Security in Business and Applications

Madison Hajeb
Stefan Hurst
Benjamin Von Slade
Introduction

- Project Concept - Implement security in a small business setting
- Original Plan - Do some security audits for small companies
- Actual Plan - One company need a security review and the other company needed help with user tracking security
Two Different Projects

1. Krames Staywell Access Tracker
2. Wind River Security Review
Krames Staywell Access Tracker (KSAT)
Help them achieve HIPAA compliance by implementing a new applications
Two Initial Projects

Application 1
• Track the access employees have to applications that deal with Electronic Health Patient Information (E PHI)

Application 2
• Collect all the log files in a central location and create an application that can easily present those logs to an end-user for later review
• Dropped because they already have a Splunk server doing what they need
Plan

• Initially wanted to implement with Request Tracker, or RT for short.
  o Even though we looked into this, it seemed as if this may be scope creep.
  o Step Back: What is the end goal of this application?
  o RT is meant to do just that, organize requests.
    ▪ NOT for tracking access to applications
  o They could change some policies and use RT to make application requests, but, in the end, they still need to track who has access to what
KSAT - Requirements Gathering

- CRUD application
- Store all pertinent employee information
- No application specifics, just free form applications
- Ability to edit all information
- Search fields for things
- RT Integration?
- Log usernames, what they did, and timestamps
- Finish by interviewing all employees
Setting up a testing environment

- Windows Server 2008 Standard VM
- XAMPP Server (Apache, PHP, and MySQL)
- Cisco VPN from home
  - If we are on the school's network, VPN is not required

Special thanks to Jon Soldan and Dr. Randy Boyle for helping to get a testing environment up and running
Process

• Agile process
Settings File

- We created a central location for are specific url, database, and user settings.
- This made the transition from our testing environment to their production environment much easier.

```php
define('AD_HOST', '155.97.56.231'); // Active Directory Server IP address
define('DN', 'CN=Users, DC=msv, DC=local'); // Common Name Information
define('USER_GROUP', 'KSAT'); // Active Directory Normal User Group
define('MANAGER_GROUP', 'KSAT'); // Active Directory Manager Group (Same as User group if using ONE group)
define('DOMAIN', '@msv.local'); // Domain Name for authenticating username
define('MYSQL_HOST', '155.97.56.231'); // MySQL Server IP address
define('MYSQL_USERNAME', 'ksat_user'); // MySQL Username to access DB
define('MYSQL_PASSWORD', 'TASk65$w0rd'); // MySQL Password to authenticate user
define('MYSQL_DB', 'ksat'); // MySQL DB Name
```
Login Page

• Connects to a Microsoft Active Directory
• Allows to have a normal user group and an administrator group
  o We only utilized one group, so both settings point the same group. Allows them to add more control later if needed
Successful Login Landing Page

- After a successful login, the user is taken to the employee page
KSAT Demo
Interviews

• After application completion
• Given company laptops
• Each individual employee
• Query employees about all access they may have to applications dealing with EPHI
KSAT - Complications

- Unforeseen application errors
- Slight miscommunication on how the application functions
  - After KSAT was developed we found out that many of the applications go through a Development, Staging, and Production environment.
    - It would have helped to have an extra table in the DB where we could define "environments"
- Interview Communication
  - Each employee has their own naming conventions for applications, making populating KSAT difficult
- INTERNET EXPLORER!
  - CSS always looked slightly different in IE
KSAT - Lessons Learned

• Planning Planning Planning…
• Understand the business process to the fullest
  o Helps for application building process
  o Helps for interview process to fill database
• Constantly make sure you are on the same page as the company
• Some people are going to be difficult to work with
Wind River Security Review

- Excavation company located in Salt Lake City with job sites throughout Utah
- Have done many jobs here at the University of Utah, including work on the new business buildings
Task

• Security review of the technology and physical space of the office
  o Followed a security checklist for small businesses
• Provide recommendations about security and system upgrades
• Provide recommendations for security policies in the office
Requirements Gathering

• Access files from home
• Monitor employee activity
• Feel confident in computer security
• Change as few habits as possible
Initial Review

- Logged all hardware on the network
- Renamed computers numerically
- Physical security interview

<table>
<thead>
<tr>
<th>Device Information</th>
<th>CPU Information</th>
<th>RAM Information</th>
<th>Hard Drive Information</th>
<th>Monitor Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>CPU Type</td>
<td>Memory Amount</td>
<td>Memory Type</td>
<td>Hard Drive Space</td>
</tr>
<tr>
<td>192.168.1.101</td>
<td>Intel</td>
<td>2 GB</td>
<td>1 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>192.168.1.102</td>
<td>Intel</td>
<td>2 GB</td>
<td>1 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>192.168.1.103</td>
<td>Intel</td>
<td>2 GB</td>
<td>1 GB</td>
<td>8 GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Main Entrance</th>
<th>Front Door</th>
<th>Back Door</th>
<th>Side Door</th>
<th>Server Room</th>
<th>Filing Cabinets</th>
<th>Cameras</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Everyone</td>
<td>Rachel</td>
<td>Cameron</td>
<td>Kelly</td>
<td>Brian</td>
<td>None in office</td>
</tr>
<tr>
<td></td>
<td>Rachel</td>
<td>Kelly</td>
<td>Kyle</td>
<td>Mark (building entry)</td>
<td>Fonz desk unlocked</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chal</td>
<td>Rachel</td>
<td>Kylie</td>
<td>Mark</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kelly</td>
<td>Rachel</td>
<td>Mark</td>
<td>Mark</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chal</td>
<td>Rachel</td>
<td>Mark</td>
<td>Mark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Action

- Set up SSL on email
- VPN
- Nessus scan for vulnerabilities
  - Fixed all critical and important errors
- User accounts and folder access on server
  - Active Directory Workaround
- Trained employees
  - Keyloggers
  - Browser Security
  - Monitoring Systems
  - Backup
Key Learning Points

• Small companies are less receptive to monetary solutions
• Money was a large stalling point
• Security policies are difficult to enforce in a small casual office (without AD)
• People are resistant to change and new habits/software/policies
Comparison

Wind River

• Concern: General Security

• Medium Risk: They are not dealing with health information, but they are dealing with many clients and financial bids

• Legally bound to protect client financial data housed on the server

Krames Staywell

• Concern: HIPAA Compliance

• Higher Risk: Dealing with Patient information and employee login information

• Legally required to provide a log sheet of employee access according to HIPAA, so pressed for time before the next audit
Conclusion

• Security practices can be applied in many different business applications and scenarios
  o Two completely different businesses need security, but they need very different things
  o The umbrella of "security" is large and disparate at times
Questions?