Big data convenient environment free fast access to data and the analysis of the resulting data security

Ying,WU
Shanghai university of political Science and law, Shanghai,China

Keywords: big data, data use, data security

Abstract. Big data applications involving more and more, especially in recent years to accelerate the development of Internet technology to facilitate data acquisition gave Big Data security threat to bring more great data security threat that has been extended to the various fields, especially leakage of sensitive corporate data to the enterprise's economic development and the loss of corporate reputation fatal danger. Based on the development trend of big data, analyze corporate data security threat facing, and this needle propose policies and measure to be taken.

1.Introduction

As the big data applications more and more involved in the field, especially in recent years the Internet technology and accelerate the development of electronic commerce, information security has been extended to all fields, especially enterprise sensitive data leakage, not only cause great economic losses to the enterprise, also can bring fatal influence to the enterprise credit. 2011 well-known programmers CSDN website user information leakage of more than 600, 2013, part of the brand chain hotels "key data breaches" events, in December 2014, 12306 sites included the information leak, result in more than 130000 users' personal information was made public, as well as on May 28, 2015, ctrip outage, lasted for up to 11 hours, setting a new record for the domestic Internet company system paralysis, this a series of events show that the data security no small matter, if do not take effective means to improve the security of data protection, the resulting loss is incalculable.

2.The big data age enterprise data security threats

Although now more and more enterprises begin to attach importance to the business data security protection work, data protection center of gravity has shifted from system and network infrastructure of protection and to focus on the key on the level of data protection. In spite of this, there are still some enterprise data security problem didn't get enough attention, therefore, the enterprise generally concerned about data security threats mainly has the following kinds:

2.1 Corporate leadership for data protection seriously, but the execution is not in place

Information security domain business leaders know the idea of "three seven technical management", but the resulting "a deployment nine points to carry out the" problem, is increasingly apparent, and has become the information security construction, especially the key and difficult point for data security management. Unfortunately, in practical work, the security requirements of execution does not reach the designated position is still quite common. Such as some enterprises in the process of independent development part of the application system, although can according to the internal overall safety strategy formulated the development standard, but will these specifications for a variety of reasons for which the split and refinement, lead to the developer in the development process is very difficult to put these requirements to the specific development process, it left a hidden danger to application system in the use of stage, and may lead to critical data leakage. This example also many, they are caused because of management implementation does not reach the designated position.

2.2 The emerging technology system framework, but data protection application abilities lag

As a product of the development of computer and Internet technology fusion, represented by cloud computing, Internet of things system of emerging technology is gradually being extended to the

application domain, and the model of the information technology industry has brought significant innovation, but do not underestimate the resulting data security challenges. Cloud services, for example, in April 2011, amazon cloud computing center in northern Virginia downtime, amazon cloud outages lasted nearly four days; In July 2012, the cloud storage service Dropbox, confirmed that the hackers stole some user information and affects their cloud service account.

2.3 The enterprise internal employee vandalism and carelessness

Internal attack is one of the greatest threats to data and system, employee is access to the network in the IT team, data center and special members of the management account, may cause serious damage. And staff visit unauthorized website or suspicious E-mail, click link to open the email attachment, also can give the company's system and data security threats.

2.4 Mobile devices (BYOD)

Employees use mobile devices to share data, access to company information, or ignore the change mobile phone password, at this moment the most prone to data theft. In fact, as more and more enterprises to accept BYOD, they face from enterprise risk of these devices on the network (behind the firewall, VPN) in the application to install malicious software or other Trojan software.

2.5 The third party service providers

As technology is becoming more and more specialized and complicated, the company is relying more on contractors and suppliers, support and maintenance system, however, the third party usually use remote access tools to connect to the company's network, but not always follow the security best practices. If an attacker to guess the password, he immediately through this connection network of these customers. According to recent reports, most data leakage (76%) were attributed to the supplier for the development of remote access channel.

