Project overview for portfolio upload

Project Title:

Case study: Human-Centred Security in Scottish Glen (Insider Threats & Authentication Design)

Project Description:

Literature review of authentication design mechanisms and insider threats. Following this, recommendations are made on how the company in the case study can improve their authentication mechanism. Additionally, it discusses the countermeasures and practices a company can implement to help mitigate insider threats

Grade: A

Appendices have been removed to avoid plagiarism from future students, however I am happy to provide additional information or discuss the work further if desired.

<u>Disclaimer</u>*: I do not give permission for this work to be copied, those who do may be liable for plagiarism.*

Table of Contents

1. Introduction

Scottish Glen suspects insider involvement in their systems data breach which was attributed to exploited manager credentials. Therefore, it is essential to make recommendations that provide improved authentication design and so that steps are taken to mitigate future insider threats. Understanding the current literature on authentication design and Insider Threats will enable a foundation for effective recommendations to be made to Scottish Glen. This understanding will also enable Scottish Glen to help mitigate the challenges that they will face when attempting to implement these proposed changes across the company.

2. Authentication Design

2.1 Defining Authentication Design

Authentication mechanisms can broadly be assigned to one of the following areas; as 'what you know', 'what you have' and 'what you are' (Amuairfi *et al*., 2013) . These are further defined in sections 2.1.1, 2.1.2 and 2.1.3. Through assigning authentication mechanisms into three distinctive groups, it becomes easier to identify how they are compromised for malicious purposes. Additionally, it can become simpler to assess their effectiveness for keeping companies such as Scottish Glen secure. When making the assessment, it can be useful to think of the mechanisms in terms of usability, deployability and security (Bonneau *et al.,* 2012). This is the result of each group of mechanisms holding their own unique strengths and limitations, thus finding the correct solution for a particular company will vary on the companies' requirements and existing security structure. Mechanisms can be combined to form part of a bigger system (Amuairfi *et al*., 2013), enabling coverage for possible limitations, and will provide the foundation for the recommendation that will be made to Scottish Glen in section 2.2.

2.1.1 'What you know'

Mechanisms defined as 'what you know' authentication can also be known as knowledge-based systems. In addition to passwords and pins - passphrases, security questions and pattern-based authentication all make up this category. Passwords have inherently weak security despite being very easy to deploy across companies due to their high usability (Bonneau *et al.,* 2012). This weak security is the result of passwords being susceptible to several attacks including brute force attacks, phishing or the malicious actor simply guessing poorly created passwords (Shen *et al.,* 2016). Passwords have commonly been made up of numbers and letters, however, policies are now suggesting including special characters to help mitigate brute force attacks or the likelihood of an individual guessing them (Shen *et al.,* 2016). However, this change to policy has done little to impact attempted phishing attacks.

2.1.2 ‘What you have’

‘What you have’ authentication mechanisms utilise physical methods such as hardware tokens to help authenticate users. Hardware tokens can take the form of smart cards or USB security keys that will hold further information for authentication. Hardware tokens are difficult to compromise as the malicious actor will often have to obtain the token in person (Li *et al.,* 2022). However, hardware tokens are very difficult to scale, as companies would need to ensure every employee has access and knows how to use one, which is often not the case (Bonneau *et al.,* 2012). Therefore, the work carried out by (Sun *et al.,* 2015) highlights the necessity for OTPs. OTPs are unique codes that are sent to phones or other devices and that become invalid after use, preventing repeated use (Sun *et al.,* 2015). Combining onetime passcodes with traditional passwords form the principle of MFA increasing the overall security of each mechanism (Bonneau et al., 2012).

2.1.3 ‘What you are’

Biometric authentication relies on physical characteristics most individuals will possess such as fingerprints, hand geometry or iris recognition. Therefore, this universality allows for biometric authentication to be usable by most individuals (Bonneau *et al.,* 2012). However, there some inherent issues with these mechanisms. Biometric authentication can be compromised trough spoofing. Spoofing is the process of presenting fake data to gain unauthorised access to systems (Amuairfi *et al*., 2013) . A method of spoofing is sticky residue being left by a finger on an authentication device. This enables the fingerprint to be reused to authenticate, lowering the overall security of biometric authentication - one of its strongest characteristics (Bonneau *et al.,* 2012). When combining this lowered security with the high cost for separate technologies such as fingerprint scanning, it makes it difficult to recommend to a small company such as Scottish Glen.

2.2 Recommendation: Multi-Factor Authentication

Scottish Glen requires an authorisation system that will help protect against social engineering and future insider attacks. Therefore, recommending Multi-Factor Authentication (MFA) to Scottish Glen would be the optimal solution. MFA is a two-pronged authorisation mechanism that requires the user to enter a password and further authorise with an OTP. When implementing MFA within Scottish Glen, it is important both phases of this authentication mechanism are done correctly.

Firstly, starting by implementing a password policy to increase password security at Scottish Glen. This password policy will be created by following guidelines provided by the National Cyber Security Centre (NCSC, 2018). Utilising the information provided by the NSCS, it enables employees to recognise actionable steps to create secure passwords. This is important as users will often be deterred from following password policy if the policy is too difficult to understand (Shen *et al.,* 2016). Whilst this policy will not entirely eradicate the possibility of the passwords being open to a brute force password attack, passwords with variation can make it much more difficult.

