February 2017 ISC Meeting

Contact us anytime at infosecurity@utdallas.edu
Nate Howe
CISO
nate.howe@utdallas.edu
CISO Update

• Compliance Training due February 28
• Honeypot collaboration with Computer Science
• Upcoming budget hearings
• Disaster Recovery internal audit
• Helen Mohrmann named CISO at UT System Admin
• UT Dallas CIO search
## Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percent of computers not encrypted or exempted, where required</td>
<td>15%</td>
<td>24%</td>
<td>30%</td>
</tr>
<tr>
<td>Percent of systems with one or more critical vulnerability</td>
<td>36%</td>
<td>30%</td>
<td>26%</td>
</tr>
<tr>
<td>Percent of users not covered by Exchange ActiveSync policy</td>
<td>100%</td>
<td>100%</td>
<td>96%</td>
</tr>
</tbody>
</table>
WHAT CAN YOU DO?

• Ensure that laptop and desktops are encrypted or exempted

• Review vulnerability scans and correct high-risk findings; install patches including 3rd party software

• Work with us to apply Exchange ActiveSync policy to your area
WHAT WILL WE SHARE TODAY?

• Identity Management
• IRS scams
• LastPass
• SecureWorks
• Identity Finder
• Compass
NetID System Upgrade

Powered by Microsoft Identity Manager

Shivani Narain

OIT – Systems & Operations

sxn125330@utdallas.edu
Change can be scary...

...but it doesn’t have to be.
"You’ve got to start with the customer experience and work backwards to the technology."
Did you ever...

Have trouble with your password?

Get locked out of a system?

Need support after hours?

Wish you didn’t have to keep renewing employees?
Improved self-service features including out-of-band authorization, available 24x7

Password changes take effect immediately

Less likely to get accidentally locked out

Less frequent password expirations

No more sponsorship renewal for current employees
More staff productivity

More focused user support

Reduced software and support costs

Reduced possibility of account takeover

In summary...happier users and better security
Project Timeline

**Planning** 7/1/2016 - 8/2/2016

**Design** 7/14/2016 - 8/29/2016

**Development** 8/22/2016 - 1/20/2017

**UAT** 1/23/2017 - 2/20/2017

**Focus Sessions** 2/21/2017 - 3/8/2017

- **UAT Complete** 2/17/2017
- **Demo Completion** 3/8/2017
- **Go - Live** 3/15/2017
- **Development Complete** 1/20/2017

Timeline:
- **2016** July, August, September, October, November, December
- **2017** January, February, March
**Next Steps**

- Campaign to update alternate email address for out-of-band password resets *(February)*

- Communication of upcoming changes *(February & March)*

- Demos of new NetID system *(February & March)*

- New NetID system to go-live *(March during Spring Break)*
“Behind every successful initiative is a group of supportive stakeholders!”
STEPHENIE EDWARDS
AWARENESS & OUTREACH MANAGER
S.EDWARDS@UTDALLAS.EDU
The IRS continues to expand its efforts to detect tax refund fraud. As of March 5, 2016, the report says, the IRS had identified 42,148 tax returns with $227 million claimed in fraudulent refunds.

…the IRS prevented the issuance of $180.6 million (79.6%) in fraudulent refunds.

The IRS also continues to expand filters the IRS uses to detect identity theft refund fraud. The filters increased from 11 in 2012 to 183 filters in 2016.
IRS Identifies Common Scams

- **Phone Scams**: Calls from criminals impersonating IRS agents remain an ongoing threat to taxpayers.

- **Phishing**: The IRS will never send unsolicited emails to taxpayers an email about a bill or refund.

- **Fake Charities**: Be wary of charities with names similar to familiar or nationally-known organizations.

- **Return Preparer Fraud**: Be on the lookout for unscrupulous return preparers.
THINGS YOU CAN DO

• Only use your Social Security Number when it's absolutely necessary

• Check your credit reports regularly for suspicious activity

• Don't throw away papers with sensitive information in the trash – use a paper shredder

• Information publicly displayed on social media like Facebook and LinkedIn could help criminals launch scams against you, including customized phishing messages
LastPass

Dalton Brown
Senior Vulnerability Analyst
daltonbrown@utdallas.edu
Groupon accounts hacked and thousands of pounds stolen from customers

Account details were accessed to purchase iPhones and European holidays

Hackers selling 117 million LinkedIn passwords

by Jose Pagliery  @Jose_Pagliery
May 19, 2016: 10:59 AM ET

Yahoo Says 1 Billion User Accounts Were Hacked

By VINDU GOEL and NICOLE PERLROTH   DEC. 14, 2016
Please Confirm Password
It looks like you entered a slight misspelling of your email or username. We've corrected it for you, but ask that you re-enter your password for added security.

