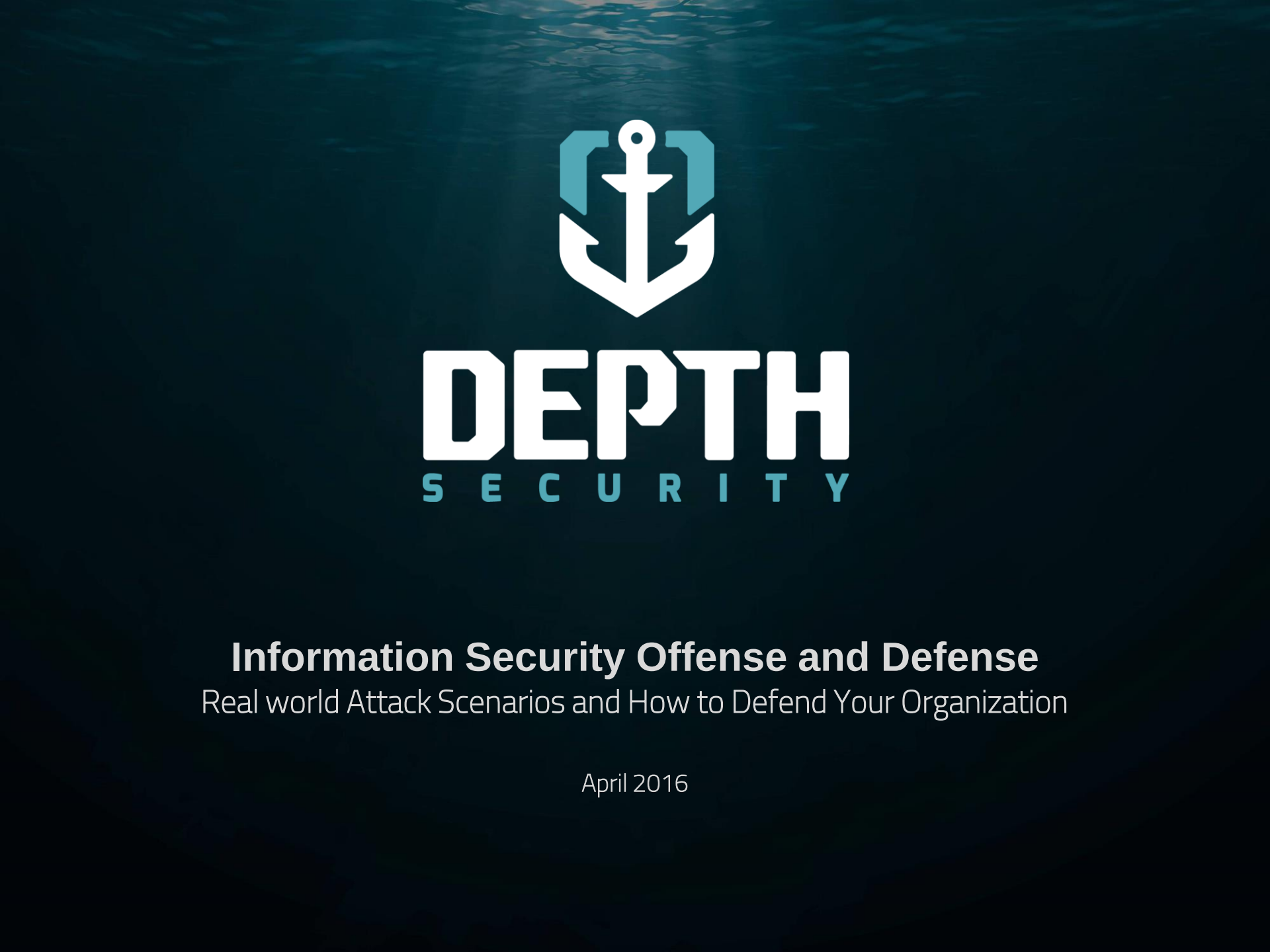


Information Security Offense and Defense

Real world Attack Scenarios and How to Defend Your Organization

April 2016

Depth Security

If there is a way in, we'll find it.