Secondly, requiring an OTP on authentication is the second step of MFA. This OTP can come in a variety of forms, allowing Scottish glen to tailor it to their requirements. For example, Scottish Glen is a small company, with no specific security expertise, therefore requiring a OTP method that has high usability and deployability is essential. These are the benefits that using a mobile phone for the OTP passcode can deliver (Sun *et al.,* 2015). This will be beneficial when considering insider threats such as the one Scottish Glen were victim too. If the proposed MFA had already been Implemented the manager who had their account compromised would have gotten an OTP to authenticate on their phone, arousing suspicion that malicious activity may have been underway. This would enable the manager to change passwords or perform other security measures such as trying to identify where the login was coming from.

3. Insider Threats

Insider threats can be defined as "*an individual who has or had authorised access to an organisations critical asset to use their access, either maliciously or unintentionally to act in a way that could negatively impact the organisation*" (Carnegie Mellon University, 2022). From this definition, it is noted that insider threats can be defined as either malicious or unintentional.

Malicious insider threats can be characterised as a deliberate exploitation of a company's security to access and share sensitive company information (Alsowail and Al-Shehari, 2022). An example of which is the breach of Scottish Glen where it is suspected that an employee has compromised the managers account and shared sensitive information with a hacktivist group. Regardless of how the employee accessed the account to exfiltrate the data, they worked with intent to gain access to sensitive information and share this data with offending parties, therefore making this a malicious and intentional insider threat. Unintentional insider threats, also known as negligent insiders, is where a legitimate individual within the company will make a mistake that can lead to sensitive data being unintentionally shared outside of the company (Liu Liu *et al.,* 2018) . This negligence can also be a fault of the afflicted company. It is not uncommon for incorrect security procedures or training to be implemented across a company, therefore resulting in employees unknowingly following vulnerable practices and thus again becoming unintentional insider threats (Carnegie Mellon University, 2022).

When looking at malicious and intentional insider threats, different motivations and risk factors are at play. Motivations are inherent to the individual, whilst risk factors are influenced by organisational practices creating a level of responsibility for the company (Homoliak *et al.,* 2019).

A common belief is that ideology, such as political ideals play a large role in the motivation for an insider threat (Homoliak *et al.,* 2019). However, from a study of 97 insider threat cases, only 5 insiders were motivated by ideology (Clark, 2016). This study also highlighted that most insider threats were motivated by revenge. A want for revenge is often found within ex-employees who feel like they were unjustly fired or present employees who may be suffering from some form of disgruntlement. This is disgruntlement is often caused by the company who will attempt to resolve it before it goes any further (Homoliak *et al.,* 2019). Typically, when these types of disgruntlements are not resolved, it is the fault of the company ignoring some other risk factors (Homoliak *et al.,* 2019). This inability to recognise and resolve employee disgruntlement is often the result of not implementing proper training previously. Implementing proper training is a crucial part of a formalised insider threat program, these programs can be created to act as a pre-emptive insider threat countermeasure.

3.1 Insider Threats: Countermeasures

3.1.1 Formalised Insider Threat Program

This type of program will act as a pre-emptive approach to mitigating insider threat, meaning it will create regulation and guidance on preventative methods (Carnegie Mellon University, 2022). This program will aim to prevent intentional or unintentional insider threat from occurring again within Scottish Glen. This program will include activities such as conducting a comprehensive risk assessment on potential vulnerabilities and individuals within the organisation. Additionally Scottish Glen should follow the guidance develop tailored policies, procedures, and controls to mitigate future risk (Carnegie Mellon University, 2022).

3.1.2 Role Based Access Control (RBAC)

RABC is an important foundational countermeasure that would have prevented the breach experienced by Scottish Glen. RBAC is a series of access controls that will limit users' system access dependent on their role within the company. Additionally, the controls provide further security for managerial accounts, assigning separate login details. This control can help prevent against employees who may be insider threats, using generic or standard user entry to gain access to managerial level data (Alsowail and Al-Shehari, 2022). This is just one of the ways in which Scottish Glens managers account could have been breached.

3.1.3 Data Leakage Prevention (DLP)

Similarly to Insider threat programs or RBAC, DLP is a pre-emptive countermeasure to insider threats. Setting up DLP strategies in advance can provide technology or procedures that act as a safeguard for sensitive information stored by a company. As outlined in (Homoliak *et al.,* 2019), there are numerous ways to develop DLP strategy. One example could include developing encrypted, secure data storage that requires external managerial confirmation before any process tries to read and write from the confidential data. Having these added layers of protection would have made it much harder for the insider threat to exfiltrate Scottish Glen's data.

3.1.4 Intrusion Detection

Intrusion detection responds reactively after an insider threat attempts to compromise security. Intrusion detection systems can detect anomalies or misuse(Homoliak *et al.,* 2019). Anomaly based detection will be modelled on a normal use of Scottish Glen's system, flagging any anomalies. Alternatively, misuse detection is modelled on malicious behaviours, flagging when activity matches this modelled malicious behaviour. For example, during the Scottish Glen data breach, unusual data movement could have triggered alters to other managers to stop the data transfer.