Password

Log In

Recover Your Account

Sign up for Facebook

⚠️ Forgot your NetID Password?
(Or password has expired)

» Answer your challenge questions and change your password
INTRODUCING LASTPASS

• Our Password Manager technical partner
• Your passwords are safely stored — no more Post-Its
• You can generate or store different passwords for all your sites
• Save time by not having to reset or retype complex passwords
HOW DOES LASTPASS WORK?
WHAT’S NEXT?

1. Go to our website: www.utdallas.edu/lastpass

2. Enroll, install and start using LastPass today

3. Contact ISO with any questions: infosecurity@utdallas.edu
SecureWorks

Jeffrey Reynolds
Senior Security Analyst
jreynolds@utdallas.edu
OBJECTIVES

- Detect malicious activity affecting campus
- Improve monitoring and incident response capabilities
- Layered defense in depth
- Scale to our growing network
HISTORY OF PRODUCTS

• All have been Snort-based
  – Created by Sourcefire (acquired by Cisco 2013)
  – Network Intrusion Detection and Prevention System
  – Uses signatures written in a well-documented format
HISTORY OF PRODUCTS

August 2011

March 2014

August 2016
SecureWorks

- Uses Snort-based intrusion detection on iSensor devices
SecureWorks

- Ingests data feeds from many sources
  - Palo Alto Firewall logs
  - ASA Firewall logs
  - System events
  - Microsoft Anti-Virus [coming soon]
- Can monitor on a ‘by host’ basis
SecureWorks

- Extends ISO team by providing analysts to research events 24x7

- Research by SecureWorks, including view of other customers, adds confidence and value
Kovter uses a combination of javascript, powershell, shellcode and lnk files combined with registry hiding techniques to maintain persistence. The following standard registry run key is utilized twice for redundancy:

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

These run keys contain a null byte in the first byte of a randomly created subname making them not show up in the standard Windows registry editor and adding an extra layer of protection. This is a known feature of windows exploited by other fileless malware such as Poweliks. If you attempt to view the Run keys with regedit, an error window will popup with the following message: ‘Error Displaying Value’ ‘Cannot display: Error reading the value's contents’
Scope

• Scan high-risk systems, not ALL systems

• Two areas of focus:
  – Unencrypted computers
  – Systems in areas that regularly handle SSNs
    • HR
    • Payroll
    • Registrar
Finding Risky Data

- Kick-off meeting
- Schedule Identity Finder scans
- Follow-up meetings
  1. If you don’t need it, delete it
  2. If you need it, move it to departmental shared drive
  3. If you have to store it locally, ensure the system is encrypted
  4. If all else fails, ask department head to accept the risk
INITIAL DEVELOPMENT EFFORTS

• Replace and enhance security functions in ISAPPS
  – Incident Tracking
  – Server Registry
  – Datacenter Registry
  – Audit & Reports

• Leverage existing data sources

• Present a dashboard of risks to technical support staff for remediation
INITIAL DEVELOPMENT EFFORTS

• Security Risk Tracking
  – Tracks all systems, not just servers
  – Replaces ISAPPS Server Registry, Datacenter Registry
  – Uses data feeds from inventory, SCCM, Nexpose, etc.
  – Presents dashboard of compliance gaps / risks
RECENT DEVELOPMENT EFFORTS

- Exemption Tracking
- Issue Tracking
- User Risk Tracking
PHASE II DEVELOPMENT EFFORTS

• TemocNet registration
• Expanded compliance tracking (HIPAA, PCI-DSS)
• Automatically-generated reports for department heads
• Vendor Risk Tracking
  – Vendor Survey
  – Ongoing due diligence
  – Published list of vetted applications
JOIN THE CONVERSATION!

• Need a onboarding course? No problem!

• The Compass Working Group will reconvene starting in March
  – Discussions will focus largely on Vendor Risk Tracking
  – RSVP to lhausman@utdallas.edu to be added to the calendar appointment
LIVE DEMO! (TIME PERMITTING)

• [https://compass.utdallas.edu](https://compass.utdallas.edu)
Thank You for Attending

Contact us anytime at infosecurity@utdallas.edu