Securing, Logging & Auditing Your ID Card Production System

Joshua J. Bodnar
Director of Access, Transaction & Video Services
Ohio University
Before We Begin. . . A Quick Survey!

- Are you tracking who prints official ID cards and when?
- How are you doing it?

- Until the summer of 2016, we were not
  - We had no way to track:
    - When an ID card was printed
    - What cards were printed
    - Who printed them
Agenda & Session Outline

**Impetus for Change**
*How an internal audit motivated change*

**IDWorks Review**
*How IDWorks functions out of the box*

**Securing the Card Production System**
*Making changes to increase security and accountability*

**Wrap Up & QA Session**
*Things to Consider Moving Forward*
Ohio University Background

• Founded in 1804, Ohio University is the oldest public institution of Higher Education in the Northwest Territory and all points West in the United States
• Our main campus is located in Athens, OH and has a headcount of 23,000
• The One Card Office was not created until the summer of 2014
  – Prior to that time, functions were spread between various other units
    • Central IT handled system administration, maintenance and imports
    • IT retail store handled ID card issuance
    • Housing handled board and debit plan management
    • Access Control handled door access
  – After the office was created, it assumed primary responsibility for all functions of Blackboard Transact
Impetus for Change
A Visit from our Internal Auditors

• Regular Internal Audits of departments is standard practice
• One Card Office audit conducted in November/December of 2015
  – Office was about a year old
• An area for improvement identified was ID card issuance
  – “An evaluation of the process to issue ID cards revealed that when a copy of a card is issued (such as to replace a damaged card), the event is neither logged nor attributed to the employee who created the copy”
  – “These issues mean it is possible for an employee to issue themselves a copy of any ID card in the system without being detected”
A Visit from our Internal Auditors

• Other concerns from the audit related to ID card issuance
  – Handling of damaged IDs prior to destruction
  – Physical security of ID card supplies
    • Card stock and printing supplies not well secured or tracked
• Given the sensitive functions tied to ID cards, addressing these concerns was a priority
ID Works Review
Understanding the Problem

• Before we could address the problem, we needed to understand it

• Management of IDWorks and project design historically handled by IT
  – At that time, I had little direct experience with IDWorks
  – First step was to research the capabilities of IDWorks and our configuration

• The security and logging built into IDWorks is rather rudimentary
How IDWorks Functions Out of the Box

- IDWorks user accounts/passwords managed locally on each workstation
  - Does not integrate with Active Directory
- Built in logging does not provide much detail
  - Log shows username, project and number of cards produced
  - Does not include information on whose cards were produced
Assessing Our Existing Configuration

• One shared windows account configured for auto-logon on the ID workstations
  – Done for simplicity / ease of configuration of printers and software
• One shared account for IDWorks Production that all staff utilized
  – Done as a result of having multiple workstations and staff turnover rates
    • Having to manage accounts on each workstation was deemed too difficult
• No logging was enabled on the workstations
• Workstations had normal access to the internet
  – Workstations were being used for ID card production and other functions needed by retail operation
  – Also frequently used by staff to access social media
Post Assessment Concerns

• After further-assessing our environment, other concerns emerged
  – Security of the workstations
  – Controlling access to IDWorks software
  – Risk of workstations having internet access
    • ID workstations have direct access to BbTs database
• Properly addressing all of these concerns would require changes in processes and behavior for staff
Securing the Card Production System
Changes We Made

• Step One – Securing the Workstations
  – Eliminated the shared windows account and auto-logon
  – Staff requiring access added to an AD group managed by One Card Office
  – Group policies applied to ‘lock-down’ the workstations
    • Only those in the AD group could log on to ID workstations
    • Access to the internet disabled
    • Limited software that could be run to:
      – IDWorks
      – VMWare Horizon View
        • Used to access Virtual Desktop Instances (VDI) for other functions of retail store / access to internet
Changes We Made

• Step Two – Modifying the IDWorks Projects for Enhanced Logging
  – Use existing ‘job name’ functionality in IDWorks for logging purposes
    • IDWorks has the ability to use data from the card to create the name of the print job
    • There is a catch – the field must be on the card (not just on the production form)
  • Created a composite field in project with data we wanted logged:
    – Customer number
    – Last Name
    – ISO Pull Setting
    – Last 4 digits of ISO on card
    – Card type produced (Student, Faculty/Staff, Affiliate, etc.)
IDWorks Job Name Field Creation
Getting the Field on the Card and the Print Job

• Remember, the job name field must be a field **on the card**

• Created a field on the back of the card that is very small and has the text color set to white
  – This makes it invisible

• Created a field connector to bring the data from production form into the field on the card

• Field from the card is then set as the field used to identify print job in the “Edit Card Design Properties” screen
Where Does the Data Go?