3.1.5 Incident Response

Unlike pre-emptive measures previously outlined, incident response planning involves developing a solution and remediation to security incidents caused by insiders after their malicious activity. Disclosure to shareholders, documentation of the breach and correct reporting procedures to ensure transparency across the company are all included in incident response. With proper incident response planning then the fallout from the breach, despite confidential data being exploited, could be mitigated by Scottish Glen taking responsibility and showing correct procedures being carried out to mitigate the damage done.

4. Challenges to Implementation

Implementing security recommendations at Scottish Glen faces challenges due to the absence of strong security culture within the company. As highlighted in (Alotaibli *et al.*, 2016) companies with strong security culture are more likely to implement security measures. Having security expertise within the company helps promote a culture of security (Ashenden, 2008). Unfortunately, Scottish Glen do not have this expertise, therefore they will need to adopt strict training to develop a bassline of security understanding before implementing the recommendations made by this report. Security training requires some level of knowledge from those teaching, therefore Scottish Glen may need to externally hire security professionals until they are up to speed, adding to an already costly change in their security systems. Overall, before changes can be made Scottish Glen have multiple challenges to address.

5. Conclusion

This breach was enabled through lax security design created from a lack of understanding for effective authentication mechanisms. A definition of authentication mechanisms and recommendations for improvements have been made to Scottish Glen. Further, because of the insider threat attack, further research has been carried out, defining insider threats and how they come to be. Therefore, countermeasures have been recommended to prevent this event being repeated. Overall, a clear outline and security strategy has been proposed to Scottish Glen.

References

Almuairfi, S., Veeraraghavan, P. and Chilamkurti, N. (2013) 'A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices', *Mathematical and computer modelling,* 58(1-2), pp. 108-116. doi: 10.1016/j.mcm.2012.07.005 https://dx.doi.org/10.1016/j.mcm.2012.07.005

Alotaibi, M., Furnell, S. and Clarke, N. (2016) 'Information security policies: A review of challenges and influencing factors', *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST),* , pp. 352-358. doi: 10.1109/ICITST.2016.7856729 https://ieeexplore.ieee.org/document/7856729

Alsowail, R.A. and Al-Shehari, T. (2022) 'Techniques and countermeasures for preventing insider threats', *PeerJ. Computer science,* 8, pp. e938. doi: 10.7717/peerj-cs.938 https://www.ncbi.nlm.nih.gov/pubmed/35494800

Ashenden, D. (2008) 'Information Security management: A human challenge?', *Information security technical report,* 13(4), pp. 195-201. doi: 10.1016/j.istr.2008.10.006 https://dx.doi.org/10.1016/j.istr.2008.10.006

Bonneau, J., Herley, C., van Oorschot, P.C. and Stajano, F. (2012) 'The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes ', *2012 IEEE Symposium on Security and Privacy,* , pp. 553-567. doi: 10.1109/SP.2012.44 https://ieeexplore.ieee.org/document/6234436

Carnegie Mellon University (2022) *Common Sense Guide to Mitigating Insider Threats, Seventh Edition.* Software Engineering Institute. Available at: https://insights.sei.cmu.edu/documents/5777/5692_CSG_Book_20-optimized.pdf (Accessed: Mar 25, 2024)

Clark, J.W. (2016) 'Threat from Within: Case Studies of Insiders Who Committed Information Technology Sabotage', *2016 11th International Conference on Availability, Reliability and Security (ARES),* , pp. 414-422. doi: 10.1109/ARES.2016.78 https://ieeexplore.ieee.org/document/7784600

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019) 'Insight Into Insiders and IT', *ACM computing surveys,* 52(2), pp. 1-40. doi: 10.1145/3303771 https://dl.acm.org/doi/10.1145/3303771

Li, S., Xu, C., Zhang, Y. and Zhou, J. (2022) 'A Secure Two-Factor Authentication Scheme From Password-Protected Hardware Tokens', *IEEE transactions on information forensics and security,* 17, pp. 3525-3538. doi: 10.1109/TIFS.2022.3209886 https://ieeexplore.ieee.org/document/9903479

Liu Liu, De Vel, O., Qing-Long Han, Jun Zhang and Yang Xiang (2018) 'Detecting and Preventing Cyber Insider Threats: A Survey', *IEEE Communications surveys and tutorials,* 20(2), pp. 1397-1417. doi: 10.1109/COMST.2018.2800740 https://ieeexplore.ieee.org/document/8278157

NCSC and National Cyber Security Centre (2018) *Password administration for system owners* . Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach (Accessed: 25th March, 2024)

Shen, C., Yu, T., Xu, H., Yang, G. and Guan, X. (2016) 'User practice in password security: An empirical study of real-life passwords in the wild', *Computers & security,* 61, pp. 130-141. doi: 10.1016/j.cose.2016.05.007 https://dx.doi.org/10.1016/j.cose.2016.05.007