DATA LOSS PREVENTION AND CHALLENGES FACED IN THEIR DEPLOYMENTS

Turobova Gulnoza Orif qizi
Gulnozaturobova14@gmail.com
940485181
Djangazova Qumriniso Abdulvaxobovna
qumri5544@mail.ru
93 853 39 88
Ganikhodjayeva Dilfuza Ziyavutdinovna
ganihodjayeva@mail.ru
90 976 24 51

ABSTRACT

The technology world has greatly evolved over the past three decades and it is at a pace where an average user's laptop can accommodate up to a terabyte of data, where a tiny SD card can store an entire database of an organization, where file transferring has become less complex, and where users can easily connect to any wireless network within the range of their wireless devices to exchange sensitive information. This evolvement has led to one of the greatest challenges organizations are faced with, which is in the area of adequately protecting their sensitive information from being lost or leaked. Data Loss Prevention techniques was created in preventing these breaches on data loss, when these breaches occur in an organization. DLP systems has gained popularity over the last decade and is now referred as a matured technology, and with the alarming rate at which digitally stored assets is growing, the need for DLP systems has also increased. This paper discusses some of DLP concepts and trends, as well as the some of the challenges these various DLPs face and proffer a solution for a successful implementation.

Keywords*-Data loss prevention; Data loss; Data protection; Data security*

АННОТАЦИЯ

Мир технологий значительно изменился за последние три десятилетия, и он идет такими темпами, когда на портативном компьютере среднего пользователя может поместиться до терабайта данных, а на крошечной SD-карте можно хранить всю базу данных организации, где осуществляется передача файлов. стал менее сложным, и пользователи могут легко подключаться к любой беспроводной сети в пределах досягаемости своих беспроводных устройств для обмена конфиденциальной информацией. Это *развитие привело к одной из самых серьезных проблем, с которыми сталкиваются организации, а именно в области адекватной защиты своей конфиденциальной информации от потери или утечки. Методы предотвращения потери данных были созданы для предотвращения этих нарушений при потере данных, когда эти нарушения происходят в организации. Системы DLP приобрели популярность за последнее десятилетие и теперь считаются зрелой технологией, и с тревожной скоростью, с которой растут активы, хранящиеся в цифровом виде, потребность в системах DLP также возросла. В этом документе обсуждаются некоторые концепции и тенденции DLP, а также некоторые проблемы, с которыми сталкиваются эти различные DLP, и предлагается решение для успешной реализации.*

Ключевые слова: *предотвращение потери данных; Потеря данных; Защита данных; Безопасность данных*

INTRODUCTION

Security breaches rocked 2017. The global outbreak of wannacry and not petya ransomware fundamentally changed the threat landscape, and attacks on organizations such as Equifax put astonishing amounts of data into the hands of hackers. It was a horrific year for data privacy and security - “cyber-geddon,” according to the BBC - and a wake-up call for CISOs and corporate legal departments everywhere. Data volume has been growing exponentially, dramatically increasing opportunities for theft and accidental disclosure of sensitive information. According to international data corp, the "global datasphere" will reach 163 zettabytes by 2025. To put that in perspective, if every gigabyte in a zettabyte were a brick, one zettabyte would be the equivalent of 258 Great Walls of China. And more than a quarter of data will be real-time in nature. This reality, along with increases in the portability of data, employee mobility and penalties for failing to comply with strict data protection regulations such as the EU GDPR raise the question: “What more can organizations do to protect themselves and their stakeholders?” An integral part of the answer is data loss prevention. DLP identifies, monitors and protects data in use, data in motion on your network, and data at rest in your data storage area or on desktops, laptops, mobile phones or tablets. Through deep content inspection and a contextual security analysis of transactions, DLP systems act as enforcers of data security policies.

DISCUSSION AND RESULTS

They provide a centralized management framework designed to detect and prevent the unauthorized use and transmission of your confidential information. DLP protects against mistakes that lead to data leaks and intentional misuse by insiders, as well as external attacks on your information infrastructure. In the wake of recent security events and regulations, interest in the technology has exploded. Gartner predicts that by the end of 2018, more than 50 percent of companies affected by the GDPR will not be in full compliance with its requirements.

