Data Loss Prevention Implementation

Posted on September 4, 2019

Introduction

Data prevention is essential to all companies because any data leakage can damage a company's reputation, which can result in loss. With the rise of theft of vital data, companies have found the best way to protect their data, and therefore, several companies are turning to DLP as the best alternative to safeguard information. According to Baylor (2017), data loss protection ensures that confidential information does not leave an organization and prevents authorized access to confidential data. The implementation of DLP requires a culture change since it introduces a new way of handling data and other sensitive company information. Prior to the implementation of data loss prevention (DLP), proper analysis of data, which includes backing up sensitive information, must be conducted.

Data Loss Prevention (DLP) Implementation Strategy

The best strategy for the implementation of DLP is to develop a clear plan, which is a clear procedure that would be adhered to to make sure the implementation of DLP is successful. First, the project team must identify sensitive data. This is done to prevent the loss of any data during the implementation stages. At this stage, the organization must make sure that all data in transit, stored and in-house, are properly protected through the protection of the channel. The second step is defining policy, which shall be used to guide the data. Once the sensitive data has been identified, an organization must derive a policy to protect the identified information from getting lost or leaked to a third party. The policy must involve some rules that can protect sensitive information, such as preventing the leaking or talking of credit card information.

The third stage of the implementation strategy is to determine the flow of information. This is done to make sure the source and the flow of data are understood so that the project team understands exactly where the software would be implemented. It is conducted to make sure that a close monitoring or information governor is put in place (Baylor, 2017). In most cases, this is conducted through questionnaires. The fourth step is to identify the business owners. This is an essential stage since the company uses an internal mechanism to identify owners of the data. It ensures that the leak is sealed and that a mixture of data is avoided. It should be done to highlight the contact person in any case sensitive data is lost. The final stage is the deployment of Data loss prevention software to safeguard the company.

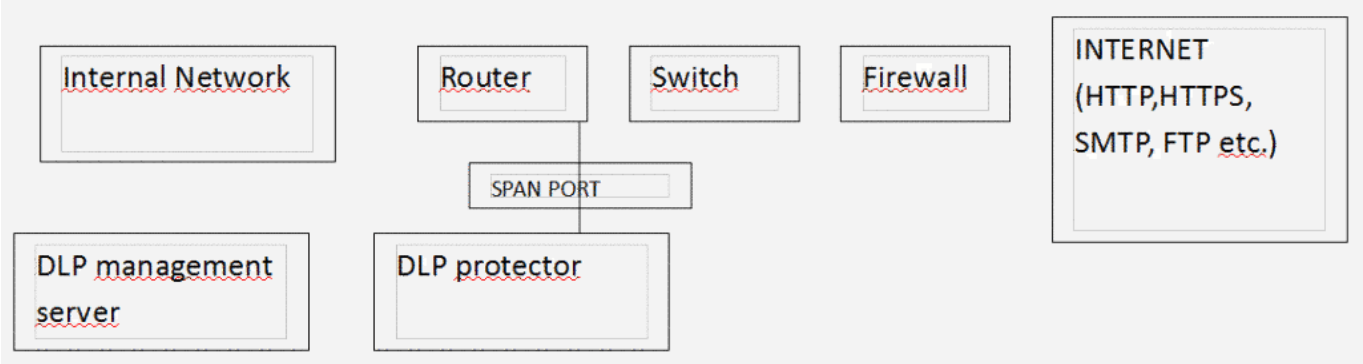

Figure 1: Data Loss Prevention Deployment Diagram

Data Loss Prevention Software

There are varieties of DLP software which can be used to protect an organization's sensitive data. Some of the software are Comodo Dome Protection, Spirion McAfee, Symantec Data Loss Prevention, Trustwave, Check Point and Digital Guide Data Loss Protection. Each of these software has unique features that make them different and can be used for specific areas (Fearn, 2017). All data loss prevention software protects unauthorized access to the system and leakage of sensitive information. Some are installed on the cloud system to protect against cybercrime and any other data breaches which can be attempted.

Symantec Data Loss Prevention

It is unique software used to monitor and protect sensitive data as well. Symantec Data Loss Prevention is scalable, it has impressived cloud coverage, and too enterprise oriented software. It is desktop-oriented software with capabilities to manage, monitor and track data. It is also one of the best DLP software for cyber security since it offers protection coverage for both consumers and businesses. It has the ability to store and monitor information, providing a platform for system administrators to monitor data performance and, hence, track any unauthorized entry in real time.

Mimecast Data Loss Prevention

This is DLP software which is used to prevent data from malicious or accidentally leaked information. The software is installed in the port to monitor any suspicious activities. It prevents data loss from the organization by stopping email leaks and making sure that all information left in the system is not confidential.

Comodo Dome

The Comodo Dome is also one of the DLP software used to protect data. It is used mostly in cloud computers to monitor and gain mobility. It is used to scan and monitor emails and transfer all outbound emails and traffic so that any unauthorized entry can be detected before causing any damage. It is, therefore, important to note that the only differences which exist among the DLP software are the features, and some perform specific roles. The software is best suited for cloud computing systems since it blocks ports which can be used by a third party to access the system.

Drawbacks

The implementation of DLP may create a lax in the prevention of data and, therefore, make the system more insecure. The fact that DLP is not a technology compromises the entire system, and a contracted company to safeguard an organization system can also access similar data. The DLP is a very expensive project to implement, and maintaining is also expensive; therefore, this can discourage other companies from implementing it. The financial support required in terms of implementation and maintenance might be a lot for some companies. It is a business product, not a technology, and therefore, it does not offer any technological solution to the problem. It can block the business process of a company instead of processing business, and this might impact negatively on a company's performance.

References

Baylor, K. (2017). 12 Steps to DLP Best Practices. *https://www.nsslabs.com/linkservid/13C2364A-5056-9046-931EC4F06A25968B/*, 2-34.

Fearn, N. (2017). Best data loss prevention software in 2017. *Avoid Data Breach*, 2-15.