Repelling the Wily Insider

Ronald Woerner, CISSP

NebraskaCERT Conference 2005

What Are You Scared Of?

Session focus

- Insiders are evil
  - OK, their not really evil, they just cause the most trouble (see slide above).
- Understanding the Wily Insider
  - Non-technical (human, process, etc.)
  - Technical (software, applications, hardware)
- Defending Against the Wily Insider
  - Non-technical (human, process, etc.)
  - Technical (software, applications, hardware)

External Threats

- Threats:
  - Viruses, worms, network attacks, application-level attacks…
- Defenses are understood but not perfected
  - Firewalls, IDS/IPS, Antivirus, Web Filters…
- Objective is clear: Keep “bad guys” from getting in and/or tracking them when inside
- We can defend because we know what and where to defend:
  - Well-defined entry points!
  - We know where to place defenses
  - Engage in application security testing
  - Usually a clear distinction between good and bad

Internal Threats

- Threats exist from people, processes and applications
- Attacker (users, malicious code) is trusted and already inside the defended perimeter
- What we know about external defenses doesn't apply to the inside!
- The clueless and careless insiders bring external threats inside!
  - Infected laptop – physically or virtually
  - Clicking on an email attachment containing a virus or spyware
  - Visiting malicious web sites
  - Downloading and installing applications
  - Etc.

