Abertay University®

CMP417 CW3

HUMAN-CENTERED SECURITY

Zack Anderson | BSc (Hons) Ethical Hacking | 05/05/2020

Introduction

After a recent data breach where an employee gained access to corporate systems to steal pay checks from colleagues, the organisation decided to review its security policies. This report focuses on similar cases where insider threats caused the loss of financial resources and intellectual property, how these incidents occurred, and how they can be prevented utilising stronger authentication mechanisms.

This report proposes that the organisation implement a two-factor authentication mechanism to create an impersonation-resistant authentication mechanism using both SMS-based and application-based systems for maximum adoption by employees. This system must be simple to set up and use for those less technologically literate while keeping employee accounts secure. This system will help to prevent unauthorised logins to employee accounts should their password authentication fail to keep their account secure and will instantly notify them of new login attempts so they can swiftly alert the organisation of unauthorised logins.

Literature Review

INSIDER THREATS

An insider threat is when is a security threat originating within an organisation. A survey conducted by Crowd Research Partners in 2018 found that, of the organisations which participated in the survey, over 50% had suffered from an insider attack in the previous 12 months (Crowd Research Partners, 2018). An example of an insider threat posed by a rogue employee occurred at Allen & Hoshall, an engineering firm based in the US, in 2017 (United States Department of Justice, 2017). Despite following proper termination procedures by revoking his access to their systems, an ex-employee who left to create his own company gained access to the companies e-mail and file-sharing systems using the credentials of a former colleague. He then used this access to download project and client information for his own business. This was only discovered when a potential client noticed a considerable number of similarities between the proposals from the 2 companies, at which point they notified Allen & Hoshall who co-operated with the Federal Bureau of Investigation to track down the ex-employee.

While insider threats are commonly associated with rogue employees intending to harm their employer for financial gain or because they feel unfairly treated, employees or contractors who have less cyber security knowledge contribute equally to the issue. This occurred in a 2017 breach of Anthem, a US health insurance company, where an employee emailed a file with private medical information to their personal e-mail with the intention of misusing the data (Davis, 2017). While this hurt the contractor's reputation, the damage to Anthem's brand was exacerbated due to the company suffering another data breach two years prior.

PASSWORD AUTHENTICATION SHORTCOMINGS

As people tend to choose passwords linked to their hobbies, interests or personal lives, to make them more memorable. The shortfall of this approach is it makes them easy for an attacker to guess, which could allow them access to personal and corporate accounts which utilise password authentication. To force users to create more secure passwords, many companies use *"Password Policies"*. These policies usually specify characters which must appear in a password, a minimum length, or a password expiry date, which are common in corporate environments. There is little evidence to support that these create more secure passwords and can instead do the opposite. A study by Carnegie Melon University's CyLab found that the most secure password policy against a brute-forcing attack was one which simply required a minimum 16-character password length. By

specifying that certain characters must appear in a password, brute-force attempts can be streamlined, as can be seen in Figure 1.

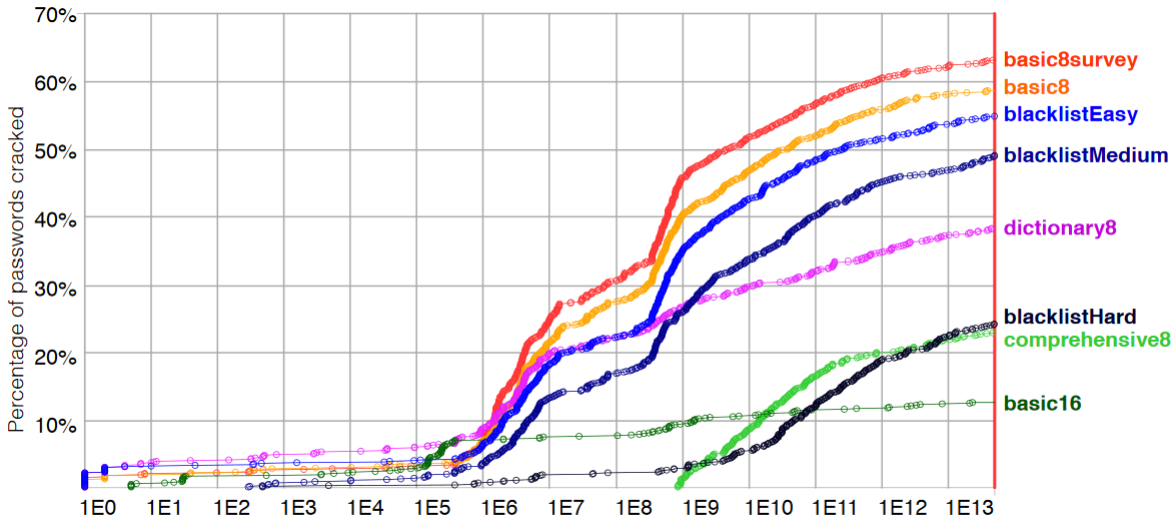

Figure 1 - The number of passwords cracked vs. number of guesses, per condition

A study by (Horsch, et al., 2016) also stated that due to the lack of standardisation when implementing password policies, password managers have limited support without the user manually specifying rules – and that this often led to users choosing weaker passwords.

