International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Data Loss Prevention: Secure Important Data & Prevent By Threats

Akash Deep Gangwar[1], J. Godwin Ponsam[2]

Abstract—***it is very important to protect the business data from all kind of data breach attacks for every organization to maintain the brand reputation and customer faith. Security of data is the biggest challenges for the organization because intentionally or unintentionally we loses our sensitive data, so I focused on this paper how the organization losses his data and discuss a solution for this Problem. We analyze so many issues and challenges in data loss prevention. And also discuss what are the current mechanism are used by the companies for implementing the data loss prevention.***

Keywords: Data loss Prevention, issues and challenges, current scenario

1. Introduction

Data is more usable and exchangeable today at any time, and the vast superiority of data is sensitive at various levels. Some data is a part of internal organization and it is confidential so we cannot meant to be available to the public . Some data is sensitive because of corporate requirements, national laws, corporate requirements, and international regulations. Data breach has been one of the biggest problem that organizations face today. Quite a few organizations have been in the news for data disclosure and a popular recent case is Petroleum Ministry document loss: Caught in corporate espionage case, Reliance Industries, Essar, Cairn India, and R-ADAG[1].

While DLP is not a mixture to such assaults, it ought to surely be in the Stock of instruments to protect against such dangers.
The term DLP, which stands for Data Loss Prevention. Just as we have witnessed the growth of firewalls, intrusion detection systems (IDS) and numerous security products, DLP has already improved considerably and is beginning to influence the security industry. While DLP solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). In data loss incidents, sensitive data is disclosed to unauthorized personnel either by malicious intent or inadvertent mistake.

So how is DLP different from any other security technology? While apparatuses, for example, Firewalls and IDS/IPS search for anything that can represent a danger to an association, DLP is keen on recognizing delicate data. It searches for substance that is discriminating to an association. It would seem as though DLP is a solution whose only purpose is to prevent data breaches from intruders.

2. Data Loss Prevention

There are many ways to revealed sensitive data from organization by untrusted internal employee or third parties, in fig.1 we investigate several field including data repositories and available data loss channels. Customer records, accounts details, employee data, source code and sensitive documents on shares are a few examples of repositories. Different prevention techniques are:-

1) Data at rest: When the data is at rest, means to inactive data which is stored physically in any digital form, the repository can be protected with access control and must be regularly checked with data retention policies of the organization and compliance procedures as it might have increased probability to be loss out.
2) Data in motion: when the data is at motion means data is travel in a network (LAN,MAN and WAN) From one end to another end prevention using access control becomes increasingly difficult but analyses network traffic to detect sensitive data that is being sent in violation of data security policies.
3) (3)Data in Use: when the Data in Use means active data which is stored in a non-persistent digital state typically in computer random access memory (RAM), CPU caches, and such systems run on end-user workstations or servers in the organization.

They are used to control data flow between groups or types of users. They prevent conflict-of-interest between 2 or more group of users within the organization also. They control IM and e-mail communications before being stored in the corporate documents. These systems have the advantage that they can provide application controls to block attempted transmissions of confidential data from physical devices with spontaneous user feedback. Disadvantage is that they need to be installed on every workstation in the network, and can't be used on mobile devices **[2].**

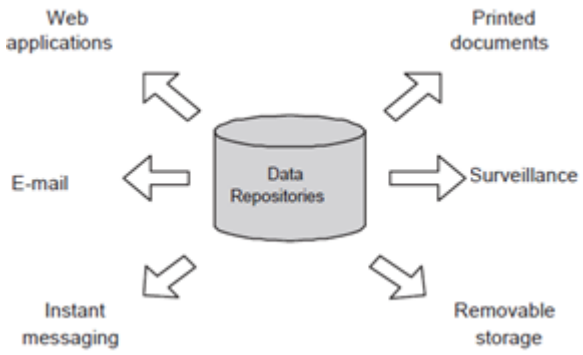

Figure 1: Data loss channels

As shown in Figure 1, Data misfortune can happen in a wide range of ways. Physical capacity, social building, observation, the inappropriate treatment of printed archives are a couple of the more customary data misfortune channels. Additionally, when electronic communications such as chat messaging, web applications and e-mail provide additional challenges. These electronic channels are highly utilized in organizations and provide means to quickly and easily send data to a third party. While traditional data loss can be more suitably defended with traditional approaches **[3].**

Protect your enterprise from data loss threats originating from the inside, such as email, IM, CD burns, web posting, USB copying, and printing. You also stop confidential data loss initiated by Trojans, worms, and file-sharing applications that hijack employee credentials without their knowledge. Consolidate snares to guarantee consistency of the imitated data& metadata, and to empower customization (robotized or manual) of the individual workload segments at recuperation site. Heat can be used to represent such workloads, as well as to automate the above processes.

