Information Security Offense and Defense

HIMSS Heart of America Chapter

February 2015

DepthSecurity

Information Security Professionals

Depth Security

Who we are

- Boutique Information Security Firm
- Founded in 2006
- Based in Kansas City, Missouri
- Your organization’s best friend of worst nightmare (perspective is everything)

What we do

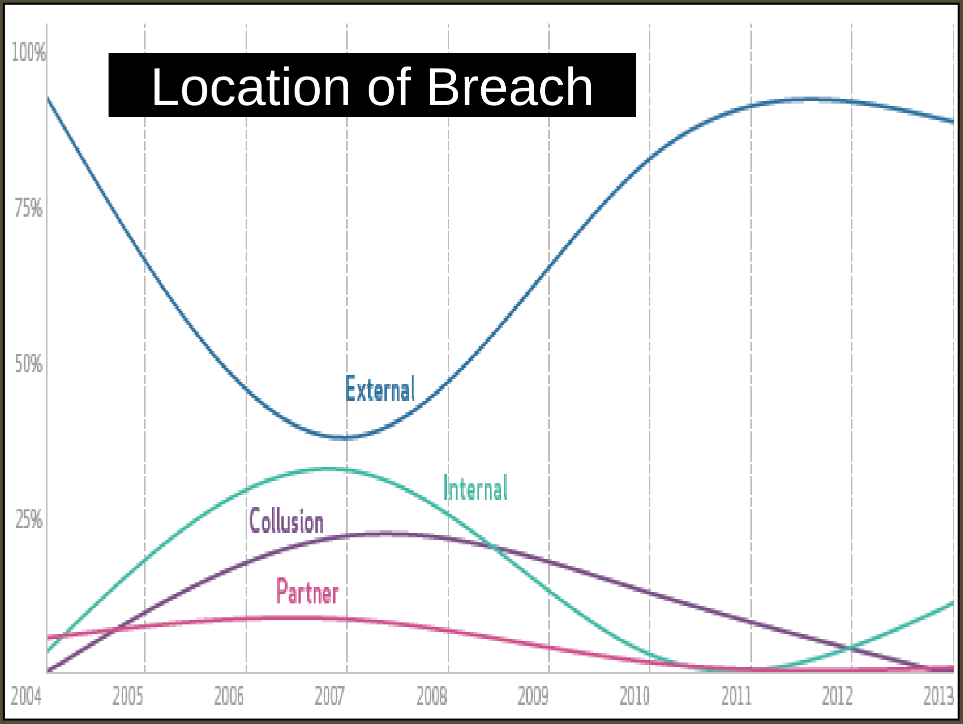
- **Offense:** Identify and exploit weaknesses in networks and applications
- **Defense:** Help defend against real-world threats utilizing services and solutions

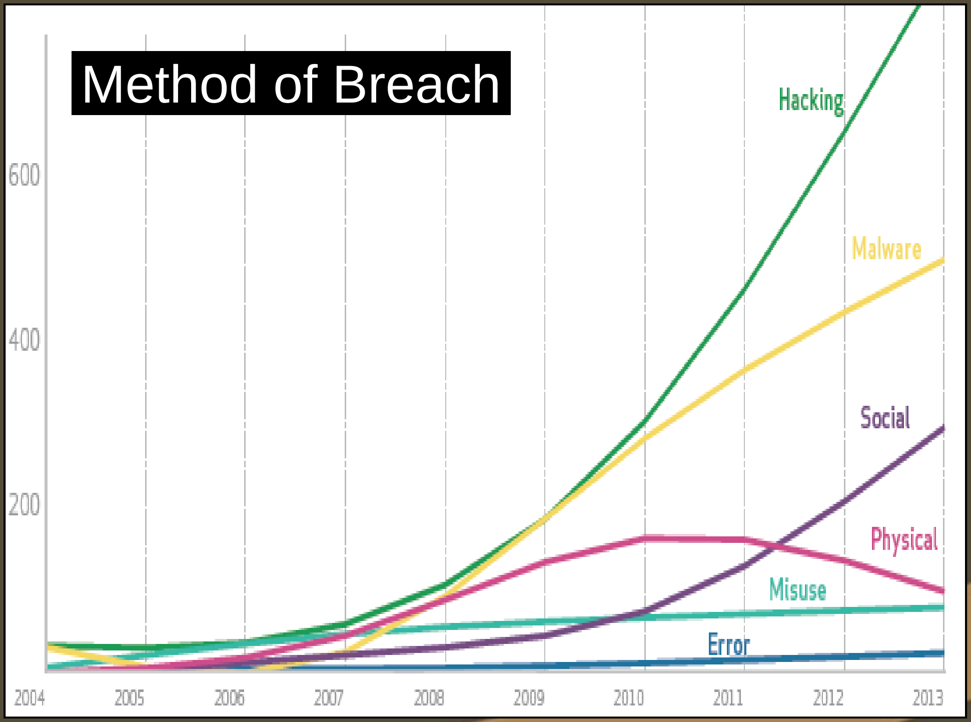
Typical order of events:

