Information Security Decisions

TechTarget

Data Loss Prevention

events.techtarget.com

Ed Gardner

Director of Infrastructure and Security Operations

Homesite Insurance

Our Experience with DLP

Information Security Decisions

TechTarget

A Tale of Two DLP Products

First Product: The Large Established Company

events.techtarget.com

Company Background

- Domestic home insurance carrier
- Private label products for large auto insurance carriers
  - Large company expectations
- Security aware senior management
- Intense regulatory pressure
  - 40+ state DOI audits
  - Model Audit Rule
  - MA 201 CMR 17 plus many other state privacy concerns
- PCI/DSS
- GLBA, HIPAA, etc

Background - Defense in Depth

- File level encryption
- Field level encryption
- Secure file transfer
- Secure email
- Locked down systems
- Least privilege approach
- Training
- And…

DLP!

Background -DLP

- Inherited a product that had been installed by Professional Services and previous staff
- Sat with basic configurations in a monitor-only state
- Required too many resources and time
- Complicated, relying heavily on both RegEx and product expertise
- Inconsistent results when investigating events
- Professional Services had to custom create all rules

Background – New DLP Product

- Manager who brought product in left before deployment completed
- Capabilities of product inconsistent with sales pitch:
  - Data at Rest on File Servers (not capable)
  - Terminal Services (not capable, remote staff)
- Sales rep and account support rep left company
- Initial agent deployment caused blue-screens on majority of test deployment group
  - Professional Services had to come on-site for two days to reconfigure agent build to not blue-screen PC's
- Final rebuild still causes periodic blue screens, and uses 10-20% of machine's resources

How It's Working

- Security Team works around deployment issues, deploys company-wide with overall positive results
- Terminal service capability in upcoming release
- Extensive work with company support to correct various configuration issues with the agent
- Correlation rules find data easily
- Working through logs and false positives to create customized rules to capture only PCI Data (still manpower intensive)
- Restricting USB port use to prevent company data from leaving the company (augmenting GPO)

Information Security Decisions

TechTarget

What the DLP Vendors Don't Tell You

Issues, Expertise, and Overhead

events.techtarget.com

Issues, Expertise and Overhead

- Very time consuming initial deployment
- Agents that control external ports can block ports inadvertently
- Having the ability to customize rules can take extensive training, or may need to be done by professional services
- NOT a “set it and forget it” solution
  - Constant monitoring and tweaking is needed, even once fully deployed

How Deep Does Business Want You to Go?

- Business buy-in is needed from the start
  - What processes will we impact by limiting data exchange?
  - Is IT or Security prepared to take over those processes?
- What do HR and legal want you to find?
  - Why do they want it? Big brother is watching?
  - What do they want you to do about findings?
  - Corporate culture impact (being watched) is non-trivial

How Sensitive is “Sensitive”?

- Do you want to deny a SSN but not a name address and phone number?
- What if an address and phone number are used with a SSN?
- Clearly define what data qualifies as “sensitive”
  - Will just one SSN or PAN cause a denial/ alert, or do you want to set a minimum threshold?

Technology vs. Education

- What should the balance of education vs. mitigating technologies be?
  - Organization dependent
  - Regulatory pressure, PCI concerns, or Intellectual Property concerns?
- Defense in depth
  - No one technology can replace education
  - No amount of education can create the safeguards of technology

Slow and Steady Wins the DLP Race

- Collecting sufficient data to create rules takes a long time and a lot of data
- The longer you collect and review in “log only”, the more false positives you can identify and eliminate
- Validate all your technical requirements with extensive pilot programs

Thank you!