Cybersecurity Landscape and Protections
What would you say you do?
Thinking security

...security is a mindset. It's a way of thinking. ... We're constantly looking at security systems and how to get around them; we can't help it.

--Bruce Schneier
Afterward to Little Brother
by Cory Doctorow
Thinking security

Security Guy – “Hey, I typed 100 random numbers into this text field on your application and it crashed.”

Developer -“Why would anyone ever do that?”

Security Guy – “Because you let me.”

Mikko Hypponen retweeted
Bill Sempf @sempf · Sep 23
Threats, Vulnerabilities, and Risks
Goals of Information Security

- Protect
  - Confidentiality
  - Integrity
  - Availability
Any circumstance or event with the potential to cause an adverse impact

- Malware
- Attacker (Can include malicious insider, careless employee)
- Mobile devices
- Social networking
- Cyber espionage
- Tornados, Hurricanes, Floods
What is the threat?
Real World Threats

- Web App Attacks: 908
- POS Intrusions: 525
- Miscellaneous Errors: 197
- Privilege Misuse: 172
- Cyber-espionage: 155
- Everything Else: 125
- Payment Card Skimmers: 86
- Physical Theft/Loss: 56
- Crimeware: 49
- Denial-of-Service: 1

Percentage of breaches

Source: 2016 Verizon Data Breach Report
Vulnerability

A flaw or weakness

- Lack of input validation
- Design flaw
- Unintended access points
- Software bugs
A measure of the extent to which an entity is threatened by a vulnerability

Risk = (Threat + Likelihood) * Impact
Security Principles
Security Principle 1

- Defense in Depth
  - A layered approach to address or protect against a specific threat or to reduce a vulnerability
  - Requires an attacker to circumvent each mechanism to gain access
  - Something WILL fail (it should “fail secure”)
Star Fort in the U.S.
Problem: Where is the perimeter?
Where is the perimeter?

Dropped infected USB in the company parking lot as a way of getting malware onto the company network

By Cory Doctorow at 4:00 pm Tue, Jul 10, 2012

Workers at the Dutch offices of DSM, a chemical company, report finding USB sticks in the company parking lot, which appeared to have been lost. However, when the company's IT department examined the sticks, they discovered that they were loaded with malware set to autorun in company computers, which would harvest employee login credentials. It appears that criminal dropped the keys in the hopes of tricking a employees into getting them into the company network.
Security Principle 2

Least Privilege

- The principle of least privilege requires that a user be given no more privilege than necessary to perform their job
- Requires identifying and understanding the user's job
Least Privilege in real world

Removing admin rights would mitigate:

- 98% of critical vulnerabilities affecting Windows operating systems,
- 99.5% of vulnerabilities in Internet Explorer
- 95% of critical vulnerabilities affecting Microsoft Office and
- 97% of Critical Remote Code Execution
- 80% of all Microsoft vulnerabilities

Security Principle 3

Never Trust Input

- Never trust data until the data is validated
  - Unless you have complete control of the data, it must be considered untrusted

- Don’t trust client side validation
  - You don’t have control of the client, the attacker does

- Don’t look for bad data -- look for the good data -- then reject input that does not pass your validation
Bad input checking
Social Engineering
Perspective

NIGERIAN PRINCE NEEDS $100K?

WHERE'S MY CHECKBOOK?
## Social Engineering

<table>
<thead>
<tr>
<th>Phishing</th>
<th>Spear Phishing</th>
<th>Vishing</th>
<th>Smishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass SPAM mailing to lure unsuspecting users.</td>
<td>Directed attempt focused on specific high value targets.</td>
<td>Phone scams directed at users.</td>
<td>SMS / Text Message scams.</td>
</tr>
<tr>
<td>An Ethiopian Prince has died and has left you millions of dollars.</td>
<td>Utilize social networks and deep company insights.</td>
<td>I’m from Windows and I’m calling to help you remove a virus.</td>
<td>Confirms active phone numbers and connection to banks.</td>
</tr>
</tbody>
</table>
Phishing

- Running a campaign with just three e-mails gives the attacker a better than 50% chance of getting at least one click.
- Run that campaign twice and that probability goes up to 80%
- Sending 10 phishing e-mails approaches 100%

From 2013 Verizon DBIR
Phishing

- Running a campaign with just three e-mails gives the attacker a better than 50% chance of getting at least one click.
- Run that campaign twice and that probability goes up to 80%
- Sending 10 phishing e-mails approaches 100%
- within 12 hours

From 2013 Verizon DBIR
Phishing Targets

Go where the money is

- **Financial** = 23%
- **Cloud Storage / File Hosting** = 22.6%
- **Web / Online Services** = 20.6%
- **Payment Services** = 14%
- **E-Commerce** = 11%
The headline you don’t want

Phishing attack leads to breach at government agency

Spear Phishing Attack Cause of Massive South Carolina Data Breach

Saint Louis University notifies 3,000 patients of data breach
Municipalities at risk

- Ransomware Attacks
  - City of Atlanta, GA
  - Montgomery County, AL
  - Mecklenburg County, NC

- Dallas, TX
  - Emergency sirens hacked in the middle of the night.