3. Issues and Challenges

The greatest challenges for data loss is that there are so many ways data loss occur-

- Customer data: Improper access Rights to applications with sensitive data.
- Corporate data: A worker leaving the organization on Monday, Accessed the expert record of client detail and sent out it to an exceed expectations document.
- A call focus staff part gave screenshots of inward frameworks to fraudsters to help them figure out an application.
- A database director with a comprehension of test systems had the capacity figure out a cleaned process by referencing shrouded tables.
- Crooks have begun to influence web advertising as an apparatus to advance and shell their administrations on the underground market.
- Preparing and mindfulness projects don't concentrate enough on securing delicate data, suitable utilization of email and the web, utilization of security apparatuses, for example, document encryption and each worker's moral obligation regarding following data security/data assurance strategies.
- Modern noxious programming (malware) is stealth and showing signs of improvement, more astute, speedier and strong.
- Employees feel free for breaking the organization guidelines and think nobody is observing so I won't be caught.
- Remote laborer security: 46 percent of representatives confessed to exchanging documents in the middle of work and PCs when telecommute.
- Misuse of passwords: 18 percent of employees share passwords with co-workers. That rate jumps to 25 percent in China, India, and Italy.
- Encryption is making the determination of which data is private and which is most certainly not. It is improbable to anticipate that clients will make this determination in the process of directing business, improving the probability of agreeability infringe me.

Access control provides the first line of defense in DLP. Then again, it doesn't have the correct level of granularity and may be obsolete. While access control is suitable for data very still, it is hard to execute for data in travel and being used. As such, once the data is recovered from the store, it is hard to uphold access control. Furthermore, access control systems are not always configured with the least privilege principle in mind. For example, if an access control system grants full access to all code repositories for all programmers; it will not effectively detect data loss where a programmer accesses a project that he/she is not involved in.

4. Current Scenario

Various companies have recently started providing data leak Prevention solutions. While some solutions secure ‘data at Rest’ by restricting access to it and encrypting it, the state of Art relies on robust policies and pattern matching algorithms for data leak detection. Related academic work in data leak prevention focused on building policies [4], developing watermarking schemes [5] and identifying the forensic evidence for post-mortem analysis [6].
The current state of the art in data leak prevention focuses on pattern matching, which suffers from the general shortcoming
Of misuse detection techniques: an expert needs to define the signatures. Given the elusive definition of data loss, signatures should be defined per corporation basis, making the

Widespread deployment of current data leak prevention tools. A challenge. On the other hand, the relevant academic work
On data leak prevention and text mining takes a forensics approach and mainly focuses on the post-mortem identification. Thus, detecting complex data loss in real-time remains an understudied field.

- Discover where data is put away over your endpoints and servers; recognize genuine data holders and be alarmed to abnormal movement.
- Monitor how data is being used when users are on and off the corporate network.
- Protect data by advising clients about strategy infringement, securing uncovered records and organizers, and halting outbound correspondence.
- Manage data loss policies, work process and remediation, reporting and organization from an intense online administration reassure. Single Server Installation backing empowers you to send the Enforce stage, discovery servers, and database on a solitary physical server for extension workplaces or little associations, and brings down equipment and upkeep cost.
- Data Insight Self-Service Portal enables business data owners to review and remediate network file policy violations through an easily accessible web page, and streamlines the incident remediation process.
- Endpoint Agent finds data on endpoints running Mac OS X; screens occasions on endpoints running Microsoft Windows 8.1; screens virtual desktops and applications facilitated by VMware View and Microsoft Hyper-V;

screens data exchanged through the Microsoft Remote Desktop Protocol.
- Endpoint Communications allow more endpoint agents to connect to endpoint servers and improve system scalability.
- Endpoint Indexed Document Matching evaluates documents for exact content matches on endpoints in real-time and provides greater control over data use when users are off the network.
- Enforce Platform provides more flexible endpoint agent group configuration and enhanced agent health status reporting.
- Exact Data Matching enhancements increase the accuracy of data loss policies that look for fingerprinted data.
- Mobile Email Monitor recognizes secret email downloaded by clients to Android and iOS gadgets over the Microsoft Exchange ActiveSync convention, and gives more prominent deceivability into BYOD.
- Network Monitor distinguishes private data sent over the new form of the Internet Protocol, IPV6.
- Prevent from threats by analyzing the outgoing and incoming traffic in the network with the help signatures.

