RESEARCH REVIEW JOURNALS
Volume-05
Issue-07
July-2020

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[Peer Reviewed Journal]
DOI: https://doi.org/10.31305/rrijm.2020.v05.i07.002

Data Security Solutions

Vincent Xu

Graduate Student, University of California – Riverside, CA, USA

ARTICLE DETAILS

Article History
Published Online: 15 July 2020

Keywords
Data security, Solutions, Cybersecurity, data protection.

***Corresponding Author**
Email: vincexu0[at]gmail.com

ABSTRACT

The data collected and accumulated within a company is a real treasure much more precious than you could imagine. It is a veritable bank of information and knowledge that allows the company to progress and grow little by little. It would be a real tragedy if important content were to disappear, be altered or be visible to malicious people. If the data were lost, you would have to practically start from scratch to find most of the important information. This article will explain two parts in terms of protection and backup for maximum secure data[1].

1. Introduction

Just as the world of cyber security is moving forward, technological advances are attracting more and more hackers and cybercriminals looking for security vulnerabilities to exploit to steal your data. Internet users and businesses are concerned - and rightly so - about the steady increase in the number of cyber security attacks. The assault on the Want toCry ran same ware illustrates the growing scope of these types of attacks –Want toCry has been one of the most significant in recent years, both in scale and in the number of businesses affected worldwide. Hence the question: "How is it that small and large companies were affected and affected by this attack?". A real awareness is emerging on the importance of strengthening security measures.

2. The risks the data faces [2]

The main dangers of poor security are data loss, accessing data from people who shouldn't, and data corruption. Regarding data loss, which is much more common than you might think, here are some typical cases that could happen:

- Hard drive crash or miscellaneous failure
- Improper handling
- Computer attack
- Theft of computer equipment
- Virus
- Fire / flood

Unfortunately, we tend to believe that these phenomena only happen to others. But it only takes one time to radically change your mind about it. Imagine the time wasted and the impact on the image of the company if a customer database were to disappear. Likewise, imagine what could happen to you if a competitor had access to your detailed financial reports.

3. Data security solution [3]

It must be understood that not all data are created equal. Faced with the dilemma between risk and cost, many companies do little or nothing, they save money but increase their risk exposure, when others overinvest and overprotect themselves, eliminating the risk but bearing excessive costs. The right strategy is to classify the data according to its importance and degree of sensitivity for the company and to deploy a solution adapted to the situation of the company, in terms of cost vis-à-vis the risk. Here are some considerations that partners should consider to help customers adopt the right solution that guarantees the right degree of data protection:

4. Data protection [4]

4.1. Limit access to data

Most companies grant privileged access to certain employees and internal collaborators to access their sensitive data. Do you know who in your company has access to sensitive customer data? Are you able to identify each person's access rights? Most executives do not know in detail that has access to the data and for what reason - which represents a huge risk of loss, theft and hacking of your data.

It is important for companies to limit access to their data. They must determine the data to which this or that employee can access and ensure that they can only access what is strictly necessary. Applying these restrictions would allow companies to manage their data more efficiently and protect themselves from theft or loss of data.

4.2. Identify sensitive data

Businesses need to know where their strategic data and sensitive information are located. This allows them to rely on accurate information to allocate additional resources to protect the most sensitive and crucial resources for them.

Even if sensitive data should only represent between 5 and 10% of your company's total data volume, even the smallest breach of these types of data can have huge repercussions in terms of image and turnover. But back to access management and access rights. Sensitive data should ideally be subject to more stringent protection measures than other corporate data.

4.3. Plan your data security policy in advance

Now let's look at the actions and processes to put in place to limit cyber attacks. With this type of plan, the company will be able to intervene more quickly in the event of a critical problem and incident. The rules allow you to react immediately to prevent the most devastating consequences of a cyber-attack.

Access management and access rights make it easy to identify your employees' access settings, so you can spot potentially compromised user accounts. Never forget that safety rules and plans will only be effective when they are last revised. Technologies, sectoral regulations, and good practices are constantly changing. You need someone responsible for these rules and processes who are constantly looking for new ways to update them to ensure their relevance.

4.4. Use strong and separate passwords for each department

Sensitive company data should be locked and protected with strong passwords. Strengthening passwords is essential to protect against the tools used to crack passwords - tools that are otherwise easy to obtain on the market. A strong password will combine several characters, upper- and lower-case letters, numbers, and symbols.

It is also dangerous to use the same passwords for multiple accesses and programs. Once your password is hacked, hackers will quickly reuse it on your other user accounts.

Companies must ensure that there is a unique password for each employee and each department. To simplify the task, companies can use password management tools. They will also ensure that all of their employees are properly trained in data security and receive advice on the use and creation of passwords.

It is also recommended to set up, where possible, a multi-factor authentication system. Each additional step in the password login process is one more step for hackers to take - making hacking even more difficult. Biometrics, sending notifications to smartphones, authentication to SmartCard and other tokens are all examples of high-performance multi-factor authentication.

4.5. Update and back up your data regularly

Security checks and regular data backups are the latest key security measures to protect data. Thus, in the event of an improper attack or breach of data, the company will appreciate having backed up its data. For the sustainability of your business, make it a habit to perform manual or automatic data backups every week or every day.

To properly protect your data, your software should be updated regularly, and you should use good antivirus software. Your IT department must be at the forefront and proactive. Hire reliable and competent collaborators to carry out their mission seriously.