- Schuyler County, NY’s
  - 911 emergency management system was hacked and taken offline.
A common refrain

- City's procurement officers received what appeared to be a legitimate email from a purchasing coop.
  - The city does business with the coop.
- The email requested that the city change banking information and pay outstanding invoices to the new account.
- The procurement officer forwarded the request to the Finance Department, which changed the information and paid the $250,000
Yarrow Point, Washington

- Email scam targeting town’s financial coordinator
- Coordinator wired $49,284
- Annual budget around $2 million
Case Study – South Carolina Story

Department of Revenue breached
• 3.8 million tax payers and 1.9 million dependents
• 5,000 credit cards 3.3 million bank accounts

Result of a phishing attack
• Employee opened an infected attachment
• Attacker got username and password
• Attacker used valid accounts to gain continued access
What is the cost?

No final numbers on South Carolina breach

– Estimates from $14 – 25+ Million
– $12 Million for credit monitoring services

$20 Million Loan to Cover Breach Costs

South Carolina Lawmakers React with Slew of New Bills

Eric Chabrow (GovInfoSecurity) • December 13, 2012

The five-member South Carolina Budget and Control Board has approved a $20.1 million loan to cover costs associated with a breach of the state's tax IT system that exposed personally identifiable information of nearly 4 million taxpayers last summer.

See Also: Balancing Fraud Detection & the Consumer Banking Experience

The loan to the Department of Revenue will come from the

http://www.bankinfosecurity.com/20-million-loan-to-cover-breach-costs-a-5355
Social Engineering threatscape

- W2 scam
- Microsoft Support
- Ransomware

IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s

IR-2016-34, March 1, 2016

WASHINGTON — The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.
Phishing IRL

Dear Daniel,

I am pleased to inform you that you have qualified for an award of 2 roundtrip airline tickets. Congratulations. These tickets are valid for travel anywhere in the Continental U.S. from any major international airport. The retail value of this award is up to $1,298.00. Certain restrictions apply.

We have attempted contacting you several times without success. This is our last attempt. If we do not hear from you soon, we may need to issue the ticket vouchers to the alternate.

Please call me today at 1-866-568-9312.

Vice President

August 13th, 2012

US Airlines

[Image of the US Airlines logo]
Controls
Solutions
Knock down 80% of the attacks

- User training
- Keep software up to date
- Be aware of phishing, beware of suspicious emails and phone calls
- Backup data
- Mobile safety
- Avoid public wireless
- Don’t plug in random things
- Strong Authentication
## Legacy Systems

<table>
<thead>
<tr>
<th>Product</th>
<th>Mainstream Support End Date</th>
<th>Extended Support End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Vista</td>
<td>4/10/2012</td>
<td>4/11/2017</td>
</tr>
<tr>
<td>Microsoft Windows 7</td>
<td>1/13/2015</td>
<td>1/14/2020</td>
</tr>
<tr>
<td>Windows Server 2008 R2 Service Pack 1</td>
<td>1/13/2015</td>
<td>1/14/2020</td>
</tr>
<tr>
<td>Windows Server 2012 R2 Standard</td>
<td>10/9/2018</td>
<td>10/10/2023</td>
</tr>
<tr>
<td>Windows Server 2012 Standard</td>
<td>10/9/2018</td>
<td>10/10/2023</td>
</tr>
</tbody>
</table>
Solutions to Authentication Issues

- Single Sign-on
  - Easier to remember a single password

- 2 Factor / Multifactor
  - Something you know (password/pin)
  - Something you have (key fob, phone)
  - Something you are (biometric data)

- Role Based
  - Least Privilege

- Treat passwords like your underwear
  - Change regularly
  - Don’t share
  - Don’t leave them laying around
Preventive Controls

- Keep errors or irregularities from occurring in the first place

<table>
<thead>
<tr>
<th>Technical</th>
<th>Non-Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Access Controls</td>
<td>Training</td>
</tr>
<tr>
<td>Network Access Controls</td>
<td>Physical Security</td>
</tr>
<tr>
<td>Device and Software Hardening</td>
<td>Security Guards</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td></td>
</tr>
<tr>
<td>Patch Management</td>
<td></td>
</tr>
<tr>
<td>Application Security</td>
<td></td>
</tr>
</tbody>
</table>
Detective Controls

- Detect errors and irregularities, which have already occurred and to assure their prompt correction

Technical
- Audit Log Analysis
- Intrusion Detection/Prevention Systems (IDS / IPS)
- Security Testing and Audits
- Burglar Alarms

Non-Technical
- Metrics
- Managerial Reports
- Threat Intelligence Feeds
- Threat Sharing
Corrective Controls

- Respond to and fix a security incident

<table>
<thead>
<tr>
<th>Technical</th>
<th>Non-Technical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensics</td>
<td>Computer Incident Response Teams (CIRT)</td>
</tr>
<tr>
<td>Logging</td>
<td>Legal</td>
</tr>
<tr>
<td></td>
<td>Media Relations</td>
</tr>
<tr>
<td></td>
<td>Insurance</td>
</tr>
<tr>
<td></td>
<td>Exercises</td>
</tr>
</tbody>
</table>
Information Sharing

- Talk to people in similar positions
- Make use of federal, state, and local resources
- Let go of embarrassment
- Support curiosity
Thank You

Edward H. Block
CISSP, CIPM, CIPP/G, CEH, CISA
Foley Gardere
Foley & Lardner LLP
P 512.542.7052