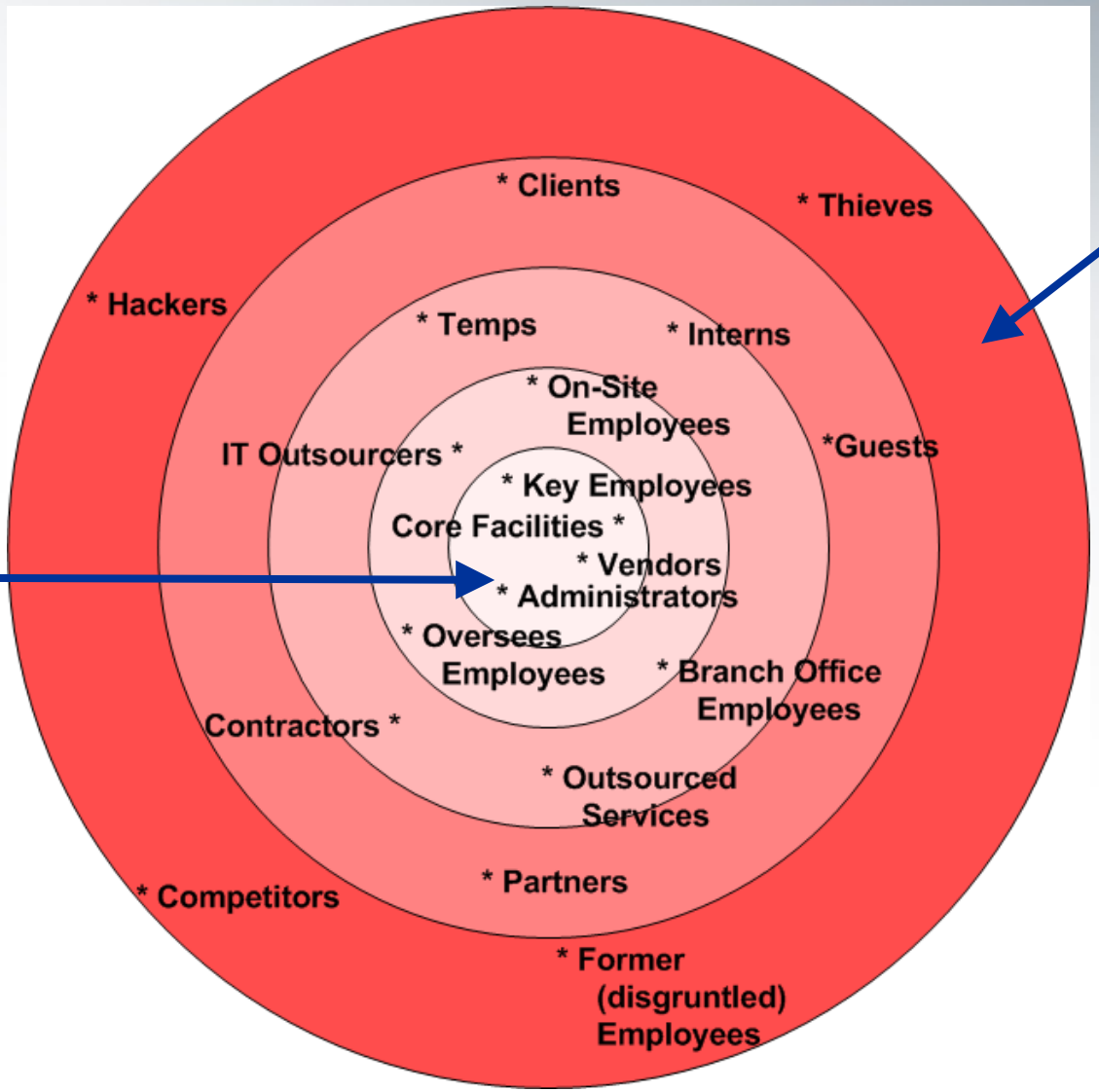
The Wily Insider

- It is estimated that 80% of computer crime is committed by insiders.[1]
- Insiders can be employees, partners, customers or even applications.
- Made possible by the extension of trust – applications, people and processes
- Insiders know what and where the crown jewels are!
- Insider damage may not be intentional (opening infected attachments, creating shares, bringing infected laptops, installing Trojan-ed programs, curiosity, etc.)
- Human error – not technical malfunction – is the most significant cause of IT security breaches in the public and private sectors.[2]

[1] Source: InterGOV http://www.intergov.org.

[2] Source: CompTIA Survey: http://www.comptia.org

The Blurry Definition of “Insider”

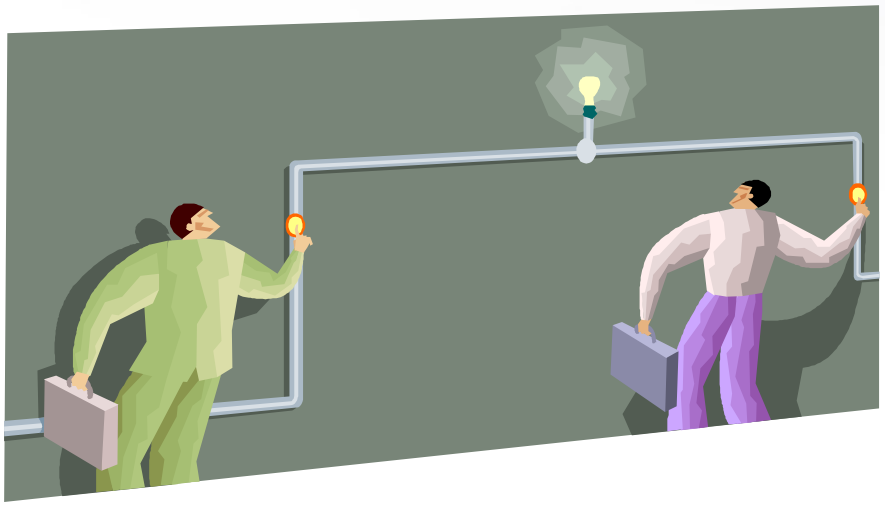


Untrusted

Most Trusted

Understanding The Wiley Insider

- People
  - Malicious (social engineering)
  - Accidents
- Process
- Technology
  - Software



Understanding Risks - People

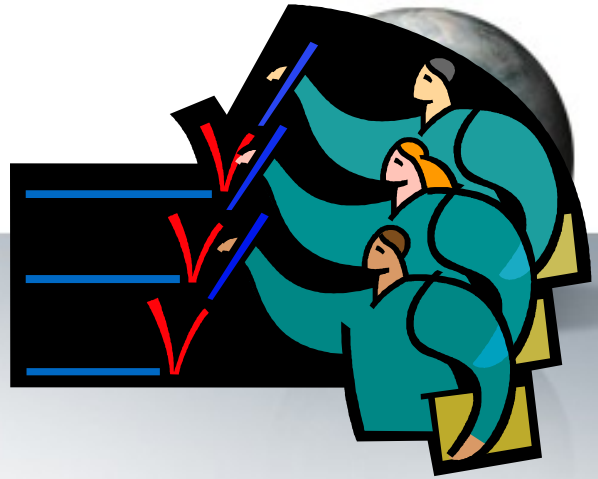
- Insiders are those individuals who work for or have a relationship with the target organization
  - Employees
  - Contractors
  - Business Partners
  - Subcontractors
  - Consultants
  - Customers

Understanding Risks - People

- The clueless/careless insider exposes company to:
  - Social engineering
  - Viruses through infected laptops
  - Stolen equipment
  - Mistakes / Accidents

- The malicious insider:
  - Theft
  - Sabotage
  - Espionage

Understanding Humans



- People will use almost any way to get what they want.
- The oldest, easiest and most prevalent method is Social Engineering.
- It is the art & science of using fraudulent methods to gain unauthorized access to an asset.
- Preys on the qualities of human nature:
  - The desire to be helpful
  - The tendency to trust people (especially insiders)
  - The fear of getting into trouble

Plausibility + Dread + Novelty = Compromise

Identity Paradox

Who am I?