5. Conclusion

This paper described current activities toward the prevention of data loss in a multi organization environment. Organization protecting data from external intruders, but does not protect against theft and accidental disclosure of sensitive data by employees and partners. DLP can detect files that contain confidential data and prevent them from leaving via the network. It can block sensitive data transfers to Universal Serial Bus (USB) drives and other removable media. DLP also offers the ability to apply policies that safeguard data on a case-by-case basis. It Stops malicious insiders from stealing valuable intellectual property such as product designs and financial reports.

6. Future Work

Further research on DLP for securing the data on cloud computing and social network analysis.Social network analysis involves the mapping and measuring of relationships between people, groups and organizations by representing the relationships in terms of nodes and connections. Social networks can be derived from communication channels such as email, forum discussions, and social networking sites. Analysis of social networks can improve our understanding of the relationships and groupings between the parties involved in electronic communications, email in particular. Thus the goal of social network analysis for data leak prevention is to identify the communication patterns within the organization and employ feedback from the administrator to identify unusual communications to uncover to data loss.

Diesner et al. [7] performed a social network analysis of the Enron email [8], which contains the email correspondences of top-level Enron workers before and amid the Enron outrage. The informal organizations separated from the email correspondences take the type of coordinated diagrams where each edge is weighted by combined recurrence of messages traded between the hubs (i.e. individuals) in the chart. The correlation of the correspondence structure before and amid the emergency demonstrated a development toward imparting just between trusted gatherings, because of responsibility.

References

[1] http://www.financialexpress.com/article/economy/delhi-police-arrest-2-petroleum-ministry-employees-for-leaking-secret-data/44979/.
[2] Network Intellignce “data leakage prevention – implementions and chalnges”. http://www.niiconsulting.com/innovation/DLP.pdf.
[3] J. Livingston, “Tips and Strategies to Protect Laptops and the Sensitive ata They Contain,” *Data Systems Control Journal*, vol. 5, 2007.
[4] N. Vachharajani, M. J. Bridges, J. Chang, R. Rangan, G. Ottoni, J. A. Blome, G. A. Reis, M. Vachharajani, and D. I. August, “Rifle: An Architectural framework for user-centric data-flow security,” in *MICRO 37: Proceedings of the 37th annual IEEE/ACM International Symposium on Microarchitecture*. Washington, DC, USA: IEEE Computer Society, 2004, pp. 243–254.
[5] J. White and D. Thompson, “Using synthetic decoys to digitally watermark personally-identifying data and to promote data security,” in *2006 International Conference on Security and Management, SAM 2006*, June26-29 2006, pp. 91–99.
[6] S. Lee, K. Lee, A. Savoldi, and S. Lee, “Data leak analysis in a Corporate environment,” in *ICICIC ’09: Proceedings of the 2009 Fourth International Conference on Innovative Computing, Information and Control*. Washington, DC, USA: IEEE Computer Society, 2009, pp. 38–43
[7] J. Diesner, T. L. Frantz, and K. M. Carley, “Communication Networks from the enron email corpus”it’s always about the People. enron is no different”,” *Comput. Math. Organ. Theory*, vol. 11, pp. 201–228, October 2005. [Online]. Available: http: //portal.acm.org/citation.cfm?id=1110938.1110942
[8] J. Shetty and J. Adibi, “The Enron email dataset database schema and Brief statistical report,” *Information Sciences Institute Technical Report, University of Southern California*, 2004.

Author Profile

Akash Deep Gangwar is an M.Tech Student in SRMUniversity. HisSpecialization is Information Security and Cyber Forensics.

J. Godwin Ponsam is an Asst. Professor (Sr. G) in department of Data Technology at SRM University. His area of interest is Network Security.