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

Espionage and the Insider

> Main Entry: **ES·PI·O·NAGE**
> Pronunciation: 'es-pE-&-"näzh, -"näj, -nij, Canad also -"nazh; "es-pE-&-'näzh; is-'pE-&-nij
> Function: noun
> Etymology: French espionnage, from Middle French, from espionner to spy, from espion spy, from Old Italian spione, from spia, of Germanic origin; akin to Old High German spehOn to spy -- more at SPY
> Date: 1793
> **:** the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company <industrial espionage>[1]

Often associated with classified information, governments, intelligence and counterintelligence agencies, espionage is often considered a funny word for those involved in business sector information security. Is there a connection? Given the fact information security professionals are responsible for securing information, while those involved in espionage are focused on obtaining information, I would argue there is. Unfortunately this connection between espionage and the business world is either overlooked by statements of "Who would want to target my company?" or attributed to mischievous "hackers" who are only doing it for the challenge and fun. If this is what those involved in information security in the business world think about espionage, they may be in for a surprise. Hopefully not one brought on by the folding of their company.

Those involved in espionage are in it for a reason. Either to advance the economy of a foreign country or to provide a customer, more than likely a competitor, with information regarding the latest product, customer or price lists, research, etc, of a business or government entity. Regardless of what type of information is being sought, it will normally provide the end user with some type of edge either in the dog eat dog world of big business or in foreign relations. Sure, in the early days of the Internet, spies, both industrial and foreign, may have used hacking techniques to obtain access to information. However, just as castle walls and moats could not stop determined invading armies, today's more effective perimeter defenses such as firewalls, routers, and proxy servers, will not stop those who truly want access to government or corporate information. Given today's high-technology environment and complex networked systems, our ability to gather and process information is unprecedented. Just as we benefit from these advances, so can our enemies and competitors.

The Environment

Long gone are the days when reports had to be transmitted by wireless or courier. With the explosion of the Internet from a strictly academic and military tool into the "information highway", the way we gather and process information has radically changed forever. From a simple closed network community, we are now intimately connected to a worldwide maze of networks. This complex environment is a double-edged sword though. Because of technological

[1] Merriam-Webster Collegiate Dictionary.

© SANS Institute 2000 - 2005 Author retains full rights.

advances, the traditional role of the spy in gathering and communicating information has been altered forever.

Formerly, the collection of information for the purposes of conducting espionage required a great deal of risk. Either hard paper copies had to be physically removed, or a device such as a camera had to be smuggled in to record the information. If sensitive data was even stored electronically, it was normally limited to one stand-alone computer of limited storage capacity that may or not have been connected to a noisy dot matrix printer. Finally, if there was a removable storage medium, it was most likely a five and a quarter inch sized limited storage capacity floppy disk, not the easiest item to hide.

Today, within the same office, each individual processes information using multiple networks from their own desks. One of the networks probably has access to sensitive, confidential, and/or classified information. The average internal storage capacity of each individual computer has increased significantly over those computer hard drives used ten years ago. On the other hand, the physical size of removable media continues to decrease while the storage capacity of these media increases.

Technology and the "Insider"

The information age, with its high-speed computers, communications lines, portability, connectivity, mobility, and advances in application software, can significantly increase the effectiveness of an "insider", while reducing the chances they will be discovered. More importantly, just as we have realized great efficiencies, the network environment allows an "insider" to be very effective and efficient as well. The amount of data processed and transmitted over today's computer systems can provide potential spies with access to vast amounts of data in a very short period of time. Additionally, the miniaturization of data storage devices, increased storage capacity of some storage media, and highly connected networks allow a potential "spy" to easily remove and transfer information from storage areas.

As offices become more and more reliant upon computers for processing and presenting classified information, the call came for the capability to transfer and store greater amounts of data than could be done on a standard floppy diskette. This need resulted in the development of early tape back-up systems capable of storing between 100 and 200 megabytes per storage cartridge. Although early tape back-up systems only held between 100 and 200 megabytes of data per cartridge, today's portable systems are capable of storing 20 gigabytes or more of data on one cartridge which is sometimes greater than the hard-drive storage capacity on many computer systems and servers.