How do you know?

How can I prove it to you without compromising my privacy?

Social Engineering Scenarios

- The help desk receives a request to reset a VP's password.
- A copier repairman comes to your front door insisting he be allowed to enter.
- A competitor finds your company phone book in the trash.
- An administrator calls a user requesting their password to fix an application.
- You receive an email from your bank asking you to update your personal information.

Understanding Risks - Processes

- No policies or processes in place (or policies are there, but no one follows them…)
- Mechanisms to enforce security can be used offensively:
  - High password complexity = Stickynote
  - Cached information on laptops
- Insider threat concerns not acted upon:
  - Little security testing done on intranet applications
  - Forensic logs and monitoring are not in place.
  - Centralized administration models
  - Who watches the watchers?

Understanding Risks - Software

- Malware
  - Users clicking on viruses, adware or Trojans not blocked by AV
- 3rd Party Software
  - You're organization inherits software vulnerabilities!
  - Backdoors
  - Trojans
- Internally developed applications
- Internally deployed applications

Defending Against the Wiley Insider

- Threat modeling & simulations
- Risk assessment
- Technology
- Awareness – Trust, but verify

Defenses – Threat Modeling

- What are worst case scenarios for a malicious insider at your company?
  - Intellectual Property theft
  - Sabotage
  - Exploiting company resources
  - Customer information theft
- Which people have the access to pull it off?
  - Create lists of people or roles that have the access necessary to carry out the deed.
  - Lists are useful to deploy technologies/policies and for forensics and prosecution

Defenses – Threat Simulation

- Based on modeling, act out scenarios.
- Either outsource or develop a team internally for social engineering attacks.
- Enlist employees at varying levels for staged malicious insider attacks.
- Imagine act has already occurred- logs? Contingencies?

Defenses – Technologies

- Access Controls
- Resource locking
- Host IDS
- Resource monitors
- Compartmentalization
- Principal of least privilege

Defenses – Internal Assessments

- Red-Teaming
- Test intranet, partner, customer and extranet applications for security!
- Form focused security test groups that are armed with the tools and techniques of an attacker.
  - Small group
  - Focused on internal applications as if they were externally deployed
- For intranet applications, has testing been done to ensure that user's cannot escalate their privilege?

Defenses – 3rd Party Assessments

- The cost of assessment is eclipsed by the cost of one major unauthorized access
- Independent assessments offer promise
  - Realistic, unbiased evaluations
  - Acceptance testing
  - Inexpensive compared to TCO
- Vendors:

Ernst & Young — Quality In Everything We Do

SI SECURITY INNOVATION — THE APPLICATION SECURITY COMPANY

TruSecure

IBM

Foundstone

@stake — Where Security & Business Intersect

Defenses – Training: Developing a Security-Minded Organization

- Develop and use policies and procedures
- Protect sensitive information and documents appropriately
- Be a little suspicious of unsolicited phone calls, emails or visits
  - TRUST, BUT VERIFY
- Teach personnel how to recognize signs of attack and what to do if they are a victim
- Grow employee knowledge on safe procedures and practices
  - Not just the “what to do” but also the “why”

Defenses – Training: Developing a Security-Minded Organization

- Train employees on secure practices to mitigate risks of:
  - Social engineering
  - Carelessness and its implications e.g. Infected laptop
- Training should be broadly focused – not just IT
- Training programs offered by:

CSI COMPUTER SECURITY INSTITUTE

SI SECURITYINNOVATION THE APPLICATION SECURITY COMPANY

@stake Where Security & Business Intersect®

Foundstone®

SANS

Summary

- The insider threat is very real
- Traditional security practices don't address the threat
- Most companies don't have the necessary checks and balances in place
- There IS hope!
  - Model the threat
  - Plan for contingencies
  - Add appropriate monitors, procedures and policies.
  - TEST YOUR INTERNAL PROCESSES & APPLICATIONS!!!
  - Educate

References & Resources

- FTC – Consumer information
  http://www.consumer.gov
- CERT – Home User
  http://www.cert.org/homeusers
- Get Net Wise
  http://www.getnetwise.org
- Microsoft Information Workers Security Handbook
  http://go.microsoft.com/fwlink/?LinkId=38060
- Stay Safe Online
  http://www.staysafeonline.info/

Questions?

Ron Woerner

E-mail & Web

ron.woerner@conagrafoods.com

http://www.conagrafoods.com

Telephone

1 (402) 577-3844

ConAgra Foods®