors at the airport, give your laptop to the security personnel for inspection instead

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

of putting it on the conveyer belt. If you are forced to but your laptop on the conveyer belt, place it on the conveyer belt only when you are next in line. Travelers should also be aware of their surrounding.

- Always lock your computer down. You can use an assortment of cables. You attached the cable to your PC and then fasten it to an immovable object such as a desk. Many security companies sell laptop cable kits. Computer Security Product, Inc. (www.computersecurity.com/laptop) has several one-piece units that uses the existing security slots and provides glue-on adapter for laptops without security slots.

- Back up all information including system and data files and store the media at home or the office.

- Use a removable drive for a second hard drive and store it in a safe place. If your laptop is stolen, this will reduce your downtime because the removable drive can be used in another machine.

- Install a utility that notifies the police when your PC is stolen. CompuTrace is a utility that allows you to do this. A program is hidden on your laptop that calls CompuTrace's server every few days to check in. If your PC is stolen, the modem silently calls CompuTrace which in turns notify the police.

- Users should encrypt all stored data. Encryption and decryption should take place each time a document is opened, saved, or moved.

- Laptops should be password protected with strong authentication. Computer Sentry Software has a product that will leave the computer useless if stolen. If your password is entered incorrectly three times, the product will contact a monitoring server, which contacts the user to tell them that someone tried to use the computer. The product also has the option of locking the keyboard and mouse.

- Companies should brief their employees frequently about laptop security. Employees should be made aware of current scams. Seminars, emails and newsletters are good ways to keep everyone informed.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- All laptops should be marked permanently with information such as the company's name with an identification number. This could assist the police in locating your system if stolen.

Laptop theft is a serious matter. Thieves are always targeting victims in airports, hotels, and conferences. A stolen laptop is more than lost hardware. If sensitive data is stored on a stolen laptop, someone can cause unlimited amount of damage to a company. Preventive measures must be taken to reduce the risk of lap top theft. Carrying your laptop in an unrecognizable case and using lock down devices will go a long in preventing laptop theft. Companies should also train their employees regularly so that they are always aware of the risk.

© SANS Institute 2000 - 2002, Author retains full rights.

Bibliography

CBOSS "TIPS: Avoid your own Computer Nightmare". http://www.cboss.on.ca/tips.html

Center News. "Laptop thefts on the rise; thieves target airports". January 16, 1997. http://www.fhcrc.org/about/CenterNews/1997/Jan16/Travel.htm

Computer Security Products. "Laptop Security/Laptop Theft". http://www.computersecurity.com/laptop/

Corporate Travel Safety. "Laptop Theft, Know Before You Go". http://corporatetravelsafety.com/laptoptheft.html

Insurance Information Institute. "LAPTOP THEFT PREVENTION TIPS". http://www.iii.aa.psiweb.com/inside.pl5?individuals=other stuff=/individuals/other stuff/laptop.html

Kensington Technology Group. "Most Reported Laptop Thefts Occur Inside the Office". January 26, 1999. http://www.kensington.com/about/press/security012699.html

PC World. "Protect Your Notebook and Its Data". Monday, September 18, 2000. http://www.pcworld.com/resource/printable/article.asp?aid=18497

PC World. "Secure Your PC From Thieves". July 18, 2000. http://www.pcworld.com/resource/printable/article.asp?aid=17676.

Wall Bock's Briefing Memo. "The Cost of Laptop Theft". http://www.bockinfo.com/docs/laptheft.htm.

© SANS Institute 2000 - 2002, Author Retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.