Data Loss Prevention - An Auditors Guide

April 16, 2015 – Webinar 12pm – 1pm

Auditing DLP Tools and Using DLP Output During Audit Engagements
Webinar Focus/Features

• In this 60 minute seminar you will learn how DLP can assist in the audit process. You will learn about the purpose of DLP and how the systems output can assist in meeting regulatory compliance.

• At the end of the course the participant should have a better understanding of DLP. Auditors should have a better understanding of how to enhance their existing audit programs to provide assurance related to Data Loss Preventions Programs effectiveness.
Session Topics

What You Will Learn

• What is Data Loss Prevention
  – Purpose of DLP Tools
  – How They Work

• Common DLP Tools
  – Types – Enterprise Content Aware; DLP Lite; Channel DLP

• Tips for Configuring DLP and It’s Reporting to Achieve Regulatory Compliance and Context Awareness

• Tips on Auditing a DLP Solution

• Tips for Using DLP Originated Data During Audit Engagement
WHAT IS DATA LOSS PREVENTION

Purpose and How They Work
Data Loss (Leak) Causes

- Company Intellectual Property being exposed by external parties (Hackers)
- Company Intellectual Property being exposed by internal parties (Employees, Boards, Consultants/Temps)
Border Protections

• Firewalls, Intrusion Detection Systems, Vulnerability Scans, Penetration Tests focus on whose trying to infiltrate network from the outside
DLP

• Monitoring the way data is handled within the organization and the outflow of information
  – Emails
  – Shared Screens During Webinars
  – Instant Messaging
  – Downloads
    • External Drives / USB drives
    • Content Management Applications
Characteristics and what the auditor should consider reviewing

COMMON DLP TOOLS
Types

• Enterprise Content Aware - centralized management console, advanced policy definition and event management that supports complex workflows

• DLP Lite – Limited protocols and usually end point or network perimeter based with consoles supporting basic centralized policies and very limited or no event management

• Channel DLP – Integrated into another product like Exchange 2013 such as when to encrypt an email or send via secure tunnel
Best Data Leakage Prevention (DLP) Solution

Products in this category include those that help organizations safeguard their intellectual property and customers' critical data persistently – inside and outside the company. Network-based and endpoint data leakage prevention products will be considered.

Products should prevent data from unauthorized exit from the network, or protect data on the endpoint – whether the endpoint is connected to a network or not. Products typically are policy-driven and should include scanning of all data, regardless of protocol or application leaving the network, and/or keep track of peripherals, such as removable storage and attached to the endpoint – reporting that inventory to a central location or administrator. All entrants should have the capability of being managed by a centralized administrator.

Those products considered part of this category include: network DLP products, which are typically gateways; those products protecting only endpoints; and hybrid products that operate at both the gateway to the network and at the endpoint. Specifically for endpoint DLP, traffic should be monitored and encryption should be available.

- AirWatch by VMware for AirWatch Secure Content Locker
- Check Point Software Technologies for Check Point DLP Software Blade
- General Dynamics Fidelis Cybersecurity Solutions for Fidelis XPS
- McAfee for Data Loss Prevention (DLP)
- Varonis Systems for Varonis IDU Classification Framework
- Websense Triton AP-Data + AP-Endpoint
Simple checks to determine effectiveness and efficiency of deployed solutions

DLP CONFIGURATION AND REPORTING REQUIREMENTS
Basics

• Ensure the solution is aligned to information classification rules and that all information is classified electronically and the policies are written within the tool to discover new data and classify based on certain characteristics/patterns.

• The DLP solutions should be configured to identify sensitive information, monitor what ID or device is attempting to access it and stop it from leaving the organization through the use of content-level scanning and deep content inspection (DCI) technologies when deemed inappropriate or malleolous by policy and/or data signature or initiate the appropriate level of encryption before passing data to receiver.
Basics

• Egress Points (outward bound) should be configured and monitored by DLP Policies. Egress Points include end points/external gateways such as those for data storage and file transfer... including Ingress points when sensitive data is moving between systems like SAP and Hyperion

• Ensure all incidents/exceptions to policy are written to a separate mailbox for this specific purpose
AUDITING THE DLP SOLUTION

Overview of audit test plan
What to Review

• For First DLP Audit:
  – Review project initiation documentation
    • Determine business driver which lead to selection of tool and implementation
    • Determine Business Owner

• Scope of DLP Policy Enforcement
  • Engress Points Included... what’s excluded
  • Ingress Points Included... what’s excluded
  • Cloud... Mobile... BYOD... Social Media...
What to Review

• For Every DLP Audit:
  – Request a list and sample of current DLP reports
  • Review the Standard Operating Procedure for maintaining and monitoring the DLP Tool and Reporting Results
    – Review Topologies showing Ingress and Egress Points and interconnections to DLP solution
    – Review section on Report Analysis and Remediation
      » Shadow staff during the daily report review process
      » Review tickets recording review and, if separate, tickets documenting finding/exceptions/results requiring further research/remediation
What to Review

• National Vulnerability Database
  – Known vulnerabilities in your DLP solution
    • Vulnerability Scans... are security tools included?
  – How management patches 3rd party applications

For Example: http://www.cvedetails.com/cve/CVE-2015-1305/

McAfee Data Loss Prevention Endpoint (DLPe) before 9.3.400 allows local users to write to arbitrary memory locations, and consequently gain privileges, via a crafted (1) 0x00224014 or (2) 0x0022c018 IOCTL call.
Publish Date : 2015-02-06 Last Update Date : 2015-02-19
Ideas on where data from the DLP can assist in determining effective of good controls including configuration and monitoring capabilities

USING DATA ORIGINATED FROM DLP FOR VARIOUS AUDITING ENGAGEMENTS
• Blocked Transmissions –
  – This may signal a need for greater user awareness on acceptable sharing practices
  – It may also signal an external hacker in the network attempting to harvest information
  – False positives may also be identified where policies are not effective and may require modification/tuning
Sources


Gartner's - Magic Quadrant for Content-Aware Data Loss Prevention Published: 12 December 2013


[http://www.itpro.co.uk/data-loss-prevention](http://www.itpro.co.uk/data-loss-prevention)


Webcast: [https://www.brighttalk.com/webcast/9665/125463](https://www.brighttalk.com/webcast/9665/125463)
Questions / Thank You

If you would like additional information regarding any of today’s discussing please contact me by email, LinkedIn or Phone:
Shawna M Flanders
sflanders@bustechga.com
www.bustechga.com
727-483-3662