Taking this one step further, to accommodate the increase in the use of notebook computers, the notebook computer industry developed hard-card storage systems that fit into PCMCIA slots in both notebook and desktop computer systems. No larger than a credit card, hard-cards are easy to conceal and they can hold up to approximately 8-gigabytes of data, equating to the entire hard drive contents of many average office desktop computer systems used today. Though not as easily hidden as the hard-cards, the built-in USB and IEEE1394 interfaces standard on many new

© SANS Institute 2000 - 2005 Author retains full rights.

computers today can allow anyone with access to a system to easily connect hard drives, CD-Rs and CD-RWs. Data can then be stored on easy to conceal CD-ROMs or external hard drives capable of holding up to 60-gigabytes of data.

Although data encryption can allow an individual to maintain privacy when transmitting data through the Internet or other systems, it poses a problem for security personnel who may be trying to determine if someone may or may not be involved in stealing company information. With the proliferation of Internet connectivity, someone could easily encrypt and transmit sensitive information over a system from their office, home, or a public computer system. With the complexity of today's public encryption systems, security officials and/or investigators would not only have a hard time identifying the data but also trying to break the code to see if it was actually sensitive company material.

On the other hand, since encryption schemes tend to follow well-defined formats it is not that difficult to spot encrypted emails. Steganography attempts to overcome this vulnerability by hiding the fact that an encrypted message or file even exists. In order to eliminate any suspicion, messages and files are hidden in other harmless messages and files such as image, audio and/or video files. To make matters in more difficult, the hidden message can be encrypted for additional security. So even if such a message or file were found, security officials would again be faced the daunting task of unencrypting suspicious items in order to determine what is was.

Friend or Foe?

In order for information to be of any value it must be accessible, at the right place, time, and by the right people. This statement is the bane of the information security professional. How so you ask? Accessible information should always be considered at risk since anyone with access poses a potential threat and any information that is accessible can be exposed, manipulated, damaged or destroyed.

Although many attempts have been made to determine the causes or indicators of espionage activity, each one attempts to focus on personal traits and characteristics as the contributing factor resulting in espionage activity. Unfortunately, these studies fail to identify the two common elements involved in every incidence of espionage; betrayal of trust and access to information. Betrayal of trust is driven by personality and as the Hanson espionage case highlights, the information security arena has only realized limited success in identifying or controlling the factors resulting in or contributing to such a betrayal. Regardless of the cause, the greatest damage is and will continue to be caused by "insiders" (someone with access to the information).

Many of the studies available today on the "insider" threat tend to focus primarily on those responsible for maintaining information systems. Unfortunately, they often overlook the fact that anyone with access to information can pose an "insider" threat. For example, in credit card skimming scams, anyone with access to your credit card such as waiters and store clerks can use a publicly available magnetic card reader to obtain and store your credit card information. This information can then be exploited to make online purchases, used to create duplicate credit cards,

© SANS Institute 2000 - 2005 Author retains full rights.

or outright sold to another person.

Additionally, though normally considered an "outsider," temporary hires, outsourcing, and contractors are integral components in today's business model. The rotation of personnel for many of these personnel, particularly in the information technology arena, can be very fluid, and the practice of subcontracting to another corporation, even one employing foreign nationals, is a routine practice. For instance, it was discovered in mid 1999 that Indian nationals, illegally present in the U.S., were actively writing software for the U.S. Air Force Personnel Center at Randolph Air Force Base, Texas. Although there was no indication the Indian nationals were writing malicious code or exploiting any of the information they had access to, this example highlights how the line between "insider" and "outsider" is rapidly blurring.

Countering the Threat

Access has always been key when it comes to identifying individuals to recruit as spies. Today's typical workplace environment has actually made this task far easier for Intelligence Services, business competitors, and other hostile groups targeting businesses and groups. Yes, believe it or not, in the post cold war environment foreign governments are actually targeting the U.S. companies in order to advance their own industries and economies. Networked computers with both confidential and openly available information have become the norm in the modern offices. Ten years ago, a typical employee may have had access to one or two safes or filing cabinets that contained vital information. Today, that same employee can have access to virtual file drawers of vast amounts of highly sensitive and confidential information via computer terminals that resides on his or her desk.

