THE SOCIAL MENACE

SOCIAL MEDIA AND ITS IMPACT ON SECURING SENSITIVE DATA

ISACA Geek Week 2016

Kevin Carpenter, IT Risk and Security Consultant, RSM US LLP
Agenda

- Introductions
- Cyber threat landscape
- Threat scenarios
- What can be done
- Q&A
Kevin Carpenter
Manager, Risk Advisory Services
- PMP, CISA and QSA
- Over 12 years of Information Security experience
- Former Big 4 consultant specializing in enterprise risk, SOX, IT risk assessments, and vulnerability management.
- Designed and implemented projects across numerous industries including healthcare/life sciences, manufacturing, higher education, financial services, consumer products, retail, public sector, automotive and gaming/hospitality

RSM US LLP
Cincinnati, OH
Kevin.Carpenter@rsmus.com
### Security and privacy services

#### Security Testing Facilities

- Dedicated Testing and Forensic Facilities

#### Overall Certifications

<table>
<thead>
<tr>
<th>Category</th>
<th>Certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Security</td>
<td>CISSP, CISA, CISM, CRISC, CSSLP, CIPP, GSEC, GCIH, GSFA</td>
</tr>
<tr>
<td>Security Testing</td>
<td>OSCP, CEH</td>
</tr>
<tr>
<td>PCI</td>
<td>QSA, PA-QSA</td>
</tr>
</tbody>
</table>

#### Security Services

<table>
<thead>
<tr>
<th>Category</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Governance</strong></td>
<td>- Management and frameworks (ISO, NIST, HIPAA, etc.)</td>
</tr>
<tr>
<td></td>
<td>- State, federal, international regulations</td>
</tr>
<tr>
<td><strong>Security Testing</strong></td>
<td>- &quot;On the keyboard&quot; i.e., ethical hacking</td>
</tr>
<tr>
<td></td>
<td>- Penetration testing</td>
</tr>
<tr>
<td></td>
<td>- Vulnerability assessments</td>
</tr>
<tr>
<td><strong>PCI</strong></td>
<td>- PCI DSS assessments/gap analysis</td>
</tr>
<tr>
<td></td>
<td>- Approved scanning vendor</td>
</tr>
<tr>
<td></td>
<td>- Review of payment applications</td>
</tr>
<tr>
<td><strong>Digital Forensics and Incident Response (DFIR)</strong></td>
<td>- Investigative support</td>
</tr>
<tr>
<td></td>
<td>- Incident response</td>
</tr>
<tr>
<td></td>
<td>- Real time threat detection and malware analysis</td>
</tr>
<tr>
<td><strong>Security Architecture</strong></td>
<td>- Process integration</td>
</tr>
<tr>
<td></td>
<td>- Vendor selection</td>
</tr>
<tr>
<td></td>
<td>- Performance improvement / Architecture design</td>
</tr>
</tbody>
</table>
CYBER THREAT LANDSCAPE

Misconceptions and Attack Vectors
Definitions… “the hacker” versus “the attacker”

**hacker** noun ˈha-kər
- A technologically savvy person, good at finding weaknesses in complex systems
- Two ways to describe hackers depending on how they use their skills
  - White Hat (For “good”)
  - Black Hat (Very “bad”)

White Hat methods mean using technical skills with permission of system owners and with the goal of fixing any weaknesses.

**attacker** noun əˈtækər
- A hacker who uses Black Hat methods, which means using their skills to find and exploit weaknesses for financial gain, or personal and/or ideological reasons
- These are the gals/guys that:
  - Infect computers with malware, trojans or viruses
  - Breach security systems to steal or destroy data
  - Steal identities and commit fraud
  - Engage in phishing
  - Carry out denial-of-service attacks
  - Steal intellectual property
Security misconceptions
*The attackers are not exactly who you think they are*

- Many of the standard methods of protection are now being bypassed with ease
- The underground economy has lowered the knowledge threshold
- Skilled attackers make more money at less risk by selling their knowledge in packaged form: Kits, automation, subscriptions, malware pre-packs, etc.

- Result: Pseudo “APT” attackers
- Result: Attackers have moved from brute force to simplicity, misdirection, abuse of trust
- Advanced Persistent Threats
  - a.k.a “Idiots with nuclear weapons”

The more we see the less we know
Security statistics

*Three most prevalent attack vectors*

- **Hacking**
  - “Traditional” hacking is used post-breach, not as the original entry point
  - Current methods focus on web apps and browser plugins

- **Malware (keyloggers, ram scrapers)**
  - Finding and purchasing nondetectable malware in the underground market is trivial
  - Modern anti-virus is an 80–20 proposition at best

- **Social engineering (phishing for credentials and more)**
  - Why bother to do all the heavy lifting involved with “hacking” when you can just ask someone to do something for you?
  - While there is a technical component, the attack is against human nature
What is the relationship with these objects?
What is a data breach?

