MBIE/PGBIE2201-8151
Information Security Management

Explore the importance of a Password Management Procedure in an Organization to ensure Information Security Management

Name : Hemal Samaranayake
Student ID : 105123

Table of Contents

Content **Page No.**

1.0 Introduction

Password is an important aspect in terms of information security. It is a front line of protection for user accounts, applications, data base, network and websites (Kruger, Steyn, Dawn Medlin & Drevin, 2008). The maintenance of high standard in creating and using a password with maximum security and minimizes the risk of miss use and compromise in day today processing.

The password management procedure is applicable for all the employees including contractors and third parties with access to any business application and technology, to be treated as strict confidential (Kuka & Bahiti, 2018).

2.0 Literature Review

2.1 Evaluate Password Management Procedure in an Organization in terms of Information Security Management aspects and impacts

In the presence of incremental transactions on e-commerce and heavy usage on multiple platforms and applications using a weak password has identified with a great vulnarability for maintaining a sound information security environment, in the current business contents. A strong password is recommended to consist of secured length and time, including multiple special characters, upper and lower characters and alpha numeric, assuring an inbuilt nature to avoid the password been cracked by hackers, unauthorized observance and fraudulent initiators (Weber, Guster, Safonov & Schmidt, 2008).

Besides the fact that a weak password is identified in the user practice with some dictionary words, names and personal data with features of easy guessable and predictable enabling an unauthorized person to misuse. Further studyreveals that a sound password policy document should be existence in an organization where the users can read as a guidance enabling to have a competent idea of user disciplinary and compliance to the organization's best practice. This policy needs to be clear, specific and possess an ownership and the same need to be

periodically reviewed in terms of business requirement and mainly focusing on information security aspects (Shen, Yu, Xu, Yang & Guan, 2016).

Multi factor authentication (MFA) is an advance and innovatively secured method of protecting the legitimate user from unauthorized access by way of requiring users to provide two or more verification factors to gain access to their accounts. Also there are different factors to ensure the high security matrix. Such as using a password/Personal Identification Number/One Time Password as knowledge factor, possessing factor being considered as using a Smart card and inherence factor including face recognition, Fingerprint and voice recognition. In combination of the above three factors, the greater the combination leads greater secured access to the system (Dipankar, Arunava Roy, Abhijit Nag,2017).

The habitual pattern of users to login with the same password when they are required to give access to multiple exposing with high risk since if the password is tracked there can be high possibilities and unauthorized user can login to the systems and cause a high inherent security risk.Further high tendency is revealed to save the password for user convenience. In terms of default administrator passwords of all systems (applications, servers, routers, switches and firewalls) need to be kept under the custody of the IT security officer for retrieval. Passwords should not be embedded in auto programs, utilities or applications such as “auto exe.bat” file, batch job files, terminal hot keys etc. Further an account lockout and session management strategy need to define for all information systems through documentary evidence (Butler & Butler, 2018)

Organizations need to heavily invest their funding reserves to protect the systems from password hackers. However the ultimate investment perspectives towards the system integrations are noted to be seen that the user behavior and their inefficient and irresponsible attitudes makes the investment unproductive due to mismanagement, privacy concerns by

sharing the password among coworkers, family friends (Tam, Glassman & Vandenwauver, 2010).

Usage of graphical passwords is an alternate and a solution to avoid an unsecured exposure when using the traditional user name and password authentication. The scope of this can be categorized in to three main proceedings namely,

- Click based
- Choice based
- Draw based

The process is been initiating the controls the choice of images through a automation platform by enhancing the performance in terms of usability and security (Jali, Furnell & Dowland, 2014).

Compromising passwords by employees, expose the organization with great unsecured status. Identifying high user sensitive passwords could be protected by giving the appropriate level of access to perform the user functionalities. Subsequent to the identification of each password can be reset automatically and bring the control aspects immediately. This process will enhance the required privileges when performing their functions (Ganesan, 2016).

2.2 Evaluating the standards related to Information security – ISO 27001

Password length is to be retained with 8 characters as per NIST – 800 standards without an expiry when the same is initiated by a user. And the same to be included in the policy but without mentioning the strength aspect. As per ISO 27001 standards it is specified that it needs to use a relatively strong cryptographic methods for sufficient transmitting password information. ISO 27001 states that organization must have access control policies with protected logon methods along with password management system. As per NIST – 800 the defined password length should be minimum 8 characters if it is a user initiated password and if the same is credential service provider, generated password, then it needs minimum 6

characters. All default passwords need them to be prior registered on the networks as per NIST – 800 standards. (Vorster, Irwin & Van Heerden, 2022)

2.3 Evaluating the process through National Institute of Standards and Technology NIST 800 for password management

NIST document is developed in statutory responsibilities under the federal information security management act; organization wise risk based approach is elaborated to ensure secured password management process governing with a password management policy document to be in place in the organization. The policy document needs to have an administrative ownership with the characteristics of clear, understandable with guidelines to maintain high standards password handling formalities. In event of major changes in system innovations or implications this document needs to be revised accordingly to ensure the users are competent to handle access in the systems with confidentiality, reliability and with accountability. A high secured password will ensure no cracking access by unauthorized users and prevent the data base, network, software and hardware. Sharing and compromising of passwords, writing passwords while exposing to other staff, saving passwords in desktop and notepads, discussing password in public and shoulder surfing is highly recommended to avoid ensuring high disciplinary staff maintenance and following ethics and practices in a secured office environment (Scarfone & Souppaya, 2009).

3.0 Task 2 – Cyber attack on Hospital and the Implementations taken in according to the given standard.

The South Eastern Norway regional Health Atuthourity is a state owned regional specific organization of specialized hosptals healthcare services created in 2002. They announced that in January 2018 the protected health information and records approximately 2.9 million of population had been compromised and organized criminal group from foreign spy or state agency initiated the attack focasing the patient health data and Norway's armed forces details. The weakness is believed to initiated from legacy system, windows XP. This organization as initiated security controls to mitigate the risk brought by Windows XP along with strategies to encounter it, but attack was created before they could placing the security measures. While this attack did not seem to pose risk to patient saftety or disterbing in hospital operations, this incident trigered about future attacks on health data for the purpose of political gain and alert for future exposure (Argaw et al., 2020).

As per the Health Insurance Portability Accountability Act (HIPAA);2007 electronic protected health care inofrmation is to maintain privacy standards and prevent sharing medical inofrmation with other entities in order to avoid and safe guard information in internal data base during the data transmission to be extra vigillent (Sirilla, Copelan, Elder & Davis, 2006).

Further in this act focusing on digital base approaches such as online counselling need to be maintain the confidentiality and privacy. In terms of ethic codes to be maintain as per American Counsiling Association (ACA), the guidence is given to maintain records in a secured location granting access only by dedicated persons. Data storage and retrieval in an encrypted backup in terms of disaster recovery plan to protect loss data in an additional secured location should be implemented. Further mail communications and video conferencing need to be in secured and clinical matters should be encrypted before electronic transmission (Lawley, 2012).

Further interms of health information technology for economic and clinical health (HITECH) needed to have a mechanism as a plan to be given notice with regard to affected clients in a case of breach, exposing electronic information and take to the notice of the secretary of Health and Human servies exceeding 500 clients. In this standard it is requested medical service professionals to encript all local data and advice the councellor to initiate a policy in respect to give nocifications to clients of loss of encrypted data. It is evident that care receivers are heavily relying and depending on smart phones and mobile applications in order to link with the clinical activities of medical service provider, In this case study of the South Eastern Norway regional Health Atuthourity. As a result clients need to be educated at the point of service registration to ensure the devices are protected secured user login (Lawley, 2012).

A clear policy guideline needs to be in place, documenting the practices and procedures including industrially accepted standards to fall in line for the effective and efficient rooting work. The accountability, reliability and proper medical code of conducts should be updated accordingly to fulfill the risk base approach.

In this case study, if the authority had maintained medical records including historical health records of care receivers separately from the current counseling in an expanded protected manner the risk would have been minimized in a greater extend. In the current context we experience there is a high tendency for online counsiling been falling in line innovatively for the convenience of treatments and concultations. When it is critically reviewed we realized that the above concept is not legistically covered by the HIPAA and HITECH acts. Hence the authority should have had an awareness of the abive limitations and develop a internal procedure for date storage and transmission with encripted matrix.

References

Agrawal, V., Paliwal, R., Sharma, P., & Shrivastava, A. (2019). Web Security Using User Authentication Methodologies: CAPTCHA, OTP and User Behavior Authentication. doi: 10.2139/ssrn.3360306

Argaw, S., Troncoso-Pastoriza, J., Lacey, D., Florin, M., Calcavecchia, F., & Anderson, D. et al. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics And Decision Making*, *20*(1). doi: 10.1186/s12911-020-01161-7

Butler, R., & Butler, M. (2018). Some password users are more equal than others: Towards customization of online security initiatives. *South African Journal of Information Management*, *20*(1). doi: 10.4102/sajim.v20i1.920

Dasgupta, D., Roy, A., & Nag, A. (2017). *Advances in user authentication*. Cham, Switzerland: Springer International Publishing.

Feldkamp, J. (2009). HITECH HIPAA Ahead: Proceed With Caution. *Caring For The Ages*, *10*(11), 12. doi: 10.1016/s1526-4114(09)60297-3

Ganesan, R. (2016). Stepping up security with password management control. *Network Security*, *2016*(2), 18-19. doi: 10.1016/s1353-4858(16)30019-8

Golla, M., & Dürmuth, M. (2018). On the Accuracy of Password Strength Meters. *Proceedings Of The 2018 ACM SIGSAC Conference On Computer And Communications Security*. doi: 10.1145/3243734.3243769

Jali, M., Furnell, S., & Dowland, P. (2014). Investigating the Viability of Multifactor Graphical Passwords for User Authentication. *Information Security Journal: A Global Perspective*, *23*(1-2), 10-21. doi: 10.1080/19393555.2014.891274

Kuka, E., & Bahiti, R. (2018). Information Security Management: Password Security Issues. *Academic Journal Of Interdisciplinary Studies*, *7*(2), 43-47. doi: 10.2478/ajis-2018-0045

Lawley, J. (2012). HIPAA, HITECH and the Practicing Counselor: Electronic Records and Practice Guidelines. *The Professional Counselor*, *2*(3), 192-200. doi: 10.15241/jsl.2.3.192.

Scarfone, K., Souppaya, M., (2009). Guide to Enterprise Password Management. NIST National Institute of Standards and Technology special publication; U.S. Department of Commerce

Sihwi, S., Andriyanto, F., & Anggrainingsih, R. (2016). An expert system for risk assessment of information system security based on ISO 27002. *2016 IEEE International Conference On Knowledge Engineering And Applications (ICKEA)*. doi: 10.1109/ickea.2016.7802992

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers &Amp; Security*, *61*, 130-141. doi: 10.1016/j.cose.2016.05.007

Sirilla, J., Copelan, E., Elder, P., & Davis, R. (2006). Creation of a research database to comply with the HIPPA Privacy Act. *Biology Of Blood And Marrow Transplantation*, *12*(2), 149. doi: 10.1016/j.bbmt.2005.11.459

Somepalli, S., Tangella, S., & Yalamanchili, S. (2020). Information Security Management. *HOLISTICA – Journal Of Business And Public Administration*, *11*(2), 1-16. doi: 10.2478/hjbpa-2020-0015

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour &Amp; Information Technology*, *29*(3), 233-244. doi: 10.1080/01449290903121386

Varshney, M., Shrivastava, A., Aggarwal, A., & Kumar, A. (2018). Cyber Security through Password Management Strategies. *International Journal Of Computer Sciences And Engineering*, *6*(12), 919-923. doi: 10.26438/ijcse/v6i12.919923

Vorster, J., Irwin, B., & Van Heerden, R. (2022). Violations of good security practices in graphical passwords schemes: Enterprise constraints on scheme-design. Retrieved 12 April 2022, from http://hdl.handle.net/10204/10919

Weber, J., Guster, D., Safonov, P., & Schmidt, M. (2008). Weak Password Security: An Empirical Study. *Information Security Journal: A Global Perspective*, *17*(1), 45-54. doi: 10.1080/10658980701824432