Fortunately, unlike the personality driven betrayal of trust element where we have only limited control, we can fully control and manage access to information. Companies have and continue to make significant investments in an infrastructure to protect their vital networks and information from "outsider" threats. Even though the "outsider" poses a threat to the critical information and resources of businesses, it is the "insider" who can and will cause the greatest damage. Given this information, processes and procedures must be designed based on the "Principle of Least Privilege" in order to deter, detect, and identify suspicious or anomalous "insider" activity on internal networks.

Restrict user read/write access to only those files actually needed for their jobs. In some instances this may mean restricting a user to only have access to what is on their own hard drive. However, this is a time consuming process that can easily overwhelm even the most experienced system administrators. As such, it is much easier to grant group access to files than individual access. The problem with this concept is that the branch secretary making $25,000.00 a year may now have access to propriety research data, or a database of customer credit card numbers both worth millions of dollars. Why would you want a secretary or any other employee who does not have a need know to be able to research any of the drives on the network from his or her desktop computer system?

Remove all the extraneous equipment from your desktop systems to include floppy drives. Most

© SANS Institute 2000 - 2005 Author retains full rights.

computers today come with a multitude of added extras ranging from built in modems, tape backup drives, universal serial bus and IEEE 1394 "firewire" interfaces as standard equipment. Some even come with CD-Rs and/or CD-RWs. Most typical computer users do not use these added extras and many could not even tell you what some of the items are. The problem is that "insiders" can use these added items to enhance there gathering capabilities. For example, an IEEE 1394 external hard drive with a 60-gigabyte storage capacity can be purchased for under $300.00. In a matter of hours, a trusted employee could easily download the entire contents contained on the servers of a small enterprise in a unit the size of a small computer book. To make matters even worse, a friend of mine recently showed me USB flash drive on a key chain that holds 1-gigabyte of data. Most guards would not even give it a second look, would you?

Tightly control notebook computers and their access to databases containing critical information. Unfortunately, our society loves mobile computing. These systems pose multiple problems. First, they come with all the bells and whistles contained on most desktop systems, and it is difficult to remove them from notebook systems. Next, they can hold significant amounts of vital information, be easily lost or stolen, and often are connected to systems outside of an enterprise's layered defensive mechanisms. Lastly, the proliferation of notebook computers has resulted in their wide acceptance in the workplace. Most people do not even give them a second glance, if they notice them at all.

Last but definitely not least, after spending vast amounts of money securing the perimeter of your information systems, it is time to spend more time and resources devoted to what research has shown to be the greatest threat to your information and systems – the "insider." Unfortunately, information security personnel and policies were not able to keep up with the rapid integration of computer and information systems into government and business processes. As a result, the monitoring of activity on computer systems and implementation of security procedures did not keep up with the change. Although efforts are being made to deploy automated monitoring systems designed to detect outside penetration of systems, this systems are still not fully developed and sadly efforts are just now being made to field systems designed to track the activity of "authorized" users.

This list of items is not all-inclusive, nor does it or could it ever replace the need to have good security policy or layered defenses. It does, however, attempt to make information security professionals understand that they can and should control access to information deemed to be vital to governments and businesses. The best method to do so is to use the "Principle of Least Privilege," in order to overcome the vulnerabilities brought on by convenience and the "insider" threat, thereby reducing the risk to information and information systems.

Recommendations

The information security community must remain responsive and flexible in order to overcome the many challenges the information age will pose to its efforts to deter, detect, and neutralize the espionage threat. To start with, "insider" indicator lists must be updated to reflect such activities as extensive use of encryption software, extensive data surfing on databases with access to critical information, and the downloading of files not responsive to a person's area of

© SANS Institute 2000 - 2005 Author retains full rights.

responsibility. Similar computer virus infections on systems authorized to access sensitive information and those without access to such information in the same or closely located work areas may be indicative of unauthorized data or file swapping between the computer systems. Likewise, extensive file uploads and a corresponding ratio of file downloads between systems with different levels of access may also be indicative behavior of espionage. Finally, discrepancies in the diskette and cartridge inventories may reflect suspicious activity. Again, though far from complete, this list only attempts to show the need to reevaluate the current indicators of illicit activity as technology leads to more exploitable capabilities.