Actual release or disclosure of information to an unauthorized individual/entity that relates to a person and that:

- May cause the person inconvenience or harm (financial/reputational)
  - Personally Identifiable Information (PII)
  - Protected Healthcare Information (PHI)

- May cause your company inconvenience or harm (financial/reputational)
  - Customer data, applicant data
  - Current/former employee data, applicant data
  - Corporate information/intellectual property
Personally identifiable information

What it is...

Personally identifiable information” (PII), as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

First name (or first initial) and last name, in combination with any of the following:
• Social security number
• Date of Birth
• Driver’s license / State identification card information
• Credit card / Debit card numbers
• Health records
• Genetic Information
• Financial account numbers
• Face, fingerprints, or handwriting
• Etc.

Top 10 Types of Information Exposed

<table>
<thead>
<tr>
<th>2015 Type</th>
<th>2015 %</th>
<th>2014 Type</th>
<th>2014 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Names</td>
<td>78%</td>
<td>Real Names</td>
<td>69%</td>
</tr>
<tr>
<td>Home Addresses</td>
<td>44%</td>
<td>Gov. ID Numbers (e.g., SSN)</td>
<td>45%</td>
</tr>
<tr>
<td>Birth Dates</td>
<td>41%</td>
<td>Home Addresses</td>
<td>43%</td>
</tr>
<tr>
<td>Gov. ID Numbers (e.g., SSN)</td>
<td>36%</td>
<td>Financial Information</td>
<td>36%</td>
</tr>
<tr>
<td>Medical Records</td>
<td>36%</td>
<td>Birth Dates</td>
<td>35%</td>
</tr>
<tr>
<td>Financial Information</td>
<td>33%</td>
<td>Medical Records</td>
<td>34%</td>
</tr>
<tr>
<td>Email Addresses</td>
<td>21%</td>
<td>Phone Numbers</td>
<td>21%</td>
</tr>
<tr>
<td>Phone Numbers</td>
<td>19%</td>
<td>Email Addresses</td>
<td>20%</td>
</tr>
<tr>
<td>Insurance</td>
<td>13%</td>
<td>User Names &amp; Passwords</td>
<td>13%</td>
</tr>
<tr>
<td>User Names &amp; Passwords</td>
<td>11%</td>
<td>Insurance</td>
<td>11%</td>
</tr>
</tbody>
</table>

Security Statistics

Compiled from:
- NetDiligence/McGladrey 2015 Annual Cyber Claims Study
The Privacy Rights Clearinghouse maintains a Chronology of Data Breaches

- Since 2005 there have been over 4,852 data breaches made public which resulted in 898,590,196 records breached and increasing (as of June 1, 2016).

- The numbers are not complete, many small breaches are not reported and the amounts of records breached in many cases is unknown

- The reported data breaches includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers

- Also includes some breaches that did not expose sensitive information.

THREAT SCENARIOS

Recon—Social Engineering—Attack—Payday
Recon and social engineering

• Recon:
  – What is a potential target advertising or broadcasting?

• Social engineering: Fancy name for traditional “con games”
  – Attacking an environment via manipulating people
  – Focused on user habits, mannerisms, human nature, entrenched organizational procedures and activities

• Hacking by the KISS principle
  – Keep it simple, stupid

• Why go through all of the effort to bypass firewalls, anti-virus, monitoring solutions, etc.?

• Why not just have the target do all the work for you?
SOCIAL MEDIA

Attack Vectors
Social media
Yeah, it’s huge…

• Social Media adoption across public and private sectors has risen drastically.

• It is not realistic to block employees from social media sites.

• Social Media, like all other cloud services, adds a layer of complexity to an organization’s security posture and security awareness program.
Recon—social media

- Corporate website
  - Org chart(s)
  - Employee information
    - Title
    - Phone number
    - Email address
    - Roles/bio
Recon—social media (cont.)

- Linkedin—Business Presence
  - Current and past employment
  - Contact information
  - Education
  - Skill sets
  - Roles/bio
  - Colleagues
  - Interests
  - Common connections
  - Physical characteristics
Recon—social media (cont.)

• Facebook—Personal presence
  – Contact information
  – Education/work
  – Family/friends/relationships
  – Current/previous residences
  – Interests
  – Connections to organizations and/or beliefs
  – Physical characteristics
  – Good/Bad/Ugly
ATTACKERS + SOCIAL MEDIA = TROUBLE

Putting It All Together
Social media and phishing
*Social engineering at its finest*

- Participation in social media can make an individual an easy target.
- Makes it easy to do recon on targets
- With higher volume, comes “lazy clicks.”
- Attackers capitalize on this using “Phishing Campaigns.”
- Phishing provides attackers with two main attack vectors:
  - “Watering Hole” attacks for hijacking credentials
  - Embedded malware for exfiltration user credentials and data, including PII
- Freely available tools allow phishing campaigns to be setup and executed in hours.
Attack scenario #1

- Phishing emails no longer look like a third grader created them.
Attack scenario #1 (cont.)

