Cybersecurity – The Insider Threat

Student Guide

August 2017

Center for Development of Security Excellence

Introduction

Our adversaries quickly share new tools and tactics within their circles, leveraging threats within the world of cybersecurity. It is difficult to detect, defend, and remediate these threats since they can involve a combination of ways, including human behavior and the use of hardware and software technologies.

Often, cybersecurity attacks are posed by an action or failure of an insider. This session covers how to recognize and mitigate the most common cybersecurity attacks from the witting and unwitting insider.

Welcome to CDSE's Short on cybersecurity attacks conducted by witting and unwitting insiders and the ways to mitigate them.

Types of Insiders

While cybersecurity attacks can and do come from the outside, human behavior from insiders is often the cause. These insiders can act maliciously with intent or inadvertently.

The witting entity is an insider that operates with intent, seeking the use of cybersecurity tools and methods as a means of compromise.

The unwitting entity can adversely compromise an environment using cyber technology through carelessness or being tricked into doing something on behalf of the attacker.

A type of witting entity, a malicious insider can be an internal employee or contractor—either a criminal agent or a disgruntled worker—who deliberately compromises or breaches data or systems with the intent of harm. Malicious insiders account for the lowest percentage of internal incidents, yet they are the most costly. They are also the most difficult type of insider to detect, as these persons may have an awareness regarding organizational security practices.

One type of unwitting entity is the careless insider. The careless insider can be an employee or contractor who makes a mistake with data in the course of simply trying to do his or her job. Examples could include having a laptop stolen, using a personal email account, sharing files using dropbox, lack of password management, clicking on malicious email links, or connecting unauthorized devices.

Another type of unwitting entity is the victim insider. Victim insiders are often high-value employees—such as system administrators, IT help desk teams, and executives—who are deliberately targeted and exploited by outsiders trying to gain access.

Attacks from Malicious Insiders

The types of attacks launched by the witting and unwitting entities are varied. We'll examine several examples.

Malicious code is any code in any part of a software system or script that is intended to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. Malicious code can be developed and transmitted by outsiders as well as malicious insiders, often criminal agents or disgruntled employees.

Malicious code has the ability to copy itself and can be spread through executable file sharing or transfer on USB thumb drives, file transfers through a file sharing protocol, malicious URLs, instant messenger, or email attachments, as examples. Malicious code is often combined and spread with other cyberattacks including phishing and social engineering.

There are several common types of malicious code attacks perpetrated by malicious insiders:

- **Backdoors** which allow an attacker to remotely access compromised computers.
- **Trojans** which are downloaded through opening email attachments or via internet links.
- **Viruses** which propagate by infecting existing files on infected computers.
- **Worms** can replicate on infected computers or removable devices.

Several factors contribute to malicious insiders and their use of malicious code:

- **Human behavior.** Malicious insiders are adept at reading and exploiting human tendencies, such as carelessness and curiosity. Despite warnings and even suspicion, users do not take proper care and heed security warnings. Malicious insiders take advantage of this human behavior in their co-workers.
- **Financial gain.** Malicious insiders are often motivated financially with the intent to sell breached data on the dark web.

Attacks from Careless Insiders

Password cracking is the process or application used for guessing or recovering an unknown or forgotten password from stored locations or from a data transmission system.

Password cracking is an attack engaged by a malicious insider or outsider to take advantage of an insider's carelessness. By using passwords that are easy to crack, the careless insider creates a vulnerability that malicious insiders or outsiders can exploit. Password cracking is the process or application used for guessing or recovering an unknown or forgotten password from stored locations or from a data transmission system.

To identify passwords and use them maliciously, password crackers use techniques such as:

- **Dictionary Cracking** by trying possibilities based on words in the dictionary,
- **Rainbow Tables** or precomputed tables for reversing cryptographic hash functions, and
- **Brute Force** where a computer tries every possible password until it is successful.

The time it takes to crack a password is dramatically influenced by the number and type of characters. It only takes a hacker 5 hours to crack an 8-character password comprised only of alphabetic letters. The time changes exponentially by expanding the password—even with only alphabetic letters—to 12 characters. Longer passwords with alphanumerics, mix of capitalization, characters, and symbols are best.

A variety of careless insider habits make password cracking easier for malicious insiders and outsiders:

- Using passwords that are easily guessed, such as:
  - Names, special dates, or dictionary words.
  - Passwords that are too short.
  - Passwords that use all lower case or all upper-case letters with no special numbers, characters or symbols.
- Writing a password on a paper left in plain view. It seems obvious, but people have a hard time remembering complex passwords. They write them down exposing them to insider threats. If writing a password down is the only way to remember it, keep the reminder out of sight and locked.
- Re-using a previously used password or using the same password for multiple systems. Every time a password is changed, it should be changed to something new. Recycling an old password or using the same password across systems creates vulnerability for password crackers to exploit.

Attacks from Victim Insiders

Phishing is the practice of sending emails or malicious links, supposedly from reputable sources, to induce individuals to reveal sensitive information, such as passwords and credit card numbers. It is a technique employed by malicious insiders or outsiders to exploit victim insiders. Phishing attacks usually involve a lure, such as the portrayal of a popular or well-respected third party, with a specific request to provide sensitive information. The receiver is lured by the trustworthiness of the third party.

Imagine that you receive the following email from support@technology.net:

> We would like to inform you that we are currently conducting scheduled maintenance on behalf of your IT department. Your account must be upgraded. To maintain your account, you must reply to this email and provide your user name and password. Failure to provide this information within 72 hours will result in deactivation.

In this scenario, two lures are used. The first is the reference to an email address that appears valid. It is a common phishing lure that takes advantage of careless and victim insiders. The second is the alignment with IT. This lure makes the email seem more trustworthy and is a common lure. The timeframe indicator adds urgency to the message, and the notion that maintenance has been scheduled lends validity. However, these two references are not lures.