3.Big data era development trend of data security

3.1 Data security is a new generation of information security system competitive high ground

In 2015, the data security has become a traditional information security companies and even other areas listed companies like most on the forehead, although the data security of alkaloids in refined into Rome was not built in a day can, but means that data security as the core of a new generation of information security has been widely accepted. In 2016, the label has posted good companies will be competing in the data security market, is trying to occupy the high ground of the new generation of information security system. The enterprise that has core technology accumulation and familiar with the user business will win in the competition.

3.2 Data security technology into the fusion intelligent era

Big data, cloud computing and mobile Internet technology put forward higher request to data security, data security protection from static to dynamic, from certainty to the demand of the intelligent transformation, prompting data security technology further development, the integration of machine learning, fast search, data interpretation, data encryption and the fusion of natural language understanding intelligent data security technology will gradually appear.

3.3 Push open sharing data security technology is widely used

When the data is sufficient cognitive value, after only in a data sharing environment can fully reflect the values of the data security. The government to promote economic context, open and sharing data will enable data liquidity increased significantly, also will promote data security technology be more widely used.

3.4 Data security becomes a new generation of information security standard basic content

The past few years, data security has been gradually incorporated into some industries in the specification, such as gm in 2016 level for the protection of data security in a new generation of national standard is expected to be included in the content, data security will become a new generation of the basic content of information security standards.

3.5 Data security to promote information security technology and application integration

Traditional information security technology is common architecture in the application system, and data security protection object - "data" are widespread in the application within the system, which

makes the data security has natural gene technology and application of fusion, data security technology is widely used to drive a new generation of information security technology and the application of fusion, gradually change the current "plugins" the status quo of information security technology.

4.Big data trigger data security guard measure

Data security can be divided into security and data security, data transmission in the network data interaction in big data, virtualization, cloud resources environment, how to ensure data security in the transmission, storage, ensure confidentiality has become a widely discussed issue. In this paper, using the following two measures for enterprise data security protection:

4.1 Raising the level of safety in site

(1) Website user authentication

General user name + password authentication, can be used to confirm the user login identity and according to the database default permissions, to show the corresponding to the user interface. For important site applications, need according to the mechanism of PKI authentication certificate provided by the user, thus the user identity authentication, non-repudiation and ensure the deal. Certificate provides two ways can be used documents: certificate or USB storage. Certificate file stored in the disk and file system, has the certain security risks, but you can free; USB certificate of high safety, but generally need to charge to the user.

(2) Site data encryption transmission

For online application system using a Web browser, using SSL + digital certificate, (namely the HTTPS protocol), to ensure that the communication data encryption transmission, also guarantee the client to the server side authentication at the same time, avoid the user is pretending to be legitimate websites "phishing" cheat, so as to disclose confidential information (user name and password, etc.), cause irreparable economic losses.

(3) User accounts using logging and auditing

System server shall be according to the account, the use of user behavior to carry on the detailed logging and auditing, through the above factors of logging, periodically audit (time interval should be smaller) and so do find user account theft, malicious use, etc., as soon as possible for processing.

(4) A malicious user detection, filtering and blocking traffic

System server should deploy IDS intrusion detection system, IPS intrusion protection system, firewall and other equipment or deployment of efficient, popular UTM device, to a malicious user USES the means of detection and protection, key filtering malicious flow, breaking flow, etc.

(5) Filtering and processing of abnormal application request

System of the server, database server, in particular, should increase the user through the configuration and application requests very filtering and processing module, in order to avoid the database patch their own vulnerability is not timely, the current epidemic of SQL injection attacks, etc.

(6) Disaster backup and recovery

Any system cannot say 100% of all security, need to be considered in the attack or backup restore to withstand natural disasters.

4.2 Developing a successful database security strategy

To develop a successful database security strategy is the key to why you have to know to protect the database, which protect the database, and how to best protect the data in response to all types of threats. Suggested that the enterprise according to the following three points to build complete database security strategy:

(1) To establish a set of authentication, authorization, access control, discovery, classification, and patch management, which integrates a solid foundation.