• Phishing emails payloads no longer look and function like a third grader created them.
  - Branded invoice
  - Bypasses most anti-virus
  - Embedded macro
    • Macro reaches out to the attacker’s servers to download malicious payload
  - Credential Harvester/key logger
  - Ransomware
Attack scenario #1 (cont.)

Follow the flow of how its done..

• Attacker offers something to the target
• Attacker needs the target system to come to them or accept something from them
• Simple as viewing a web page but can also involve local files such as documents
• Happy attacker dance!

Mr. Hacker

Emailed Doc

Control

User Action

Mr. Target
Ransomware

• Ransomware is a form of denial-of-service malware that attempts to export money from a computer user by restricting access to their computer and or files stored on it, including network shares.

• Most ransomware today utilizes very advanced techniques to evade traditional anti-virus/malware programs.

• It functions by encrypting the files stored on a computer system and on attached network shares.

• Options: pay ransom/restore from backups or…
Attack scenario #2

• Vendor Fraud aka. Invoice Fraud aka. Supply Chain Fraud:
  • Attacker identifies a vendor of the organization
  • Attacker attempts to convince the organization to make a normal or additional payment to a new account
  • Organization unaware of fraud until notified by the vendor

To: [Someone in finance]
From: Executive@vendor.com
Sent: Mon, Oct 5, 2015 at 2:01 am

Mr/Mrs. Someone, please be aware that we have recently changed banking providers. Our new account and routing numbers are in the attached pdf. Respectfully, Mr. Vendor Executive
Hi John,
We are acquiring a foreign company and you are the only one who can help me. No information can be leaked to anyone, even your superiors, or the SEC will cancel the process. Can you assist me with a wire transfer?
-Jim, CEO

Sure Jim,
Send me the bank information and I will be happy to take care of this. I understand and respect the confidentiality of this matter. I won’t tell anyone.

Attached is the bank information. The wire transfer for $750,000 must be completed today or the deal will fall through. Please let me know when this is done.
Well received, thank you. Tomorrow I will be sending you further instructions. Again, please respect the confidentiality of this deal.

Good morning,
An additional wire transfer of $400,000 must be completed today. I have attached the bank information. Please let me know when this is done. Thank you.

The wire transfer has been sent successfully. Attached is the confirmation. Let me know if you need anything else.

The second wire transfer has been sent. Attached is the confirmation.
Attack scenario #3 (cont.)

Hi John,
This is a scam. DO NOT open any attachments, and DO NOT forward any money. Please inform others about this scam as well.
-Manager

Dear Manager,
I am forwarding this message to you. Do you know what these instructions are? I am concerned about them.
-John

Unfortunately, I already forwarded $750,000 a few days ago, but was able to cancel another $400,000 transfer. I trusted the email instructions I received. I’m very sorry for this mistake.
WHAT CAN BE DONE

It’s Not Hopeless
Ask yourself…

• Does your organization have a social media policy?
  – Does it explain the risks of social media?
  – Does it define acceptable social media outlets?
  – Does it discuss information that is NEVER allowed to be discussed or posted on social media?
  – Does it define who is the key person that is responsible for maintaining and managing your organization’s presence on social media outlets?
  – Does it define who is the key person that is responsible for monitoring your organization’s social media presence?
  – Does it address any regulatory compliance requirements?
  – Does it define who is responsible for employee training?
  – Is training conducted regularly and repeatedly?
Basic security concepts

Make sure you have basic controls in 3 layers

- Prevent → Detect → Correct
- Have you made yourself a hard target?
- Are you capable of knowing if you have been breached?
- Can you respond effectively?

- Preventative controls
  - Vulnerability management
  - Patch management
  - Access and authentication
  - IPS
  - Configuration management
  - AV blocking

- Detective controls
  - SIEM and MSSP
  - IDS
  - DB activity monitoring
  - Compliance monitoring
  - Operational monitoring
  - AV host and network alerts

- Corrective controls
  - Incident response
  - Forensics
  - AV quarantine
  - Isolation
  - DR/BC
  - Admin/legal actions
What are the risks?

• Best case
  – Preventative controls are in place to identify detect, prevent and block attack.

• Worst case
  – Interruption of business
  – Loss of reputation
  – Loss of public and client trust
  – Endanger financial stability
  – Loss of client PII data may affect vulnerable groups
What should organizations do?

• Comprehensive “security awareness” campaigns
• Security Information and Event Management (SIEM)
• Incident Response Program (CIRT)
  − Scenario planning
  − Cyber simulations
• Disaster Recovery Plan (BACKUPS).
• Malware detection/avoidance:
  − End-point protection for hosts
  − Intrusion detection for networks
• Secure coding practices in SDLC
• Formal processes to authorize access to client and employee PII and/or financial information
QUESTIONS AND ANSWERS?