• Data is headed for the Windows PrintService Operational log on the workstation

• **There are a few catches**
  
  – The PrintService Operational log is often disabled by default
    
    • You can manually enable by launching Event Viewer and navigating to: *Applications and Services Logs\Microsoft\Windows\PrintService*
    
    • Then right click on “Operational Log” and select “Enable”
  
  – Job name is not sent to the log by default for privacy reasons in Win 8 and up
    
    • This can be changed in Group Policy by launching gpedit and navigating to: *Computer Configuration\Policies\Administrative Templates\Printers*
    
    • Enable the “Allow Job Name in Event Logs” policy
Centralizing the Data from Multiple Workstations

• With a multi-workstation environment, we wanted a solution that would centralize the data from all workstations into a single log

• There are multiple log-gathering tools that could be used
  – We elected to use nxlog to gather and forward logging data to our central logstash system

• We also wanted a visualization tool to make the logs more accessible and easier to search
  – We elected to use a tool called Kibana to handle this
Configuring NXLog to Gather Logs

We have nxlog running using a network service account so that it can save data to shared network storage.

We are sending data to:
- Local machine
- Network share
- Centralized logging system
Kibana Log Repository Dashboard
Kibana Log Repository Record View

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>February 10th, 2017, 11:21:05.818</td>
</tr>
<tr>
<td>@id</td>
<td>1</td>
</tr>
<tr>
<td>@timestamp</td>
<td>February 10th, 2017, 11:21:05.818</td>
</tr>
<tr>
<td>@version</td>
<td>1</td>
</tr>
<tr>
<td>Hostname</td>
<td>OIT-ATHCAP2-2G ohio.edu</td>
</tr>
<tr>
<td>AccountName</td>
<td>jp888711</td>
</tr>
<tr>
<td>AccountType</td>
<td>User</td>
</tr>
<tr>
<td>Category</td>
<td>Printing a document</td>
</tr>
<tr>
<td>Channel</td>
<td>Microsoft-Windows-PrintService/Operational</td>
</tr>
<tr>
<td>Domain</td>
<td>OHIO</td>
</tr>
<tr>
<td>EventID</td>
<td>307</td>
</tr>
<tr>
<td>EventReceivedTime</td>
<td>2017-02-10 11:21:05</td>
</tr>
<tr>
<td>EventTime</td>
<td>2017-02-10 11:21:04</td>
</tr>
<tr>
<td>EventType</td>
<td>INFO</td>
</tr>
<tr>
<td>Message</td>
<td>Document 103, 100170165</td>
</tr>
</tbody>
</table>

*100170165|Crockston|1|0191|STU* owned by jp888711 on \OIT-ATHCAP2-2G was printed on XPS Card Printer through port Depot_CD800_10. Size in bytes: 578507. Pages printed: 2. No user action is required.
Non-Technical Changes

We also addressed non-technical security issues

– Cards awaiting destruction are kept in a locked box until shredded
  • Box is affixed to counter and only the manager has the key
– Supplies (blank cards and ribbons) are kept in locked storage and inventoried
– Used ribbons are sent to our confidential materials shredding provider
  • Used ribbons have negatives of all data printed on the cards
– Our service counter is covered by surveillance cameras
  • This was done when the retail store was renovated a few years ago
Wrap Up & Questions
Things to Keep in Mind

• The solution we came up with might not work for everyone
  – Assess your processes and environment
  – Investigate what tools your campus already has that you can utilize
    • VDI and Logstash/Kibana were significant benefits to our project
• Determine what level of risk is acceptable to you / your institution
• Test your changes before deploying
  – IDWorks can be very finicky
  – Group policy settings can have side-effects
    • This was especially true with our ‘lock-down’ GPOs
Questions?

Thank you for attending!

Josh Bodnar – bodnar@ohio.edu