Who we are

A boutique information security firm founded in 2006 and based in Kansas City.

What we do

Offense: Identify and exploit weaknesses in networks and applications

Defense: Help defend against real-world threats utilizing services and solutions

Our clients

We work with a wide range of clients from SMBs to the Fortune 500.

Notable Data Breaches

Who, What, Where, When and Why

- Avid Life Media (AshleyMadison.com) – July 2015
  - Employee credentials, Emails, Files, Bank Account info, EVERYTHING
  - 37 million customer records including:
    - Names, addresses, account passwords, email and lots of other “items”
  - A screen was displayed on employees systems notifying them of a breach
  - Attackers later released a “data dump” containing most of the data gathered
  - “the impact team” wanted ALM to cease their operations
- The Office of Personnel Management – June 2015
  - 22 Million current and former federal employees (including me)
    - Names, Addresses, SSNs, Fingerprints, etc.
  - Breach was discovered after 343 days due to anomalies in SSL traffic
  - This appeared to be a data mining operation, seeking information for intelligence purposes.
  - The stolen data included information on various law enforcement and intelligence personnel.

Notable Data Breaches

Who, What, Where, When and Why Continued

- Premara Blue Cross – 11 million records of customer data and bank info
- Anthem – 80 million records of customer data
- IRS - Tax records for 330,000 taxpayers
- HackingTeam – 1 million emails of customers and exploits themselves
- Hyatt Hotels – Payment card breach across 250 hotels in 50 countries
- Hilton Hotels – Unknown number of payment cards breached
- Scottrade – 4.6 Million customers contact info and SSNs

Attack the Infrastructure

No User Interaction Required

- Infrastructure-focused attacks
  - Starts with a vulnerability or weakness within a network, host or application
  - “Pivot” inward gaining additional access to other systems, accounts, data
  - Escalate privileges 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 infrastructure, not users
  - Difficult against smaller organizations with less infrastructure exposed

Attack the Users

Every organization has users

- User-focused attacks
  - Users are initial targets rather than infrastructure
  - Email/Messaging phishing is the most common
    - Open an attachment
    - Click on a link and enter your credentials
    - Click on a link (yes, it's that easy sometimes)
  - Escalate privileges and take complete control of the environment
    - accounts, passwords, email, file shares, databases, everything.
- Facts:
  - In many cases exploitation is the result of vulnerable client-side software or as simple as users entering their credentials
  - Web browsers and plugins, MS Office, Adobe, Java, etc.
  - These are the most common attacks that face organizations today

How we and “they” do it

An example “attack chain” from our penetration testing practice

1. We discovered a blind SQLi (SQL injection) flaw within one web site / application
2. We exploited the SQLi flaw to dump database contents which included usernames, passwords, PII, PHI, payment card data
3. Gained administrative control of the database server and “pivoted” attacks inward
4. Gained 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

How we and “they” do it

An example “attack chain” from our penetration testing practice

7. We dumped all password hashes from the Windows domain
8. We began cracking those hashes to obtain clear text 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, CIO, CFO, etc.

Game Over

No one noticed this had occurred

In many cases, organizations usually don’t know until we call them

Attacking users is even easier!

An example “attack chain” from our penetration testing practice

1. Perform some basic reconnaissance on the target organization (emails, 3rd parties)
2. Register and stand up a new domain name
3. Send out emails from the new domain to employees
4. Employees just click the link and/or enter their credentials
5. We may have control of the employee’s system OR->
6. We reuse those credentials to log into remote access (Citrix, VPN, etc.)
7. We pivot our attacks inward and then escalate until:

