Mock Incident Walk-through:

Oh...Pastebin, what have you done to me now?

Agenda

- A Brief Introduction
- What is ISC2?
- What is an Incident and how do I know I’m having one?
- 2013 Pastebin-Apocalypse
- Questions

A Brief Introduction

- Joe Daw - Information Security Manager for Jones Day LLP, ISC2 Chapter President
- Christopher Robinson aka CRob -Sr. Technical Account Manager for Red Hat Inc, ISC2 Education Chair
- Combined over 30 years Enterprise Engineering/Operations, Management, Strategic Planning, and Security experience

What is ISC2 and what's a CISSP?

- International Information Systems Security Certification Consortium
    - A global non-profit recognized as a leader in educating and certifying security professionals
- Certified Information Systems Security Professional

The recognized "Gold Standard" for confirming security experience and knowledge. The CISSP has worldwide recognition of competence

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY

Why should I care about “Incidents”

- Anyone can be a target. No, you’re not too small and no you don’t not have anything of value.
- 80% of all attacks in 2012 were a result of password guessing/reusing valid credentials.
- Phishing (attacks via email) are the new go-to attack vector; chances are if you have email, you’ve been phished.
- Most breaches (62%) take months or years to discover. Sadly, 70% of those breaches are reported back to you via an external entity.
- 2012 had 855 documented incidents involving

Why does security matter?

- Private customer data must be protected from unauthorized use/access (Identity Theft)
- Trade Secrets and the like must be protected from competitors (Industrial Espionage)
- Company Reputation/Brand must be protected (Character/Brand Defamation)
- Financial Transactions must be guaranteed authentic (Theft, Fraud, Money Laundering, etc.)
- Business Continuity must be ensured (Natural/Political Disasters – Hurricane Katrina, Japan's 2011 Tsunami, September 11th, 2001)
- And dozens of other reasons....

The Cyber-Incident

s

The Stages of an Incident

Identify

Containment

Eradicate

Recover

Lessons Learned

The Players

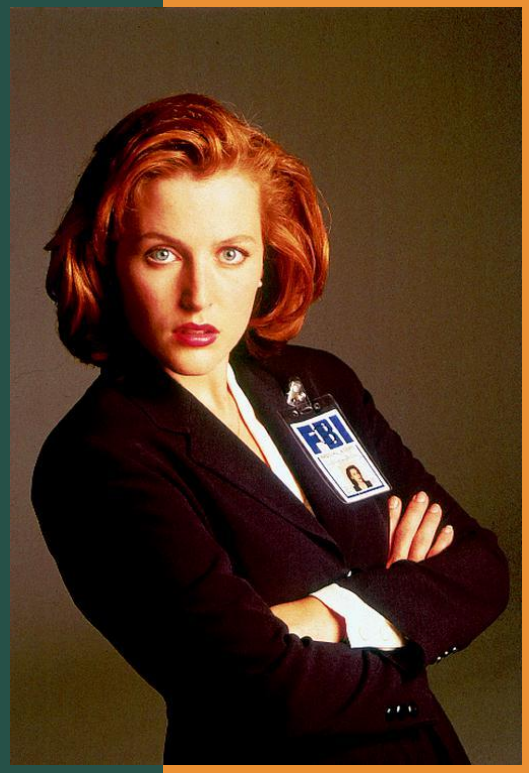
- The “Ops” Team – technologists who manage the infrastructure and implement the software that helps run the company.
- The Security Team – policy and process focused, no direct contact with impacted systems.
- Senior Management/HR – The leadership of the company, no technical skills, focused on the business.

Who are you?

- Who you are and what you do will determine how you react to incidents

Saturday 2pm – A call from the FBI

- Data from your company has been posted to pastebin
- What is your goal: eradication or prosecution?
- Who is engaged at this stage?



Saturday 6pm – A call to the helpdesk

- “Vlad” calls the helpdesk stating he will post more data unless you pay him $1mil. to his Swiss bank account.
- Helpdesk has a caller ID # and a Bank Acct #

Sunday 10am – DBA reports issue

- DBA see excessive logs from “a service ID” on “a database server”.

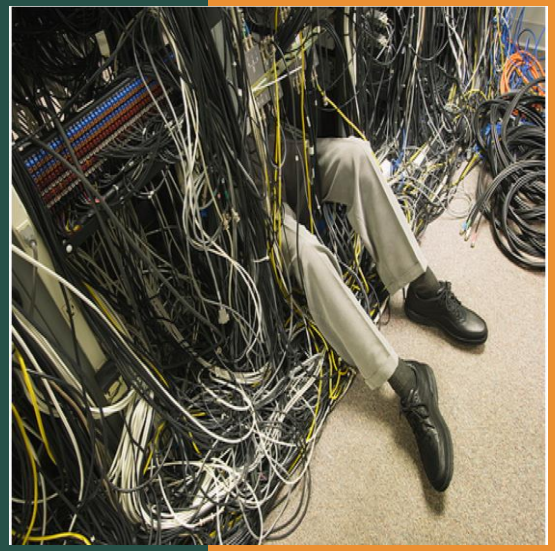
-DBA then logs off and goes to church.

Sunday 1pm – DBA back online

- Service ID is “TESTAPP10” and is active on TESTAPPDB12.
- A recent copy of Production data has been copied here for weekly build testing.

Sunday 3pm – Unknown process

- Server team discovers unknown process running as TESTSRV11 service ID



Sunday 5pm – “Ex” Employee

- Service ID found to be created by contractor who left 3 months ago.
- Password for account was never changed.
- Process TESTSRV11 is SSH’ing out Prod data from Test server.
- Prod “backup” is a well-known process internally.

Lessons Learned?

-
-

The 10 Principles of Incident Response

1.) Assign an executive responsible for the plan.

2.) Develop a taxonomy of risks, threats, potential failure modes.

3.) Develop easily accessible quick-response guides for likely scenario.

4.) Establish processes for making major decisions.

5.) Maintain relationships with key external stakeholders, such as law enforcement.

6.) Maintain SLAs and relationships with breach-remediation providers/experts.

7.) Ensure the documented response plan is available to the entire organization.

8.) Make sure staff members understand their roles and responsibilities.

9.) Identify individuals who are critical for incident response and ensure redundancy.

10.) Train, practice, and run simulated breaches.

Cleveland ISC2 Chapter

- Our Goal – To Educate, Inspire, and Entertain
  - Focused on the entire InfoSec Professional
  - We meet the last Tuesday of every* month at 5:30pm at varying locations (generally in/near Independence, Ohio)
  - Great guest speakers from Security, Business, Education and other fields.
  - Excellent peer-to-peer conversations on relevant InfoSec issues.

Visit http://www.isc2chapter-cleveland.us/ for more details!

*every month, mostly

(ISC)² SECURITY TRANSCENDS TECHNOLOGY

Questions