Two-Factor Authentication
Solution Overview

Shawn Fulton
January 15th, 2015
MSU Information Security Vision and Mission Statement

Vision
Diminish IT security risks to an acceptable level and become the most effective IT function; enable the University to make informed decisions based on risk.

Mission
Design, implement and maintain an information security program that protects the University’s resources against unauthorized use, modification and loss. Establish a practical information security program that enables MSU to be the best public research University in the world.
Two-Factor Goals

• Safe guard MSU employee data
• Safe guard MSU HR/Payroll and Finance data
• Provide additional security on EBS applications to prevent susceptibility to phishing attacks
# Information Security Risks for MSU

## Who's perpetrating breaches?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>92%</td>
<td>Perpetrated by outsiders</td>
</tr>
<tr>
<td>14%</td>
<td>Committed by insiders (+)</td>
</tr>
<tr>
<td>1%</td>
<td>Implicated business partners</td>
</tr>
<tr>
<td>7%</td>
<td>Involved multiple parties</td>
</tr>
<tr>
<td>19%</td>
<td>Attributed to state-affiliated actors (+)</td>
</tr>
</tbody>
</table>

## How do breaches occur?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>52%</td>
<td>Used some form of hacking (-)</td>
</tr>
<tr>
<td>76%</td>
<td>Of network intrusions exploited weak or stolen credentials (-)</td>
</tr>
<tr>
<td>40%</td>
<td>Incorporated malware (-)</td>
</tr>
<tr>
<td>35%</td>
<td>Involved physical attacks (+)</td>
</tr>
<tr>
<td>29%</td>
<td>Leveraged social tactics (+)</td>
</tr>
<tr>
<td>13%</td>
<td>Resulted from privilege misuse and abuse</td>
</tr>
</tbody>
</table>

## What commonalities exist?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>75%</td>
<td>Driven by financial motives (-)</td>
</tr>
<tr>
<td>71%</td>
<td>Targeted user devices (+)</td>
</tr>
<tr>
<td>54%</td>
<td>Compromised servers (-)</td>
</tr>
<tr>
<td>75%</td>
<td>Are considered opportunistic attacks (-)</td>
</tr>
<tr>
<td>78%</td>
<td>Of initial intrusions rated as low difficulty</td>
</tr>
<tr>
<td>69%</td>
<td>Discovered by external parties</td>
</tr>
<tr>
<td>66%</td>
<td>Took months or more to discover (+)</td>
</tr>
</tbody>
</table>

*Verizon Data Breach Investigations Report – 2013

(+): Is an increase of 10% or greater from last year
(-): Is a decrease of 10% or greater from last year
Payroll Incident Summary

• Millions of attempts to hack into MSU computer systems every day (>20 million prevented during month of May 2014)

• Millions of SPAM and phishing scams every day, some faculty, staff, and students take the bait

• Current safeguards in place:
  – Email SPAM filtering – Over 5 million SPAM and phishing emails blocked per day
  – Anti-virus installed on workstations
  – Security awareness training

• Two Payroll Incident Examples
  – October 2013 and March 2014
  – Phishing emails are suspected of compromising the users’ EBS login credentials (user name and password)
  – No breach of MSU systems/network appears to have occurred
  – Risk currently mitigated by disabling online direct deposit changes

• People and process changes recommended to further improve prevention, detection, and response
Addressing Security Risks at MSU

Defense in Depth Approach
- Multiple layers of controls to reduce overall risk

Business enablement combined with risk reduction
Two-Factor Authentication Overview

Two-factor authentication requires the use of two of the three authentication factors:

- **Something only the user:**
  1. **Knows** (e.g. password, PIN, secret answer)
  2. **Has** (e.g. ATM card, mobile phone, hard token)
  3. **Is** (e.g. biometric – iris, fingerprint, etc.)
Who Uses Two-Factor?

Bank of America

twitter

Linkedin

tumblr

Outlook

eyebay

Dropbox

facebook

USAA

LogMeIn

ally

SECURITY ADMINISTRATION

PayPal

EXTRADE

skype

Fidelity

Vanguard

Office 365

DISCOVER

Gmail

charles SCHWAB

salesforce

Microsoft Azure

HSBC
How Two-Factor Authentication Helps

Credentials are commonly stolen through:

– Phishing attacks targeted at MSU
– Third-party sites compromised and same username/password used for MSU applications
  • Adobe, Yahoo, LinkedIn, Forbes, Zappos, and eHarmony were breached in past year, 32 million usernames and passwords stolen
    – 15,000+ users registered with MSU email addresses, unknown how many used MSU password to register with these sites

Two-factor authentication prevents attackers from accessing your account even if they obtain your username and password.
Two-Factor Strategy at MSU