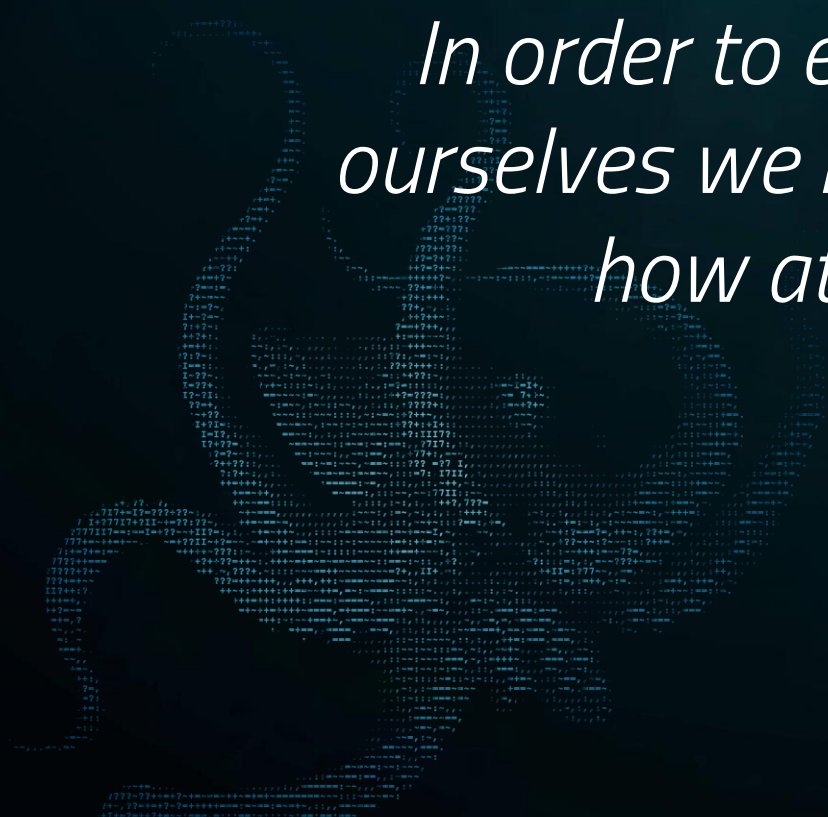
Game Over

Preventing the Attack

An example “attack chain” from our penetration testing practice

1. We discovered a blind SQLi (SQL injection) flaw within one web site / application
   - **Recurring Web Application Security Assessments to discover and remediate**
2. We exploited the SQLi flaw to dump database contents which included usernames, passwords, PII, PHI, payment card data
   - **A Web Application Firewall (WAF) could have easily prevented and alerted**
3. Gained administrative control of the database server and “pivoted” attacks inward
   - **The application’s database credentials should be restricted (not DBA)**
4. Gained control of other internal systems
   - **Anti-reconnaissance technology could have prevented lateral movement**
   - **Windows local account passwords should be unique across systems**
5. Escalated privileges to Microsoft Active Directory “Domain Admin”
   - **Advanced Endpoint Protection and Microsoft Active Directory configuration**

In order to effectively defend ourselves we need to understand how attacks occur.



It’s really not that bad, is it?

Yes, it is and here is why: What no one wants to tell you

- We live in a time where one user visiting one web site can lead to a catastrophic compromise of your infrastructure and data
- Some of the security controls that you rely upon aren’t effective
- There is a lot of “snake oil” being sold both in solutions and services
- There is an overwhelming talent deficit within the InfoSec landscape
- Where the demand is high, the talent bar is low
- Security metrics are either nonexistent or irrelevant in most organizations
- Attackers are getting better at a faster rate than the defenders are
- Most organizations do not have a complete grasp on how attacks and escalation occur

What can we do about it?

What your organization does or does not do has a significant impact

1. Perform Recurring Real-World Penetration Testing - External, Internal, Wireless, Phishing, etc. – This is a test of your people, not just technology.
2. Assess any and all web sites and web applications that your organization exposes on the Internet.
3. Consider next-generation endpoint security controls that actually prevent exploitation and escalation of systems. Your Antivirus software isn't enough.
4. Educate your employees on the various threats facing users and how to identify them. Consider executing simulations on a recurring basis.
5. Partner with an experienced information security firm that you can trust to actually help you improve your security posture, not just sell you things.

DEPTH

SECURITY

Questions?