Increasing Security by Focusing on the Endpoints

Brandon DeLeeuw, Director of Client Solutions and Support, bdeleeuw@uncc.edu
Why endpoint security?

End user devices are among the most vulnerable parts of an IT infrastructure. To help mitigate the vulnerabilities associated with these devices, the University of North Carolina at Charlotte has focused on leveraging built-in tools that secure these endpoints and reduce costs by leveraging tools that already exist.
ANTI-VIRUS

Endpoint Computer Activity Status

- **1093** Active
- **197** Inactive 2+ Weeks
- **89** Inactive 2+ Months
- **12** Not Protected

Endpoint Protection Client Status

- Total active clients in this collection protected with Endpoint Protection: **95.7%**
- Total devices in this collection: **6625**
- Endpoint Protection clients in this collection that are active: **6154**
  - Active clients protected with Endpoint Protection: **5890**
  - Active clients at risk: **264**
- Clients in this collection that are inactive or not installed: **471**
  - Endpoint Protection agent not yet installed: **21**
  - Endpoint Protection agent not supported on platform: **0**
  - Configuration Manager client inactive: **408**
  - Configuration Manager client not installed: **42**
NEW ACTIVE DIRECTORY SCHEME
ENCRYPTION
Bitlocker and FileVault
Central Key Store
New Standard
VULNERABILITY SCANS

- Assets Running Obsolete Operating Systems: 0.10% of assets running obsolete OS
- Assets by Operating System: 54% of my assets are running the Microsoft Operating System
- Assets with Critical Risk Vulnerabilities: 7.76k Assets
- Newly Discovered Assets: 2.06k Assets
- Assets by Authentication Status: 13% of my assets had failed logins
- Total Asset Trends: 14.17k Total Assets (2.092% increase in the past 30 days)
- Exploitable Assets by Skill Level: 15% of assets can be exploited by a novice
- Assets with Expiring SSL Certificates: 66 Assets
- Assets with Expired SSL Certificates: 322 Assets
MONTHLY PATCHING

ITS, 20%, 80%
OPERATING SYSTEM UPGRADES

OS X El Capitan
PCI

Credit Card

CID
(American Express)

CAV2/CID/CVC2/CVV2
(all other payment card brands)

Chip

PAN

Cardholder Name

Expiration Date

Magnetic Stripe
(data on tracks 1 & 2)
THIRD-PARTY PATCHING
OFF NETWORK MANAGEMENT
PRINTERS
Open Relay
Separate VLAN
Security Checklist
DUO

Password + Proof = Access

Username
Password
Login

Is that you?

Success!
PHISHING SIMULATIONS

95%

“95% of all attacks on enterprise networks are the result of successful spear phishing”

Source: Allan Paller, Director of Research - SANS Institute
LESSONS LEARNED

- Have the people who "care the most" "own" the service
- Everything takes time and thoughtful planning
- Use planned/phased rolls outs when able
- Have policy align with practice e.g. encrypting the mobile devices
Questions