Several factors contribute to phishing attacks that take advantage of victim insiders:

- **Lack of knowledge about how operating systems, applications, email, and the web work.** As examples, users may not be equipped to identify fraudulent URLs or to distinguish between forged and legitimate email headers, how to verify security indicators, or how to verify SSL certificates.
- **Visual deception.** Phishers often change one letter in the syntax of a standard domain, copy legitimate images that hyperlink to rogue sites, and mimic the look of browser windows to visually deceive a user.
- **Limited attention.** For users, security is often a secondary consideration, which leads to overlooking security indicators and warning messages.

Attacks from Malicious, Careless, and Victim Insiders

Social engineering is the act of tricking people into divulging confidential information and/or breaking normal security procedures. It is often used by outsiders or malicious insiders to identify and subsequently exploit careless and victim insiders.

The key to social engineering is the trickery. Attackers research information about their targets and use that information against them. They often exploit the target's social networks or already breached data to propagate malicious code or convince the target to divulge sensitive information, but it can also be initiated with voice (vishing), in person (impersonation), and text messaging (smishing).

Social engineering can also be used to confuse the careless or victim insider. Consider this example:

> Robin Sage had various social media profiles that claim she is 25-year-old cyber threat analyst at the Naval Network Warfare Command in Norfolk, VA. These sites further indicated that she graduated from MIT and has 10 years' work experience. The problem was that Robin Sage did not exist. The profiles were fictitious, created by criminal outsiders trying to take advantage of unwitting insiders. In this example, victim insiders sought Sage's opinion on important matters and even wasted hours attempting to hire Sage, who never existed.

Several factors can contribute to social engineering attacks from malicious outsiders or insiders that take advantage of careless and victim insiders:

- Making personal information readily available through social media sites such as Facebook, LinkedIn, and Twitter.
- Failing to independently verify requests that seem unusual when they appear to come from someone the target knows.
- Failing to confirm information publicized in social media profiles.
- Big data breaches that make customer data available to attackers on the dark web.

Non-technical Mitigation Methods

The ways that we mitigate cybersecurity attacks from the witting and unwitting insiders can apply to both non-technical and technical methods. We'll begin by exploring the non-technical methods.

There are four common non-technical methods for mitigating cybersecurity attacks from malicious, careless, and victim insiders: limiting the information made available on social media, limiting privilege to systems and data, implementing policies for mitigating cybersecurity attacks from insiders, and conducting training to improve knowledge and skill related to vulnerabilities and how to mitigate them.

For social media limitations, encourage employees to limit the amount or type of information about themselves made available publicly on social media. This technique reduces the information that malicious outsiders can leverage against victim insiders.

For limiting privilege, establish an access control policy that authorizes specific users to particular information and information systems. Authorizations can include system accounts, temporary accounts, general user accounts, two-person controls, and privileged user accounts, as examples. This technique reduces vulnerabilities with malicious, careless, and victim insiders by reducing the number of users who have access to systems and data.

For policy, clear, comprehensive policies and associated responsibilities and actions must be in place for mitigating cybersecurity attacks from insiders. Policies must be approved by senior management, and penalties must be clearly defined, included in training, and signed by all employees. This technique reduces vulnerabilities with malicious, careless, and victim insiders.

For training, develop and deploy effective security awareness training. There are required elements to security awareness, for DoD and Industry. Updating and reinforcing awareness training is necessary to keep pace and ensure people are equipped to identify and mitigate cybersecurity attacks from within, given their growing severity, prevalence, and complexity. This technique reduces vulnerabilities with malicious, careless, and victim insiders.

Technical Mitigation Methods

In addition to the non-technical methods, technical actions can also mitigate cybersecurity attacks from all three types of insiders—malicious, careless, and victim. There are four common technical methods for mitigating cybersecurity attacks: email filtering, host based security controls, outbound filtering, and antivirus updates and patches:

- Implement email filtering, or the organization of emails per specific criteria performed by software, such as spam filters, or by users who generate rules to pass emails to designated folders. This technique reduces vulnerabilities with malicious, careless, and victim insiders.

- Implement host based security controls, or software used to monitor, detect, and defend networks and systems through solutions such as firewalls and desktop intrusion prevention systems. This technique reduces vulnerabilities with malicious, careless, and victim insiders.
- Implement outbound filtering, or monitoring and potentially restricting the flow of information to reduce risks of the witting or unwitting distribution of malicious code. This technique reduces vulnerabilities with malicious, careless, and victim insiders.
- Stay current with antivirus updates, patches, and changes that address the onslaught of new, specific cybersecurity threats. This technique reduces vulnerabilities with malicious, careless, and victim insiders.

Summary

Let's summarize some of the key points from this Short on identifying and mitigating cybersecurity attacks from witting and unwitting insiders:

- Threats from within are a big, arguably the biggest, source of cybersecurity concern and compromise.
- Human behavior, both intentional and inadvertent, complicates the threat of compromise to cybersecurity. The motivations behind insider threats to cybersecurity are as varied as humans themselves. Outside attackers know how to exploit those human vulnerabilities.
- Cybersecurity attacks can come in combinations, such as malicious code spread by social engineering or phishing.
- Cybersecurity attacks are becoming increasingly impactful, common, and complex. They change quickly. It's important to stay current with changing threats in order to recognize them.
- Keeping pace with the dynamic nature of cybersecurity attacks is also an important part of maintaining cybersecurity. Mitigation techniques must adapt.

Congratulations! You have completed CDSE's Short on cybersecurity attacks conducted by witting and unwitting insiders and the ways to mitigate them.