The Power of the Human Shield in Cyber Defense

David Cawley
Intuit Information Security
Introduction
Who am I?

• Senior Manager
  • Intuit Information Security Team

• Background in..
  • Security Operations
  • Business Intelligence
  • Director of Engineering
  • Education

• Find me on Twitter:
  @david_cawley
Why I’m here

• Learn from the SANS Community
  Meet with others tackling similar problems

• Share Lessons Learned
  Discuss what worked and what didn’t

• Education & Training
  To support information security education
The Challenge

To Err is Human
Threat Landscape

[Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/]
Frequent root cause - Phishing

95% “95% of all attacks on enterprise networks are the result of successful spear phishing”

Source: Allan Paller, Director of Research - SANS Institute
Human Error is often to blame

BakerHostetler Data Security Incident Response Report Shows Human Error is More Often to Blame

Findings highlight employee negligence as primary factor in majority of cases; No industry is immune; Enhanced detection capabilities critical

New York (May 7, 2015) — Human error was the number one cause of data security incidents according to a new report released today by the Privacy and Data Protection Team at BakerHostetler. In the incidents that the firm worked on last year, employee negligence was responsible 36% of the time. That was followed by theft by outsiders (22%), theft by insiders (15%), malware (16%) and phishing attacks (14%).
Developing a Human Shield

*Starts with an ownership mindset*
Mindset - “Nobody ever washes a rental car”
Awareness & Education

Security University
SECURITY UNIVERSITY
SANS Securing the Human Developer Training

Training Modules
- Injection Flaws
- Authentication
- Session Management
- Cross Site Scripting
- Insecure Direct Object Reference
- Security Misconfiguration
- Insecure Cryptographic Storage
- Insufficient Transport Layer Protection
- Missing Functional Level Access Control
- Cross Site Request Forgery
- Using Known Vulnerable Components
- Unvalidated Redirects and Forwards

[Source: SANS Securing the Human Developer]
Instructor Led Training – Threat Modeling

Attacker Profiles
AP01: Thieves
AP02: Bank Robbers
AP03: Murderers
AP04: Spies
AP05: Online Criminals

Assets
A01: Car
A02: Employees
A03: Ducks
A04: Employee Workstations
A05: Office Equipment
A06: Coffee Equipment
A07: Beer
A08: Intuit Confidential Material

Controls
C01: Car locks
C02: Badges
C03: Locked Cabinets
C04: Document Shredder
C05: Front Desk
C06: Security Personnel
C07: Laptop Locks
Human Sensors - Phishing Simulation & Reporting

23% of recipients now open phishing messages and 11% click on attachments.

[Source: VDBIR Incident Report 2015]
Measuring & Accelerating

The 30-Day Challenge
Dashboard & Metrics – Measuring Success
Gamification: 30-Day Challenge

- Pilot of SANS Securing the Human Developer
- Obtained SVP support from Engineering
- Intuit Chief Architect suggested a Challenge
- Invited 3 groups to participate (~500 people)
  - 1st Group kickoff: 6th May
  - 2nd & 3rd Groups kickoff: 9th June
- Results
  - Successful pilot with great feedback!
  - ALL levels – SVP/Director/Manager/IC
  - ALL Roles – PM/PgM/Arch/Dev/QE/Ops
  - Annual Goal for ALL Product PD teams
Acquiring security talent & technology

Data Protection

What we can accomplish together
Summary
Summary

• Don’t be afraid to get in front of executives
  • Obtain buy-in for training efforts
  • Require all training for PD teams in a tops-down way

• Teams love to compete!
  • Use fun competition to drive the right security behavior
  • Put teams up to a 30-Day challenge to accelerate training

• Leverage the SANS Community
  • Network of experts – don’t reinvent the wheel
  • Resources: Tip of the Day, Ouch Newsletter, SANS Poster Series
Q & A
Thank You!