Global Information Assurance Certification Paper

Mitigating Risks to the Insider Threat within your Organization
Harry Krimkowitz
October 24, 2000

At a regional headquarters of an international energy company, a MIS contractor effectively captures and closes off the UNIX based telephonic switching system for the entire complex. Subsequent investigation uncovers that the contractor had been notified a week earlier that he was being terminated. Further investigation reveals that the employee has two prior felony convictions.

As this case shows, malicious actions on the part of insiders within your organization can have very serious consequences. Today when most everyone focuses on the threat your network from external sources such as hackers, crackers and malicious code, in reality, you are much more likely to suffer compromise of your network or loss of proprietary information by people inside your own organization. Insiders continue to pose a more serious risk then outsiders. Security breaches such as electronic sabotage, equipment theft, theft of corporate resources and access abuses are ever increasing. According to the Computer Security Institute/FBI and Ernst and Young, nearly 50% of all network attacks come from the inside, often from unhappy workers. In fact in Survey 2000 conducted by ICSA, at least half of all respondents experienced insider security breaches related to unauthorized installation of computing tools, misuse of company resources and abuse of access controls. This confirms that the insider threat represents at least as much risk as to corporate assets as external crackers and virus writers.

So, what actions can you take to mitigate the risk from loss to your organization from the insider threat?

The Insider and the Threat

Before we look at the recommended actions for mitigating risk to the insider threat, let us identify who the insider is. Although all employees in your organization potentially are a threat for computer security breaches, organizations should focus on the information technology specialist. These personnel design, maintain or manage critical information systems. They are of primary concern in your efforts to mitigate the risks to the insider threat because they are the personnel who usually hold the keys to your information kingdom. They also possess the necessary skills and access to engage in serious abuse or harm to your information systems. These information technology specialists may be regular full-time or part-time staff employees, contractors, consultants or even temporary workers. Remember that a well-placed insider can pinpoint key data quickly and that none of the operating systems used in organizations today are immune to root compromise from an existing user account.

Now that we have defined who the insider is and established the fact that your insider can pinpoint the critical information within your organization with which to perform malicious acts, what are the prudent steps that your organization can take to mitigate the risk of this threat?

Risk Mitigation steps to the Insider Threat

Each company should start their risk mitigation process against the insider threat by seriously looking at their hiring processes and procedures. I would highly recommend that a company take a serious look at paying the price to conduct some type of pre-employment screening/background checks on their prospective employees before they make an offer to hire. Although this may be a challenge in our tight labor market, there are companies that can perform these background checks very quickly. If you cannot perform background checks on all your potential hires, ensure that you do this at a minimum for your information technology specialists.

The next, thing that your organization should do is to set a structured coordinated effort with the HR, and IT departments within your organization for new personnel in-processing and for personnel out-processing. I believe that organizations don't combine in a comprehensive way, information security and physical security. For example, one of the major reasons for physical theft is the lack of asset control. With PCs, peripherals, external drives and so on so easy to acquire, companies in many cases do not know what has been acquired and as a result, asset tags are never attached to devices. Physical inventories of assets are rarely conducted and as employees come and go, or move from department to department, these small devices just get lost in the shuffle. This coordinated and structured effort must be established in the initial in processing of each individual into your organization. Your HR Department should ensure that each new employee receive:

- A briefing on the computer security policies within the organization
- An indoctrination on security awareness

Of course, everything with respect to computer security starts with your organization's security policy. By having established policies and ensuring that all employees are aware of the consequences for failure to comply with these established policies will go a long way in mitigating some of your insider risk.

Also, it would be prudent that each individual have their access privileges and or limits established by their immediate supervisor/manager and that these privileges be verified with the supervisor/manager by the system administrators prior the end of the employee's first day.

I also believe that each new employee should be required to sign a proper receipt for the equipment that they will operate and maintain.

Finally, all users should be required to sign an acceptable use policy stating that they are responsible for protecting information used or stored in their accounts.

My reasoning for the measures detailed above are because, I believe that the most common management errors/ommissions when it comes to computer security lapses are: failure to have clear standardized rules governing the use of information systems with explicit consequences for misuse and failure to punish rule violators.

As for employee out-processing, it is essential that all user accounts be terminated before the employee's last day. The number of cases that separated employees have returned to extract revenge on their former employers indicates a need for improved management of the termination process. Policy and procedures should be in place to define the steps that must be taken by HR, IT support and Security to provide prompt notification of changes in the status of your personnel.

Some Additional Actions

Organizations should require that their personnel use password protected screen savers that activate after 15 minutes or less of idle time because this can help to reduce the opportunities for unauthorized access to unattended terminals

Use of file encryption to protect your company's sensitive files stored on servers is another approach to effectively manage at-risk employees.

Also, it may be wise to install programs that monitor your employee's at-work electronic communications. However, it would be wise to consult with your legal consul before initiating any type of monitoring activities

Your security policy should only allow software to be installed by authorized members of the IT staff.

Finally, you should require system administrators to perform comprehensive information security audits. You should require that audit logs be stored and reviewed at least weekly. Of course, you must allocate your system administrators sufficient time and resources to adequately review these logs.

All of the above actions are focused on the insider threat. This list is not intended to be inclusive but to highlight those actions that I believe to be the most beneficial against this threat. Understand that your organization must also deploy other standard protective measures such as firewalls and intrusion detection systems. Companies with layered defenses detect a far greater number of both insider and outsider breaches.

Conclusion

A major factor in the rise in corporate computer fraud and computer crime is the fact that most companies have failed to establish sufficient security policies, procedures and controls on their computer systems. In addition, because of down sizing, process re-engineering and other efficiency moves, internal controls may not be adequate to deter insider abuse. Disgruntled employees and other insiders pose a tremendous threat to companies and organizations. These individuals usually know what controls are in place, and may have the ability to circumvent these controls or exploit weaknesses found in applications, systems and networks. Your information technology specialists will definitely possess the requisite skills. Only by adapting a comprehensive approach to applying technological and human factors to information security can an organization adequately protect itself from both the outside threat and the inside threat. If your organization takes to heart and effectively implements the actions delineated above, you will at least have taken prudent steps to mitigate the risk of computer security breaches from your employees. In short, when it comes to mitigating insider risk it pays to sweat the small stuff.

Sources

Berst, Jesse. "The Biggest Threat to Your Network's Security. (It Isn't What You think)". April 7,1998. URL: http://www.zdnet.com/anchordesk/story/story_1959.html.

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.

"Security Focus 2000", Information Security Magazine, September 2000.

Para-Protect, Monthly Checklist for May 2000, "Protecting Your Company from a Bad Insider". URL: http://www.para-protect.com/monthly-checklist/May2000_checklist.html

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor