Advances in Health Science Research, volume 6
2nd Sari Mulia International Conference on Health and Sciences (SMICHS 2017)

The Importance Of Securing Digital Data

Muhammad Zulfadhilah[1*]
[1] Sari Mulia School of Health Sciences, Banjarmasin Indonesia
muhammadzulfadhilah@stikessarimulia.ac.id

ABSTRACT

Objective: To awareness in securing digital data either offline or online.
Technology or Method: Based on literature studies that have been done, the increase in Internet users is not comparable with increased awareness of data security or information by users, which causes vulnerability to users of losing their data.
Result: This paper will provide recommendations for securing data, which is cryptographic techniques and steganography. Cryptography is an art or science of keeping data or message security, while steganography is the science of hiding messages or data into a media. Users in performing data security can use these techniques, data security applications are already widely provided by developers of data security. Regular change of passwords in various accounts on Internet services is also one of the ways to secure accounts and data stored on Internet services.
Conclusion: Based on the recommendation by the Internet users can minimize the theft or destruction of digital data by cyber criminals.

Keyword: Cryptography,Cybercrime, Digital Data, Internet, Security, Steganography.

I. INTRODUCTION

The Internet has become a necessity in today's society; any information is accessible on the internet via web browser. However, these activities could have an impact on users, one of which changes in behavior (1). Assessment of user behavior is often only based on interaction across the Internet without knowing any others activities [2].

The development of computer systems and their interconnections through multimedia networks has increased. Currently installed computer systems are more accessible, one of the weaknesses of data communication is time sharing and remote access. In the era of universal electronic connectivity often there are disruptions in the form of hackers, viruses, electronic fraud as well as hear silently electronically. Data security is really a very important problem, so it needs a computer network system with a security level that can be guaranteed and can be protected from attack (attack), although in the end there will be a tradeoff between the level of security and ease of access [3].

Security of information in the Internet era is very important, because the internet network is connected anywhere in the world and public (public property), it can be said internet network is very unsafe, like a car carry passengers (information) passing on the

highway, anytime The car can turn or get hit by another car on the highway [4].

One recent example of a *WannaCry* Ransomware malware attack that locks the files invades the victim's computer by locking the victim's computer or encrypting all the files so they cannot be accessed again. Ransomware of this type of targeting Windows-based PCs that have weaknesses related to the function of SMB (Server Message Block) run on the computer [5].

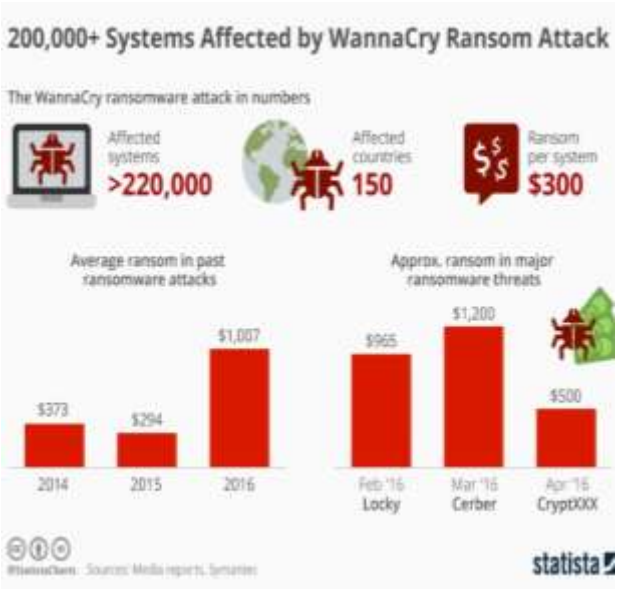


Figure 1 System Affected by WannaCry Ransom Attack

The security of data on the laptop or external hard drive, which is often carried away may be lost or stolen, if this happens the first thought is the data contained in the storage memory even though the data already has a back-up but the data and important files it becomes Main thought, especially the stored data is confidential or private [6].

According to [7] for reduce or mitigate the increasing number of crime incidents in cyberspace, it is necessary to consider the root cause first. From the various opinions and approaches, there are three kinds of business aspects to overcome them, i.e. each viewed from the technical, business, and social side.

In this paper will be given some recommendations in performing data security, it is expected that this recommendation minimizes data loss due to hacking, cracking, or stealing activities. In addition, it is expected that digital data stored offline or online can more secure than piercing by doing some security techniques.

II. METHODS

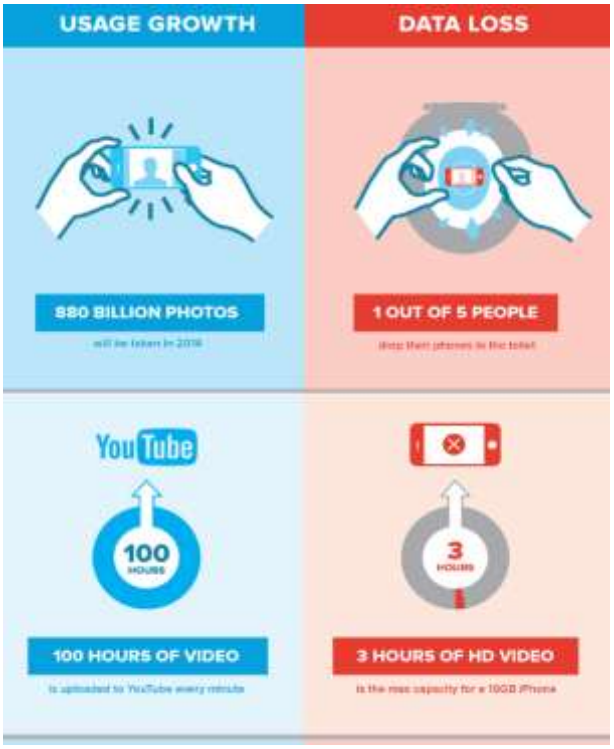
This paper was written based on the literature review according to some research on data security. In this section will present some research on data security along with recommended recommendations in securing data either online or offline. The author tries to present the literature review based on recent research on data security.

The use of computers in various fields brings rapid development to a hardware or software, even in the field of information development continues and this gives a great influence on human life [6]. In research conducted by [3] states that to secure data on the network required cryptography by encryption method. According to the International Telecommunication Union, there are two billion telephone subscribers and 1.4 billion cellular subscribers in the Asia Pacific region. India and China alone take a quarter of the world's mobile phone users by mid-2008.

The Asia Pacific region also represents 40 percent of Internet users and is the largest broadband market in the world with 39 percent of the world's total [8]. According to [9] the Internet in Indonesia currently reaches 63 million people, of that number, 95 % use the internet to access social networking.

Refers to Imran's research stating that online storage service providers apply several layers of security systems, namely the use of CAPTCHA, log records, security questions, data backup, firewall and antivirus, file access restrictions, data encryption and network connections, DdoS protection, patches and periodic updates, services 24 hours and security offline [10]. This is done so that the integrity of the service provider to the security of customer data to be well maintained.

Based on information gleaned from one of the harddisk manufacturer companies, digital users should always backup their digital data.



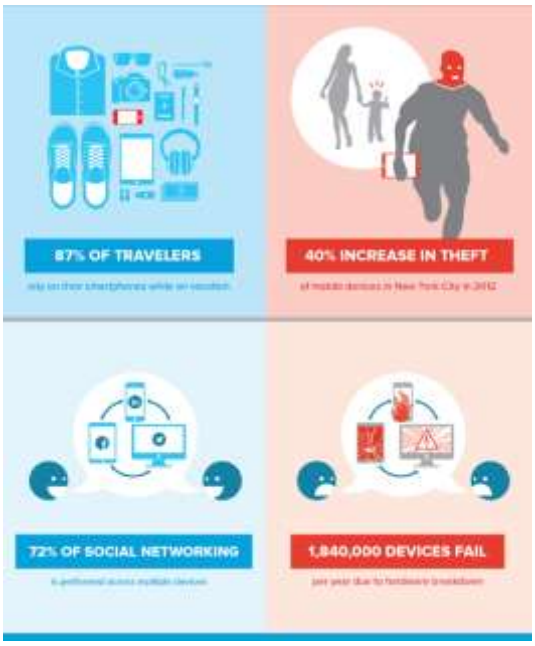


Figure 2 Infograpich digital data

In research conducted by Amin [8]mentioned that information security is needed to confidentiality (integrity) and availability (availability) of information is maintained so as not to disrupt the performance and operational organization. This is in line with the research conducted by Ihwani [11] which states that the confidentiality and security of data are of paramount importance. One of the jobs that will help information technology, that is work in hiding message [12].

In research conducted by Indriyono [13] mentions that cryptography is a science and art that is used to maintain data confidentiality, while steganography mentioned in research by Rifai [12] mentions that steganography is a science and art of hiding, steganography requires two properties where hide and message to be hidden.

In a paper published by Network C [14] mentions that there are 5 ways to secure from

hacker attacks, namely Assume a breach will happen, focus on breach containment, Adopt an app- and user-centric security policy, Extend security across all silos and Use cryptographic segmentation and isolation to protect applications.

In the research conducted by Edwards [15] states that the level of user awareness of the security does not affect the behavior of the user, but it is one of the self-achievement of data security. Because it is not the user's security consciousness that counts, but the perceived level of threat that becomes a consideration in decision-making against existing threats.

III. RESULT & DISCUSSION

Based on the above literature study, there are some recommendations that can be done by Internet users in doing digital data security. The recommendation is to use cryptographic techniques that allow our data more secure than internet theft, this technique itself has several algorithms in its application. Algorithms used in cryptographic techniques tailored to the needs and development of the world of digital security. Digital Signature Algorithm (DSA) is one of the most widely used algorithms, the use of this algorithm is used to prevent digital message forgery [11]. Furthermore, by using steganography techniques that are also effective in securing data, steganography more focused on data hiding in a file, this is to trick unscrupulous people who want to retrieve user data without permission. In addition to these techniques in the security of digital data, there are some techniques that are easy but often ignored, i.e. regular file backups on various storage media, and also if we have an account on the Internet should do regular change the password. Recommendations that have been described is expected to be a reference in the process of securing data either online or offline. This paper has many shortcomings in the presentation of its contents, because it is only based on literature study. Hopefully in the future, the authors' contribution to this paper is better by doing more in-depth research on data security on the Internet.

IV. CONCLUSION:

Based on literature studies that have been done, then there are some suggestions in doing data security either online or offline, that is by using cryptography and steganogram techniques, backup files on various storage media, and change of password periodically on the account of Internet service used. Improving the user's knowledge on the level of risk faced, the more days the level of risk is always increasing in proportion to the increased security that exists in this digital age. it is prepared to know what needs to be prepared in the face of existing security threats.

REFERENCES

[1]. Zulfadhilah M, Riadi I, Prayudi Y. Log Classification using K-Means Clustering for Identify Internet User Behaviors. Int J Comput Apl [Internet]. 2016;154(3):34–9. Available from: http://www.ijcaonline.org/archives/volume154/number3/26475-2016912076

[2]. Zulfadhilah M, Prayudi Y, Riadi I. Cyber Profiling using Log Analysis and K-Means Clustering A Case Study Higher Education in Indonesia. Int J Adv Res Comput Sci Appl [Internet]. 2016;7(7):430–5. Available from: www.ijacsa.thesai.org

[3]. Kurniawan A, Yuliana M, Hadi MZS. Analisa Dan Implementasi Sistem Keamanan Data Dengan Menggunakan Metode Enkripsi Algoritma Rc-5. 2010;1–6.

[4]. Mantra I. Keamanan Informasi Digital di Era Internet. 2013;

[5]. Kominfo. SIARAN PERS KEMENTERIAN KOMUNIKASI DAN INFORMATIKA NO. 56/HM/KOMINFO/05/2017 [Internet]. Kementerian Komunikasi dan Informatika Republik Indonesia. 2017. Available from: https://kominfo.go.id/content/detail/9637/siaran-pers-no-56hmkominfo052017-tentang-antisipasi-terhadap-ancaman-malware-ransomware-jenis-wannacry/0/siaran_pers

[6]. Krisna Prastyo A. Pengamanan Data dengan Metode Advanced Encryption Standard dan Metode Least Significant Bit. 2011;1:9. Available from: http://eprints.dinus.ac.id/13558/1/jurnal_14251.pdf

[7]. Indrajit RE. Meneropong Isu Keamanan Internet. 2009;

[8]. Amin M. Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan MCDA. 2014;5(1):15–25.

[9]. Kominfo. Pengguna Internet di Indonesia 63 Juta Orang [Internet]. 2013. Available from: https://kominfo.go.id/index.php/content/detail/3415/Kominfo+%3A+Pengguna+Internet+di+Indonesia+63+Juta+Orang/0/berita_satker

[10]. Imran S. Sistem Keamanan pada Penyimpanan File Online untuk Menjaga Keamanan dan Kerahasiaan File dan Data Pengguna [Internet]. 2014. Available from: http://ipankint.com/internet/sistem-keamanan-penyimpanan-file-online/

[11]. Ihwani M. Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma Rsa. CESSJournal Comput Eng Syst Sci. 2016;1(1):15–20.

[12]. Rifai Z, Huda S. Aplikasi Pengamanan Data Email. TechnoCom. 2013;Vol. 12(No. 2):73–81.

[13]. Indriyono BV. Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher. Junal Sisfo. 2016;6(1):1–16.

[14]. Network C. 5 ways retailers can keep data safe from hackers [Internet]. 2016. Available from: https://certesnetworks.com/5-ways-retailers-can-keep-data-safe-from-hackers-infographic/

[15]. Edwards K. Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users. 2015;(947). Available from: http://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1949&context=gscis_etd