Mitigating corporate information exposure on the web.

Introduction

With data growing exponentially every year (Raschke & Mann, 2017, p.58), Implementing security measures regularly is vital (Keegan, 2017, p.16). Three important areas in data security are: (a) protecting the data from unauthorised access, (b) protecting the system from unauthorised access and, (c) ensuring that there are no single points of failure (Ruivo, Santos, & Oliveira, 2014, p.712-714). What is the single most important factor in the securing of sensitive data?

Protecting data

Corporate information systems have experienced increased attacks which result in the leaking of sensitive data (Ferreira & Vargas, 2015, p.2077). In particular, hackers bypass security systems by exploiting vulnerabilities in storage systems (Poh et al., 2017, p.1). Therefore, securing data is considered a significant component in the reduction of corporate damage after a ‘breach’.

By law, all personal data stored must be secured in accordance with the Data Protection Act 1998 (2015). For some, "Encryption has been adopted as a possible solution" (Boonkrong & Somboonpattanakit, 2016, p.28). However, the situation is complex. Consider the reversible ciphertext method for storing data, which uses different ‘keys' to encrypt information and protect against unauthorised access. According to Boonkrong & Somboonpattanakit (2016, p.28), this is often poorly executed as the key is usually stored in the same database. Another vulnerability is highlighted by Iyer, Sedamkar, & Gupta (2016) where they show that symmetric encryption is often too simple. They suggest, as computational power is becoming more prevalent, it has become more feasible to decrypt files using standard ‘brute force' algorithms much faster than was previously possible. This raises further concerns for standard encryption technologies. It has also been shown that for authorised users, the more secure asymmetric algorithm (two keys) is not as fast as required for modern systems. A hybrid system has been proposed to create a more secure algorithm with smaller processing times (Goyal & Kant, 2017, p.197). Issues of improving algorithmic time and efficiency have been the subject of considerable debate, yet less discussion has been around the crucial issue of what are termed honeywords, namely: "The use of decoys, realistic but fake objects to divert or detect attacks" (Juels, 2014, p. 1). "A powerful tool for compromise detection and mitigation" (Juels, 2014, p. 1). This allows more secure data at an increased speed whilst hindering brute force attacks.

Conversely, hashing data creates an irreversible numerical value of the data (Ferbrache, 2016, p.6). This method is commonly used for storing passwords as sensitive data is not stored, yet a numerical representation is. This implementation is less vulnerable as it allows secure verification without the password being stored in plain text (Ferbrache, 2016). Unfortunately, by using a dictionary to look up common password hashes, the algorithm becomes redundant (Boonkrong & Somboonpattanakit, 2016, p.2). To counteract this, a salt is implemented by adding random characters to a password before hashing. This circumvents dictionary lookups as the hashed value will not be in the dictionary as the salt is unique (Kharod, Sharma & Sharma 2015, p.2). It has been suggested to implement honeywords with hashing to raise alerts if specified passwords are used to access systems (Kharod et al., 2015, p.2). The idea of storing real passwords with honeywords is also supported by Chakraborty & Mondal (2016) as this method provides warnings of attacks and prevents unauthorised access.

Securing the system

For corporate systems to be secure, they need to prevent unauthorised access before encryption or hashing is needed. To organise security effectively "Authentication, authorization, and accounting are key" (Wilamowski, Dever, & Stuban, 2017, p.187). These points allow verified access to just what selected users should have access to, whilst keeping a log of activity. The three-tier architecture supports this model and prevents against many forms of attacks (Singh, Jeong, & Park, 2016, p.217). They continue: allowing firewalls to check for malicious incoming data is achieved by separating the application layer from the data storage layer. Although this is commonly used for in-house hosting, the popularity of cloud computing is exponentially increasing (Singh et al., 2016, p.217) and businesses are no exception.

Cloud systems store data in one centralized system (Kalaiprasath, Elankavi & Udayakumar, 2017, p.605) therefore "If someone tries to illegally access the data, the hacker ends up getting the entire information stored". To improve this Goyal & Kant (2017) suggest more secure encryption. This method is still storing all data in one system though. Kalaiprasath, Elankavi & Udayakumar, (2017) argue that only parts of the data, stored on different systems, is more secure. "Migration of cloud computing from single toward multi-clouds to ensure the security of user's data" (AlZain, Soh, & Pardede, 2013, p.1071). This model prevents against complete data being stored in one location and therefore mitigating sensitive data exposure (Kaaniche & Laurent, 2017, p.137). This method addresses "important security concerns namely data confidentiality, availability and integrity" (Kaaniche & Laurent, 2017, p.137).

System vulnerability

No matter how secure computer systems are, users must also be included as part of the security system. "Besides technology, human behaviour is generally seen as the biggest threat" (Bauer, Bernroider, & Chudzikowski, 2017, p.146) which can undermine any technological security in place. The password has been used since the 1960s "despite consensus among researchers that we need something more secure" (Bonneau, Herley, van Oorschot, & Stajano, 2015, p.78). This dated system is one of the easiest ways for hackers to access corporate data (Ferbrache, 2016). With so many criteria being needed for passwords, it is a burden to remember strong unique passwords without memory aids (Bonneau et al., 2015). This is supported by showing that the use of password managers provides a single point of failure for an information system (Florencio & Herley, 2007). To be able to fully secure a system, companies should "concentrate on fostering employee information security awareness" (Bauer et al., 2017, p146.) as this underpins the entirety of the system and prevents single failure points.