1.	DLP technology provides IT and security staff with a 360-degree view of the location, flow and usage of data across the enterprise. It checks network actions against your organization's security policies, it and allows you to protect and control sensitive data, including customer information, personally identifiable information, financial data and intellectual property. With a thorough understanding of this data, your organization can set the appropriate policies to protect it and make risk-prioritized decisions about what assets need to be protected and at what cost.
2.	Not all data loss is the result of external, malicious attacks. The inadvertent disclosure or mishandling of confidential data by internal employees is a significant factor. According to Verizons 2018 Data Breach Investigations Report, 28 percent of attacks involved insiders. The insider threat can be particularly difficult to guard against - it's hard to spot, if someone is using their legitimate access to data for nefarious purposes. DLP can detect files that contain confidential information and prevent them from leaving via the network. It can block sensitive data transfers to Universal Serial Bus (USB) drives and other removable media, and offers the ability to apply policies that safeguard data on a case-by-case basis. For example, if a security event is detected, access to a specific endpoint can be blocked instantly. Policies can also quarantine or encrypt data in real - time response to events.
3.	Data breaches have been making headlines with alarming frequency. They can wreak havoc on an organization's bottom line through fines, bad publicity, loss of strategic customers and legal action. According to the Ponemon Institute's 2017 Cost of Data Breach Study, the mean time to identify breaches has reached an average of 191 days, which translates into over six months of dwell time for attackers. Dwell time enables lateral movement - the key to increasing hackers' chances of success.

4.	Requirements such as the GDPR and NY Cybersecurity Requirements are ushering in a new era of accountability, in which every regulated organization that collects, stores and uses sensitive customer data needs to raise the bar to meet new standards. Consequences for non-compliance can include fines of up to four percent of annual worldwide turnover, and instructions to cease processing. Technology controls are becoming necessary to achieve compliance in certain areas. DLP provides these controls, as well as policy templates and maps that address specific requirements, automate compliance, and enable the collection and reporting of metrics.
5.	Insiders represent a significant risk to data security. An employee who emails a work-related document to his personal account in order to work over the weekend may have good intentions. However, he or she poses a tremendous threat when there is confidential data involved. DLP technology offers 360-degree monitoring that includes email (both corporate accounts and webmail), instant messages, keystrokes typed, documents accessed and applications used. It also allows you to capture and archive evidence of incidents for forensic analysis. With DLP, you can limit and filter Web surfing, and control which applications employees can access. It is an invaluable tool in the effort to stop dangerous or time-wasting activities, and helps to detect problems before they can damage your business.
6.	Data is increasingly being moved to applications in the cloud—an environment in which it is not apparent where data will be physically stored and processed. DLP recognizes confidential data, ensures that it does not make its way into the cloud without being encrypted, and is only sent to authorized cloud applications. Most cloud DLP solutions remove or alter classified or sensitive data before files are shared to the cloud to ensure that the data is protected when in transit and in cloud storage.
7.	DLP technology monitors all endpoint activity, on the corporate network or off. It can block emails or attachments containing confidential data, enforce policies on the transfer of data to removable media devices such as USB thumb drives, and even prevent activities such as printing, copying and pasting. DLP offers complete data visibility and control, ensuring that employees, third-party vendors, contractors and partners are prevented from leaking your data—intentionally or inadvertently.
8.	DLP capabilities for the enforcement and automation of corporate policies and processes can help improve technical and organizational efficiencies,

	promote compliance, and provide methods for more comprehensive information governance. DLP provides up-to date policy templates and maps that address specific requirements, automate compliance, and enable the collection and reporting of metrics. When a policy need is identified, DLP can make the change as simple as enabling an appropriate policy template on your system. When organizations fail to take the necessary steps to identify sensitive data and protect it from loss or misuse, they are risking their ability to compete. Companies that get data protection and privacy right can enhance their brand reputation and resilience going forward. Those that get it wrong are likely to end up in the financial, reputational, and legal line of fire. DLP facilitates the protection of critical data, and helps to prevent the negative publicity and loss of revenue that inevitably follow data breaches.
9.	When used in conjunction with complementary controls, DLP helps to prevent the accidental exposure of confidential information across all devices. Wherever data lives, in transit on the network, at rest in storage, or in use, DLP can monitor it and significantly reduce the risk of data loss.

