Data Retention and Cost Effective Data Loss Prevention Techniques

Eric Conrad, Mason Pokladnik, Manuel Santander

April 2008
GIAC Enterprises’ assets are its intellectual property, in the form of small (and portable) text fortunes

Propose a 3-phase plan to mitigate risk

- Phase 1: Assessment
  - Detect all proprietary information at GIAC enterprises
  - Look for policy violations
- Phase 2: Short-term remediation plan
  - Address any policy breaches
  - Deploy improved DLP architecture
- Phase 3: Longer-term remediation
The DLP approach

- Leverage tools and policies in place
  - IBM Proventia Firewall/IPS
  - GIAC Enterprise Data Labeling Policy
- Deploy new tools and policies where appropriate
  - Modsecurity, Snort, etc.
  - Improved Data Retention Policy
    - Reduce sensitive data (e.g. credit card numbers) available to attack
- Immediate focus is on short-term, achievable goals which will improve our DLP capabilities
Canary Cookies

- Our product does not lend itself to traditional DRM watermarking
- Create ‘Canary Cookies’ that should never leave the database
  - “C is for Cookie, and that’s good enough for me”
- Configure Snort IDS to detect Canary Cookies in motion on network
- Configure ClamAV Antivirus to detect Canary Cookies at rest
DLP Architecture

- Defense-in-depth with multiple layers of firewalls, routers, IPS, and IDS
- Modsecurity reverse proxy will deny suspicious internet traffic, and normalize the rest
- Snort IDS will detect attacks and policy violations
- Hardened SQL server protects the database
- Centralized logging & event correlation via syslog server + scripts
Proposed DLP Architecture
Summary Phase 1+2 Deliverables

- Project requires two System Administrators and one Web Application Developer
- Sysadmins will implement infrastructure changes including the new reverse proxy, IDS, and enterprise certificate authority.
- Web Application Developer will update the fortune cookie application to use stored procedures and new matching client/server validation checks to identify attacks
- 3-week project timeline in handout