Conclusion

When mitigating information exposure, there are always weak links. Generally, the weakest part of a system is when humans are involved. Any user of corporate systems should, therefore, be aware of threats posed to it. Knowledge of exploitable weaknesses allows companies to foster more secure policies on data protection. Should a breach occur, companies should have measures to reduce the effect a breach. A hacker should have access to the full information if methods previously mentioned are implemented. Although there are many vulnerabilities within systems, the three areas highlighted are cornerstones of security. All elements of the Information system must work together to create an infrastructure that is more secure than each element.

References

AlZain, M. A., Soh, B., & Pardede, E. (2013). A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds. *Journal of Software Maintenance and Evolution: Research and Practice, 8*(5), 1068-1075.
DOI:10.4304/jsw.8.5.1068-1078

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145–159.
DOI: 10.1016/j.cose.2017.04.009

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM, 58*(7), 78–87. DOI: 10.1145/2699390

Boonkrong, S., & Somboonpattanakit, C. (2016). Dynamic Salt Generation and Placement for Secure Password Storing. *IAENG International Journal Of Computer Science., 43*(1), 27-36. Retrieved from http://www.iaeng.org/IJCS/issues_v43/issue_1/IJCS_43_1_04.pdf

Chakraborty, N., & Mondal, S. (2016). Towards Improving Storage Cost and Security Features of Honeyword Based Approaches. *Procedia Computer Science, 93*, 799–807. DOI: 10.1016/j.procs.2016.07.298

Data Protection Act 1998. (2015). *Legislation.gov.uk.* Retrieved 12 November 2017, from http://www.legislation.gov.uk/ukpga/1998/29/contents

Ferbrache, D. (2016). Passwords are broken – the future shape of biometrics. *Biometric Technology Today, 2016*(3), 5–7. DOI: 10.1016/S0969-4765(16)30049-2

Ferreira, R.S & Vargas, F. (2015). ShadowStack: A new approach for secure program execution. *Microelectronics Reliability, 55*(9/10), 2078-2081. DOI: 10.1016/j.microrel.2015.07.021

Florencio, D., & Herley, C. (2007, May). A large-scale study of web password habits. *In Proceedings of the 16th international conference on World Wide Web* (pp. 657-666). ACM. DOI: 10.1145/1242572.1242661

Goyal, V., & Kant, C. (2017). An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security. *In V. B. Aggarwal, V. Bhatnagar, & D. K. Mishra (Eds.), Big Data Analytics* (Vol. 654, pp. 195–210). Singapore: Springer Singapore. DOI: 10.1007/978-981-10-6620-7_20

Iyer, S. C., Sedamkar, R. R., & Gupta, S. (2016). A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach. *Procedia Computer Science, 79*, 293–298. DOI: 10.1016/j.procs.2016.03.038

Juels, A. (2014). A bodyguard of lies. *In Proceedings of the 19th ACM symposium on Access control models and technologies - SACMAT ’14.* DOI: 10.1145/2613087.2613088

Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications, 111*, 120–141. DOI: 10.1016/j.comcom.2017.07.006

Kalaiprasath, R., Elankavi, R., & Udayakumar, R. (2017). A NEW APPROACH FOR CLOUD DATA SECURITY: FROM SINGLE TO CLOUD-OF-CLOUDS. *International Journal On Smart Sensing & Intelligent Systems, 10*, 604-613.
DOI:10.21307/ijssis-2017-273

Keegan, M. (2017). It takes just one mistake for a company to be hacked. *Computer Fraud & Security, 2017*(4), 16–18.
DOI: 10.1016/S1361-3723(17)30033-7

Kharod, S., Sharma, N., & Sharma, A. (2015). An improved hashing based password security scheme using salting and differential masking. *In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)* (pp. 1–5). Noida, India: IEEE.
DOI: 10.1109/ICRITO.2015.7359225

Poh, G., Baskaran, V., Chin, J., Mohamad, M., Lee, K., Maniam, D. and Z'aba, M. (2017). Searchable Data Vault: Encrypted Queries in Secure Distributed Cloud Storage. *Algorithms, 10*(2), p.1-19.
DOI:10.3390/a10020052

Raschke, R. L., & Mann, A. (2017). Enterprise Content Risk Management: A Conceptual Framework for Digital Asset Risk Management. *Journal of Emerging Technologies in Accounting, 14*(1), 57–62.
DOI: 10.2308/jeta-51735

Ruivo, P., Santos, V., & Oliveira, T. (2014). Data Protection in Services and Support Roles – a Qualitative Research amongst ICT Professionals*. Procedia Technology, 16*, 710–717.
DOI: 10.1016/j.protcy.2014.10.020

Singh, S., Jeong, Y.-S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications, 75*, 200–222.
DOI: 10.1016/j.jnca.2016.09.002

Wilamowski, G., Dever, J., & Stuban, S. (2017). Using Analytical Hierarchy and Analytical Network Processes to Create Cyber Security Metrics. *Defense Acquisition Research Journal, 24*(2), 186–221.
DOI: 10.22594/dau.16-760.24.02