4.6. Data encryption a key step in IT security

Encryption, or encryption, guarantees the inviolability, integrity and authenticity of data during storage and transmission. Asymmetric cryptography, using a public key for encryption and a private key for decryption, offers more advantages than symmetric cryptography, which encrypts and decrypts with the same key.

5. Backup data [5]

The previous recommendations are mainly used to prevent the danger, it is still necessary to provide a backup system to prepare for the worst-case scenario. These backups should be done fairly regularly. To know the right backup frequency, ask yourself the equivalent of time that you would be ready to waste: 24h, 1 week, 2 weeks or even 1 month?

Several options are available to you regarding the backup method:

- External hard drive: simple to manage, just plug in the external hard drive and transfer the data to be saved. With a large capacity, the backup of several computer stations can be managed at the same time. Small tip: IT tools can automate the backup process.
- USB key: similar to the hard disk, with the difference that the key is smaller and of lower capacity. It is more practical to provide a backup USB key for each computer station. It is also more practical to store the USB keys in a safe for example.
- Burning to a CD / DVD: a little more restrictive since writing to the CD can take a little more time than copying / pasting files on a USB key. You have to think about choosing rewritable CDs / DVDs to be able to overwrite the data from the previous backup and avoid spending a fortune on CDs.
- Computer dedicated to backups: economical method which consists in recycling an old computer to save the data. This "D system" limits the purchase of new equipment. In addition, this computer can be connected to the corporate network so that each employee can transfer their backups there whenever they want.
- Backup server / private cloud: potentially somewhat technical, a server can be used to retrieve backups in the same way as a computer dedicated to backups. Some systems improve and facilitate data synchronization. The main advantage is that the server can be located outside the company with a dedicated host. This ensures data is secure even in the event of a fire, flood, or burglary.
- Software in SaaS mode: some solutions such as Dropbox or Google Drive allow a real archiving and recording service in the cloud through a specific user space. Again, the advantage is that the data is hosted outside the company. The other positive point is that these SaaS software are not only intended to serve as backup, they are also powerful tools to give access to a resource to all employees and to facilitate access to the resources of the business from any medium (Windows computer, Mac, Linux, Tablet, Android smartphone, iOS smartphone, etc.).

NOTE: In the case of a physical backup medium (external hard drive, USB keys, CD / DVD ...), it must be able to be stored in a safe place, outside the company. A safe located at the company will not protect these supports if there is a fire in the premises. You also must be careful that one of the backups does not disappear. Without daily monitoring, it is too easy for a malicious collaborator to steal a USB key containing confidential information. Even if the USB stick is brought back the next day, it will have had time to be copied.

6. Being able to save everything

Digital archiving isn't just about the simple files you have on your computer. There are other resources to consider:

- Emails: there are solutions to save emails. Find out according to the solution you have adopted concerning the management of your emails.
- Business software: some software stores information in a format that only software can read. Learn more about export functionality and how software stores data.
- Unique reports available in paper format: scanning all the paper sheets would dematerialize the information but would require an imposing time. Making a photocopy would be expensive and not environmentally friendly. It might be advisable to modify the working method, for example by using an application on a smartphone or touch pad.
- Photos: a digital camera is sometimes used to take a photo of construction sites. It's a good idea to use a digital device or smartphone with a Wi-Fi connection to easily sync photos. A smartphone can even use an application that will save photos to the cloud automatically.

7. Conclusion

Finally, it is important to end on a slightly more reassuring aspect than the whole of this article. It should not be forgotten that unfortunate situations are rare. Foresight is good, but you must keep a cool head and keep spending most of your time thinking about protecting yourself. So, remember to predict the worst, but to automate as many things as possible.

There is no minimum size to be interested in IT security and data protection. It is very complicated to restart an activity when the data has been stolen, destroyed, or encrypted. It is never too late to set up data governance and a security policy.

References

[1]. Raphaël Gellert. Understanding Data Protection As Risk Internet Journal of Law Regulation. in 18(11):3-15 · May 2015

[2]. Kumar, P. Ravi, P. Herbert Raj, and P. Jelciana. "Exploring data security issues and solutions in cloud computing." *Procedia Computer Science* 125 (2018): 691-697.

[3]. Sunil Ladekar.Best Practices for Information Security Breach Management. Thesis for: MS in Network Technology, Advisor: Phil Lunsford. July 2014

[4]. Bomar, Kevin B., and Glenn E. Harper. "Tokenized data security." U.S. Patent No. 10,262,128. 16 Apr. 2019.

[5]. Yining Liu, Qi Zhong, Liang Chang, Secure Data Backup Scheme Using Zhe Xia, Debiao He, Chi Cheng.A IET Information Multi-Factor Authentication. in Security 11(5). November 2016, DOI: 10.1049/iet-ifs.2016.0103

[6]. Sarmah, S.: Database Security – threats and prevention. IJCTT **67**(5), 46–50 (2019)

[7]. Redlich, Ron M., and Martin A. Nemzow. "Data security system and method with editor." U.S. Patent No. 8,176,563. 8 May 2012.

[8]. Industry, Payment Card. "Data security standard." *Requirements and Security Assessment version* 3 (2018).

[9]. Leiss, Ernst L. *Principles of Data Security*. Springer Science & Business Media, 2012.

[10]. Okuhara, Masayuki, Tetsuo Shiozaki, and Takuya Suzuki. "Security architecture for cloud computing." *Fujitsu Sci. Tech. J* 46.4 (2010): 397-402.