Data Loss Prevention should not be an afterthought

Today's digital transformation - from mobile devices to embedded systems, hypervisors, social media applications and the proliferation of connected devices - has created a "borderless" network perimeter with multiple attack vectors. To adjust to this technology revolution, organizations need to ensure their most sensitive data and assets are secured. When properly deployed, DLP provides visibility, granular control and data protection coverage to protect against mistakes that lead to data loss, intentional misuse by insiders, and external attacks. Developing a comprehensive data loss prevention strategy shouldn't be an afterthought; it can help your company protect its "crown jewels," maintain compliance with the evolving regulatory landscape, and avoid being the next data breach headline.

Some pointers on DLP

A discover utility should be able to scan the whole network and not just windows platforms. A solution may leave a file marker where confidential information did reside, though quarantining the original file. The marker would inform user on data protection policies and how they can regain access to the file. An Endpoint solution should prevent from copying sensitive data to removable devices even when off the network, via an agent installed on the local machine. Endpoint

Prevention should block files to removable media, or transferred over email, IM (Instant Messaging) or ftp. Endpoint agents should provide local detection for policies when the laptop is offline. It should be able to block users copying to removable disk and should ask a user to justify why they need to send this data. This is a good learning practice for both administrators on why users need to send such data and for end user's making them aware of the sensitivity of data. Data security policies should be defined using a policy builder within the centralised management platform. A user should be able to create a policy from scratch or use a policy template from a package of defined templates to meet different types of needs. A user should be able to write the policy once and enforce it across all defined data models. Storage areas would need to be scanned and so scanned targets would need to be defined within the central interface. Most important data first should be protected first, and then monitoring and testing this, and fine tuning where necessary. To go a step further, a technical control which proves to be very powerful is the integration of IRM/DRM solutions. If employees are allowed to take documents off site such as Microsoft Office and PDF documents, a DRM/IRM policy will keep the document tightly controlled depending on the privileges assigned.

A common example of sensitive data when protected by DLP controls;

Step 1 – A user defines a data security policy, defining detection rules and response rules. Once a policy is defined and active, network monitoring tools and or network prevention tools are able to inspect data and match this against defined policies. If network monitoring inspects and finds a match, it will report an incident.

Step 2 – An employee sends confidential data such as an attached diagram (Intellectual property, source code, payment details, etc).

Step 3 - Network prevention is able to block the email or any other type of data from leaving. The policy it hits will consist of defined detection rules and response rules. A response rule will specify how to respond to a detected incident, e.g., block email and send a notification to management. It may choose from blocking the transmission, tag for redirection or downstream processing.

Step 4 - The system can optionally send the employee a notification, referred to as a sender notification which provides real time security education of the organisations data security policy. Sender notifications should contain links to corporate policies, FAQ, and more assistance.

The incident will be logged and can later be used for reporting purposes. The notification can be customised to include variable data that was captured with the incident, for example, subject and violations or recipients email.

CONCLUSION

Many of organizations have given a great deal of attention in protecting their sensitive data from been lost accidentally or intentionally. DLP systems cannot function effectively in isolation, this implies that for a DLP system to effectively function it requires linking other security information process. However, before implementing any DLP system, there is need to adequately understand what confidential data the organization wants to hold, where does confidential data are to be stored in terms of locations as where those data are been stored are vital in its protection and the destination and the channels this information will pass through. There are several challenges associated with DLP systems, before they are deployed it is necessary and as well as important to adequately have a deep understanding and be able to analyze these various challenges associated with the system. It is also important to make the system easy to be used and managed, so as to avoid any form of complexity, as the more complex a DLP system, the more likelihood the system will be compromised by the user.

REFERENCES

[1] N. Kumaresan, "Key consideration in protecting sesitive data leakage using Data Loss Prevention Tools," ISACA Journal, vol. 1, pp. 1-5, 2014.

[2] E. Bergstrom and R. M. Ahlfedt, "Information Classification Issues," Sprin International Publishing, pp. 27-41, 2014.

[3] DataLossDB. (2016). 2015 Reported data breaches surpasses all previous years. Available: http://blog.datalossdb.org

[4] IBM and Ponemon Institute LLC, "2015 Cost of Data Breach Study: Global Analysis," Ponemon Institute LLC Research Department 2308 US 31 North Traverse City, Michigan 49686 USA 2015.

[5] Trend Micro. (2016). Data Protection Mishap leavees 55M Philippine Voters at Risk. Available: http://blog.trendmicro.com/treandlabs-security-intelligence/55mregistered-voters-risk-philippine-commission-elections-hacked