• Second Factor will be a “soft” Token
• Identify an Industry Leader for the Two-Factor Components
• Enhance MSU’s single sign-on solution (Sentinel) to integrate with Industry Leaders Solution to provide Two-Factor
• Enable Two-Factor for EBS applications (portal, HR, Payroll, Finance, BI) for all current employees.
Two-Factor Authentication Deployment Options

Multiple deployment options available for MSU users:

1. Mobile application

2. SMS text message

3. Voice call made to desk, mobile, or home phone
Appendix A – Scope diagram

Case 1: User logs into EBS Portal
1. Authenticate in Sentinel
2. Routed to EBS Portal
3. Navigate to other EBS applications

Case 2: User logs directly into EBS application
1. Authenticate in Sentinel
2. Routed to EBS application

Sentinel

Case 1, Step 1

Portal
Case 1, Step 2

Cognos
Case 2, Step 2

KFS
Case 2, Step 2

ECC

STUINFO

XI/PI

MSUEDW

Basis Team & HR/ Payroll Power Users – Central Payroll and BAS Team

SAP Internal Login

In Scope

Out of Scope

Oracle Internal Login

SAP Internal Login

XI
/PI

STUINFO

ECC

KFS

Cognos

Portal

Sentinel

Case 1, Step 1

Case 2, Step 1

Case 2, Step 1

Case 1, Step 1

Case 2, Step 1

Case 1, Step 2

Case 2, Step 2

Case 2, Step 2

Case 1, Step 3

Case 1, Step 3

Case 1, Step 3
Appendix B – Enrollment: Step 1

Enterprise Business Systems

NOTE: In order to use this application, your browser must accept cookies.

You must use your MSU NetID (NetID@msu.edu) to access EBS.

Login

MSU ID: [blank]
Password: [blank] [Show Password]
Authenticator: MSU Net [▼]

For Authorized Use Only

- Please remember to log off the portal when finished, and also “Logout from Sentinel SSO Access”.
- Manage NetID and Password
- EBS Support

Enter your MSU Net ID in lower case letters. MSU Net ID and password are case sensitive.

System Notices

EBS Applications are available Sunday through Saturday, 7 days per week, 24 hours per day except for the following:

- Maintenance and repair
- Daily Finance (KFS) maintenance 8:30 PM to 10:30 PM

Go to ebs.msu.edu for current EBS system alerts, maintenance updates and other EBS information.

Visit the Service Status website to view all current system alerts and scheduled system maintenance.
Appendix B – Enrollment: Step 2

Select Your Credential

Select the type of credential you want to register.

VIP Credential
Use a VIP mobile application or VIP security credential to securely access your organization's services.

Select

SMS or Voice
Use a security code from a text message or voice call to securely access your organization's services.

Select

Temporary Security Code

Get

Get a temporary security code to access organization services.
Appendix B – Enrollment: Step 3

Register Your Credential

* Required Information

*Credential Type: VIP Credential

*Credential Name: [Your Credential]

[*Credential ID: [Your Credential ID]]

Security Code: [Your Security Code]

Credential ID examples:
Your credential contains a unique alphanumeric ID.

VIP Security Token (Back)  VIP Security Card (Front)

VIP Access

Security Code examples:
Your credential provides a dynamic 6-digit code that changes every 30 seconds.

VIP Security Token (Front)  VIP Security Card (Front)

VIP Access
Appendix B – Enrollment: Step 3

Register Your Credential

* Required Information

**Credential Type:**
- Voice Call
- SMS (Text Message)

**Credential Name:**
Enter a simple name that is easy to remember.

**Credential ID:**
(e.g. 1-555-555-5555)
Enter your phone number, including country code and area code.

Send a security code to your phone and enter it on the next page to complete registration.

[Cancel]  [Send]

Carrier charges may apply.
Appendix B – Enrollment: Step 4

You have successfully registered Test.
Enter a security code from this credential the next time you Sign in.
Appendix C – Login

Enterprise Business Systems

You must use your MSU NetID (NetID@msu.edu) to access EBS.

Login

MSU ID:
Password:
Authenticator: [MSU Net ID]

For Authorized Use Only

Please remember to log off the portal when finished, and also “Logout from Sentinel SSO Access”.

- Manage NetID and Password
- EBS Support

Enter your MSU Net ID in lower case letters. MSU Net ID and password are case sensitive.

System Notices

EBS Applications are available Sunday through Saturday, 7 days per week, 24 hours per day except for the following:
- Maintenance and repair
- Daily Finance (SFS) maintenance 8:30 PM to 10:30 PM

Go to ebs.msu.edu for current EBS system alerts, maintenance updates and other EBS information.

Visit the Service Status website to view all current system alerts and scheduled system maintenance.

© 2014 Michigan State University Board of Trustees
© Photo 2014 Michigan State University Board of Trustees
MSU is an affirmative-action, equal-opportunity employer.
East Lansing, MI 48824
Department Presentations on Two-Factor Authentication are Available

To schedule contact:
Katherine Ball
ktball@msu.edu
(517) 353-3295