Our Methodology Provides the Necessary Insurance for an Effective DLP Implementation

Introduction

Information security was a big concern for large insurance company, which had units specializing in auto, health, and property and casualty insurance. To safeguard information and meet regulatory compliance requirements, the company had implemented ISO27001:2005 controls and achieved certification for compliance.

The company wanted to enhance its information security and privacy controls, so they retained Aujas to implement a state-of-the-art data leakage prevention technology.

Overview

Aujas leveraged its data flow analysis and incident management techniques

Aujas Solution

- ✓ Design data protection governance & incident management framework
- ✓ Conduct a comprehensive data flow assessment
- ✓ Create functional specifications for the DLP solution and select the appropriate technology
- ✓ Align rule base to business data flow
- ✓ Manage incidents, remove false positives, fine tune rules, report on key metrics

The Business Need

Our client wanted to ensure that they chose the right DLP technology and implemented it with appropriate rules. They wanted as many rules to be in 'block' mode as possible and as quickly as possible. The company also wanted to ensure that the data leakage incidents were monitored, acted upon and reported to the management along with other key metrics on the success of the project. The primary challenges included:

1. *Designing the data protection governance and data leakage incident management framework* – For consistent data protection a framework for management of data protection technology implementation, rule design and deployment had to be created. An data leakage incident management framework also had to be redesigned so that the company could manage consequences of data leakage effectively and consistently.

2. *Performing data flow analysis across the company* – data for more than 20 business functions had to be assessed. Sensitive data within each function had to be recorded along with the classification levels and data flow. The idea was to identify all sensitive data and not just the typical financial data, such as credit card numbers.

3. *Identifying and implementing the appropriate DLP technology* – it was essential to select a technology vendor who understood the insurance firm's core business applications, processes and documents, and could most effectively detect data leakages in them.

4. *Creating and testing DLP rules* – After the data flow was assessed and a suitable technology selected, the rules had to be designed to protect the company's sensitive data. A combination of keywords, RegEx, and fingerprinting techniques had to be leveraged. The rules had to be tested and made live.

5. *Managing data leakage incidents* – Identifying incidents, weeding out false positives, and working with internal teams to manage data leakage incidents was another critical requirement. Fine-tuning and optimizing the technology implementation to ensure better alignment with business data movement rules, and KPI reporting were also necessary.

About Aujas

- Aujas is an IDG Ventures company
- IDG Ventures is a $ 3 Billion Group

- Offices in USA, India and UAE
- More than 300 clients and 500 projects across 23 countries
- Over 170 professionals

Practices:

- Information Risk Advisory Services
- Security Intelligence
- Identity and Access Management
- Application Security

Aujas Solution

The engagement was delivered in five phases: Framework Design, Data Flow Assessment, Technology Selection & Implementation, Rule Design and Incident Management.

Framework Design

- To ensure ongoing **effective and consistent DLP management, a framework** for data protection governance and data leakage incident management was created and finalized after multiple rounds of discussions with stakeholders.
- The framework consisted of **roles and responsibilities, processes, teams' responsibilities, communication plans, reporting and measurement metrics**.
- The framework was presented to all the involved stakeholders for final approval and implementation.

Data Flow Assessment Phase

- Business representatives were identified and interviews were scheduled.
- **Workshops were conducted** to orient the business representatives on the need and nature of the assessment.
- The business representatives were interviewed to **capture business sensitive data (structured and unstructured) along with the classification levels, compliance requirements and flow of data** across functions.

Technology Selection & Implementation

- Create **use case scenarios** based on the client's **specific requirements**
- **Compile functional specifications** for the DLP technology based on the use cases.
- Select and implement the **appropriate technology**

Rule Design

- **Assess sensitive** data to identify the appropriate means of identification (**keywords, RegEx, fingerprint**).
- Create **rules based on the data flow** (approved senders, methods, etc.).
- Test the **rules in monitoring mode**.
- Move rules into production and move the **low false positive ones into block mode**..

Incident Management

- **Monitor the DLP incidents**
- **Filter false positives**, identify trends and **fine tune rules**
- For confirmed incidents **assess if escalation** to senior management is required and coordinate
- Provide **periodic KPI reports** to management

Key achievements for this engagement:

- Assisted the client to establish a **framework for ongoing data protection**
- Helped the company to **identify data that is relevant to their business**
- Assisted the client to select the most **appropriate DLP technology**
- Built **rules for protecting key data** and **confidently implemented** them
- Managed **data leakage incidents, filtered false positives**
- Reported on **key performance indicators** to executive leadership

Benefits and Learning

Our client was able to implement business-aligned rules and **move rules from monitoring to blocking mode confidently**. There was a marked **change in the culture** of organization with new **user awareness** about data leakage.

The company now had an **effective way to manage data leakage** incidents and **fine tune rules** to increase program effectiveness.