In keeping with some of the new indicators, the government and business sector must develop and deploy monitoring systems capable of tracking the use of encryption software for emails, and develop a system that will identify the use of steganography without having to manually dissect every up- and down loaded file. In the software development department, agencies should look into using built in machine specific watermarking systems to surreptitiously mark and track the origins and disposition of proprietary files and documents. Finally, entities must decide whether they should attempt to fully protect all of their sensitive information documents from disclosure (risk avoidance) or only implement security measures, which provide a comfortable level of security (risk management). If they accept risk management in order to reduce costs, then they need to understand they are accepting the fact they will probably have "insider" incidents regardless of the effectiveness of their information security program.

Conclusion

Human espionage is an ancient art; in fact, it has even been called the oldest profession.[2] Unfortunately, espionage is still alive and well in today's post Cold War environment. If anything, it is even more rampant. Events in the news remind us of this, such as the recent arrests of two Lucent Technologies employees, and a catering employee of MasterCard International for the theft of trade secrets. Throughout history and in current times efforts to identify indicators of espionage have been made. Unfortunately these efforts have met with limited success. In every instance of espionage, the person involved had access to information. Understanding this, and the fact we have the ability to control access to computer file systems, is critical to protecting information.

[2] Colonel John Prout.

© SANS Institute 2000 - 2005 Author retains full rights.

References:

Boston, Terry. "The Insider Threat." 24 October 2000. URL: http://www.sans.org/infosecFAQ/securitybasics/insider_threat2.htm (12 July 2001).

Cole, Eric. Unpublished lectures for SANS Security Essentials Course, conducted at the SANS 2001 conference in Baltimore, Maryland.

Easwaran, Ashok. "INS Arrests 40 Programmers at Air Force Base in Texas." India Abroad. 28 January 2000. URL: http://www.indiaabroadonline.com/PublicAccess/ia012800/Immigration/INSArrests40Programmers.html (12 July 2001).

Fischer, Lynn F. "Espionage by the Numbers: A Statistical Data Base." URL: http://www.cta.doe.gov/C/Security_Guide/Treason/Numbers.htm#Espionage by the Numbers (11 July 2001).

Heuer, Richards, J. Jr. "The Insider Espionage Threat." URL: http://www.smdc.army.mil/SecurityGuide/Treason/Insider.htm (12 July 2001).

Krimkowitz, Harry. "Mitigating Risks to the Insider Threat within your Organization." 24 October 2000. URL: http://www.sans.org/infosecFAQ/securitybasics/insider_threat.htm (12 July 2001).

Lowry, Tom. "Technology Aids Credit Card Theft." USA Today. 23 November 1999. URL: http://www.usatoday.com/life/cyber/tech/review/crg138.htm (11 July 2001).

"Merriam-Webster Collegiate Dictionary." URL: http://www.m-w.com/cgi-bin/dictionary (10 July 2001).

National Counterintelligence Center Summary. "Hidden in Plain Sight-Steganography." Counterintelligence News and Developments Volume 2. June 1998. URL: http://www.nacic.gov/cind/1998/jun98.htm#rtoc4 (10 July 2001).

Post, Jerrold M., Ruby, Keven G., and Shaw, Eric D. "The insider threat to Information Systems." URL: http://www.smdc.army.mil/SecurityGuide/Treason/Infosys.htm (12 July 2001).

Prout, John. Unpublished lectures on Principles and Practice of Counterintelligence, conducted at the Joint Military Intelligence College for the 1998-99 academic year.

The Counterintelligence News & Developments Newsletter. "Food Worker Arrested in Attempted Theft of a $Billion Trade Secret." Counterintelligence News and Developments Volume 2. June 2001. URL: http://www.nacic.gov/cind/2001/jun01.html#a6 (13 July 2001).

The Counterintelligence News & Developments Newsletter. "Former Cisco Engineer Pleads Guilty." Counterintelligence News and Developments Volume 2. June 2001. URL:

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.nacic.gov/cind/2001/jun01.html#a7 (13 July 2001).

The Counterintelligence News & Developments Newsletter. "More Theft of Trade Secrets." Counterintelligence News and Developments Volume 2. June 2001. URL: http://www.nacic.gov/cind/2001/jun01.html#a5 (13 July 2001).

The Counterintelligence News & Developments Newsletter. "Recent Arrests Alleging Trade Secret Theft." Counterintelligence News and Developments Volume 2. June 2001. URL: http://www.nacic.gov/cind/2001/jun01.html#a4 (13 July 2001).

© SANS Institute 2000 - 2005, Author retains full rights.