ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

How Data Classification Helps Improve Data Leakage Prevention

Anu Taneja
anumca707@gmail.com

Abstract

Most Information that is of utmost value to the organization is electronic and with very few controls around it. Therefore, the role played by Data Leakage Prevention solutions as part of the base security infrastructure becomes critical.

Keywords: DLP- Data Leakage and Prevention, Network Security, Data Classification, Data Protection.

Introduction

In today's age with almost all information flowing in electronic form, organizations have not much control on the flow of data within and to other organizations. We keep hearing about organizations that have suffered business and financial losses attributing to information theft. These could be IPR or other confidential information where a breach costs dearly to the organizations.

Why Data Leakage Prevention is important?

CXOs are also slowly realizing that data leakage detection and prevention is of utmost important going forward. So the investments are not only flowing from CIOs budget but we have seen with our customers that other departments like Research & Department are sponsoring such projects as the information being generated by them if the bread and butter for the organization. But with the DLP technologies in place, still organizations are either not able to get the results out of it or have been struggling for a long time to do so. We believe that "DLP is an immensely powerful tool, provided the approach and deployment right".

Biggest Challenge in successful deployment of DLP

Data Classification- Most organizations we have met have had data classification policies in place but the challenge is that is it. They have very well drafted policies, classification levels etc. but it is major on a paper.

From a DLP technology standpoint the information if properly identified and classified in a proper way, can produce very good results. Data Classification forms the base for DLP deployments. So the first step in the direction of Data Classification is identification. We need to identify the data/information first, unless we have done so there is no way a DLP can decide anything. Post Identification is the classification of data where it is tagged based on classification levels defined by an organization.

The problem of data security even after the DLP Deployment is something that technology alone cannot handle, as this product is much more integrated with business side users compared to any other IT security product. This has more inputs from and outputs to the business and is configured based on what business defines as confidential etc. So to address the issue as a whole the process of Data Classification comes into play.

Data Classification as an Agent

Data Classification works as a change agent for any organization as it works at the level of any users in the organization who is generating information. As soon as the end users start participating in the classification process the whole organization is a way comes on to a common security process. This whole process results in end users participating in ensuring that better inputs are provided to DLP systems in turn increasing its performance and reducing false positives.

Benefits

- DLP Systems do have built in templates, which are either based on industry verticals or based in standards like PCI, HIPPA etc.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

- These templates help organization to small extent as they have preconfigured objects or policies that can be configured without customization requirements.

- But the DLP System has no understanding of the organization it has been deployed in, though some data discovery mechanisms are available but are again having limited impact.

Conclusion

“Discovery or identification is only the first step in the data classification process and unless that discovered data gets properly classified and impact is assessed the DLP Detection would not be up to the mark”.

References

1. *http://freehaven.net/anonbib/papers/pets2011/p2-har*
2. *http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention*
3. *http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931*