- An organization hires us for a “penetration test or other type of assessment
- We discover security issues, exploit them and take complete control of an environment
- Defense time – short term, mid-term, long-term → EXECUTE

Real-world Breaches Today

- More high-profile data breaches than ever before
- Compromise and subsequent infiltration of networks


Location of Breach


Method of Breach

Offense: How we and “they” do it

From the “Outside” Scenario #1 – Infrastructure Focused

- Starts with a vulnerability or weakness within a network, host or application
- “Pivot” inward gaining additional access to other systems, accounts, data
- Escalate priveleges and take complete control of the environment
  - accounts, passwords, email, file shares, databases, everything.

Facts:

- In the large majority of these cases, no one notices this has occurred
- This type of attack is focused on internet-available infrastructure, not users
- Executed from anywhere on the Internet

Offense: How we and “they” do it

From the “Outside” Scenario #2 – User Focused

- Users are the initial targets in the attack rather than infrastructure
- Email “Phishing” Attacks – you click a link, we are now you ☺
- From here we have a 99.9% chance of complete network compromise:
  - accounts, passwords, email, file shares, databases, everything.

Facts:

- The initial exploitation is usually the result of vulnerable client-side software
- Web Browsers and plugins, MS Office, Adobe, Java, etc.
- Executed from anywhere on the Internet

Offense: How we and “they” do it

An example “attack chain” from Scenario 1 - Infrastructure

1. Discovered a blind SQL injection flaw within one web site / application
2. Exploited the SQLi flaw to dump database contents:
   - usernames, passwords, PII, PHI
3. Gained control of the database host server and “pivoted” attacks inward
4. Gained complete control of other internal systems
5. Escalated privileges to Microsoft Active Directory Domain Admin
6. At this point we have access to:
   - accounts, passwords, email, file shares, databases, everything.

But wait, there’s more

Offense: How we and “they” do it

An example “attack chain” from Scenario 1 - Infrastructure

7. We dumped all password hashes from the Windows domain
8. Began cracking those hashes to obtain cleartext passwords
9. Created a mailbox for ourselves with a valid email address
10. Granted ourselves rights to executive email
11. Accessed executive leadership’s email: CEO, COO, CTO, CSO

No one noticed this has occurred.

Our client’s usually don’t know until we call them

Defense: Let’s stop the attack

How we could have prevented a catastrophic compromise:

1. Discovered a blind SQL injection flaw within one web site / application

- Intrusion prevention and anti-recon technologies stop the ability to identify weaknesses

2. Exploited the SQLi flaw to dump database contents

- Web application security assessments prior to deployment and upon changes
- Properly configured WAF (Web Application Firewall)

3. Gained control of the database host server and “pivoted” attacks inward

- Limited application database credentials (not DBA)
- Proper firewall egress filtering; servers should have no outbound internet access

4. Gained complete control of other internal systems

- Randomizing local administrative passwords; no password reuse
- Proper firewall access control limiting access to other systems
- Anti-Recon technology on the internal network
- Systems are patched

Defense: Let’s stop the attack

How we could have prevented a catastrophic compromise:

5. Escalated privileges to Microsoft Active Directory Domain Admin

- Native AD account tools are disabled and all administration is done via access system
- Alerting and automatic protection for privileged groups within active directory

- **We need to understand how these compromises occur in order to defend against them effectively.**
- **There is no “magic solution” you can acquire that will protect an organization.**
- **Technologies are often the quickest path to improvement when compared to affecting process and people.**

It’s really not that bad, is it?

Yes, it really is that bad

- Companies provide more services to customers and partners online.
- The majority of organizations expose and utilize many online systems.
- The attackers are getting better at a faster rate than the defenders.
- A general disconnect exists between corporate InfoSec and real-world attack techniques.

Attacks targeting users and their systems are an even larger issue.

One user visiting one web site can lead to a catastrophic compromise of your infrastructure and data.

This could occur within your organization today

What can we do about it?

What your organization does or doesn't do has significant impact

- Perform Penetration Testing – External, Internal, Wireless, etc.
- Assess applications and infrastructure regularly to discover security issues.
- Update / Patch Often both Servers and Workstations
- Implement Technologies that Solve Specific Issues, Not Every Issue
- Partner with a Trusted, Experienced Information Security Consulting Firm
- Understand how attacks and breaches occur and work backwards

Questions?

QUESTIONS?