Know which databases contain sensitive data is the basic requirement of the database security strategy. Companies cope with all the database to a comprehensive inventory management, including

production and non-production, and follows the same security policy categories to them. All database, especially those who have private data of database, there should be a strong authentication, authorization and access control, even if the application has completed the authentication and authorization. Lack of these solid foundation can weaken the auditing and supervision, and encryption and other security measures.

In addition, if you can't patch every quarter to all the key database, so at least once half a year, to eliminate known vulnerabilities. Use rolling patch or from a database management system (DBMS) collect information of suppliers and other vendors, applying patches to minimize downtime. Always test security patches in the test environment, run the test script on a regular basis, to ensure that the patch does not affect the application functionality or performance.

(2) Using a data block, encryption, and change management, and other functions of preventive measures

In the setting up of a solid and basic database security policy, should start to take preventive measures, in order to protect the important database. Thus for production and non-production database provides a protective layer. Data privacy as a production system and not stop, it also needs to be extended to the non-production environments, including testing, development, quality assurance (QA), and training by stages, basically all private data can reside. The database security professionals should be evaluated in the test environment or outsourcing application development using data block and the effect of test data generation to protect private data.

Use network data encryption to prevent exposure to monitor network traffic or the person peep static data encryption (they pay attention to data stored in the database). When the data according to different threats, the encryption method can realize mutual independence. Normally, also won't affect the function of the application.

Protection of key database structure to according to the standardized change management program. In the past, to make changes in production plans, or other database need to be closed when the database, but the new version of the database management system allows for these changes when online, it brings new security risks. A standardized change management procedures to ensure that only the administrator after approved by management department to change the production database and track all changes to the database. Institutions should also update their backup and feasibility of the plan, to process the data or metadata changes due to these changes.

(3) Set up which has the function of auditing, monitoring and vulnerability assessment database intrusion detection system

When important data accident changes or detected suspicious data, there is a need to make a quick survey to see what had happened. Data and metadata can be accessed in the database, change, and even to delete, and these can be finished in a few seconds of time. Through the database audit, we can find "who changed the data" and "when the data was changed. In order to support the aforementioned management regulations, standards, safety and risk management professionals should track all access to private data and change situation, these private data include: credit card Numbers, social security number kaka and important information such as the database name and address. If private data without authorization changes or accessed, institutions should be the responsibility of the director. Finally, you can use the vulnerability assessment to determine the open area in the security of database, such as weak passwords, too much priority access, increase the database administrator group, and security monitoring.

5.Conclusion

In brief, under the environment of big data, data security problem has become the enterprise itself can be in an impregnable position in the competition in the business of a decision factors, so it is necessary for data security protection strategy to further strengthen, as far as possible to find more good way to ensure the safety of enterprise data.

References:

[1] Yong-di Mi . Human factors in data security. Beijing: Library and Information Service. 2006.03

[2] Xiang-xiang Meng . Small and medium-sized enterprise data security management solutions. Sichuan: Journal of University of Electronic Science and Technology of China. 2009. S1

[3] Zhuang-hong Zhang. The organization's disaster data security and backup. Shanxi: Friends of Accounting. 2009.02

[4] Deng-guo feng. Big data security and privacy protection. Beijing: Chinese Journal of Computers. 2014.01

[5] Yun-chang Sang. Big data security present situation and countermeasure research. Chongqing: computer science. 2015. S2

[6] Chao-sheng Feng. Cloud data storage technology. Beijing: Chinese Journal of Computers. 2015.01

[7] Zuo-ning Chen. Big data security and independently controllable. Beijing: Chinese Science Bulletin. 2015. Z1

[8] Zhi-ying wang. Small and medium-sized enterprise cloud computing data security risks associated effect research. Sichuan: computer application research. 2015.06

[9] Mao-yue Zhang. Big data era new threats of personal information data security and protection. Beijing: China science and technology BBS. 2015.07