MULTI-FACTOR AUTHENTICATION

Two-factor authentication was first proposed in 2001 by (Owen & Shoemaker, 2001) where the user first authenticates using their password then a second time using *"the PIN from [their] device over an ancillary communications network"*. This authenticates the user based on 2 factors; what they know, and what they possess. This second barrier of defence means that even if an attacker correctly guessed a victims password, they will not be given access to the system without also having control of their multi-factor authentication mechanism. To prevent brute-force attacks against the secondary authentication mechanism, these codes expire after a short time within which the attacker could only try a few possible combinations.

Discussion

Insider threats are commonly carried out using password attacks where the perpetrator uses other employees credentials to access systems covertly, as occurred at the client organisation. One way to mitigate attacks against password authentication is to implement a multi-factor authentication system. Traditionally this involves entering a one-time code sent to the user through an application, e-mail, or SMS message. These services are easy to set up for the user and usually involve simply signing up for them or scanning a QR code with a two-factor authentication application on their smartphone. These services provide a second wall of defence against attackers by blocking access, even if a users' password is known if they cannot guess the one-time use code. These codes are randomly generated and expire after a short amount of time to mitigate brute-forcing attacks.

Multi-factor authentication mechanisms are effective as the hacker would also require access to the multi-factor authentication mechanism, such as the victim's smartphone, to gain access to the account. Some applications and SMS messages will also notify the user when a new login occurs on their account, meaning they could instantly report the incident to be investigated further by the organisation.

Testing of a multi-factor could be completed by first making the new mechanism opt-in, before forcing users to use it after a few weeks or months. This would give the organisation time to sort any potential issues with the multi-factor implementation while also creating a help document of the most frequently asked questions to aid users in adopting the new technology. To encourage users to sign up to two-factor authentication for testing, the webpage similar to that in Figure 2 can be displayed to users the next time they log into the organisation's services. The effectiveness of the mechanism could be measured by hiring a third-party organisation to complete a penetration test of the client organisation to assess their cyber vulnerabilities and weaknesses.

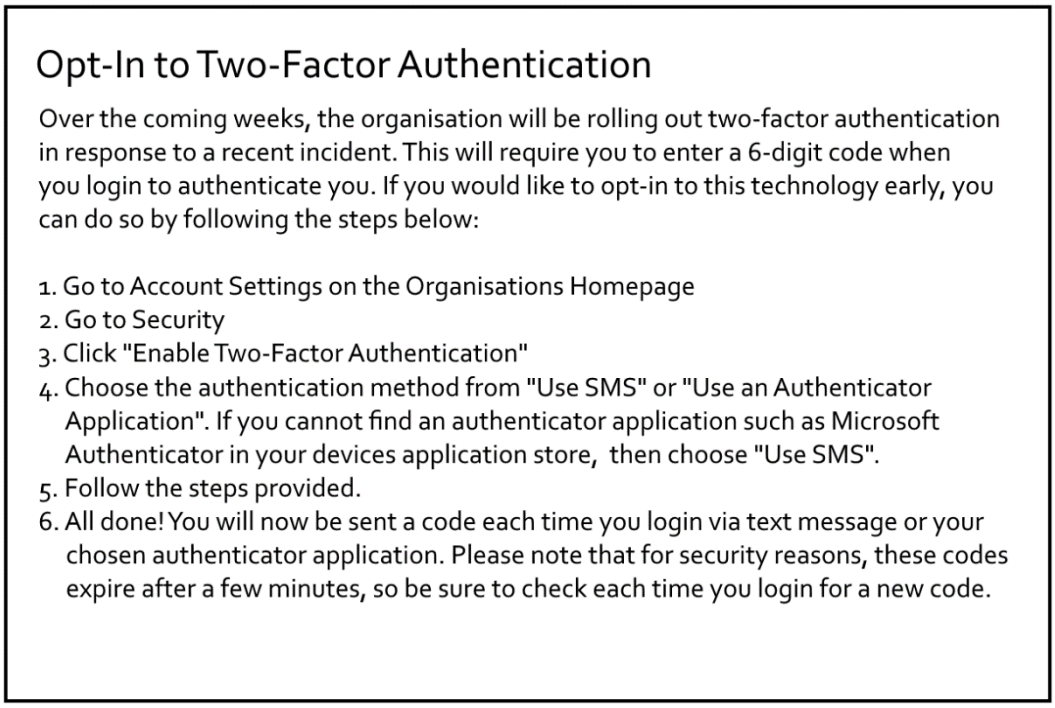

Figure 2 - Opt-In Information Webpage for Two-Factor Authentication

Conclusion

One of the challenges of implementing an impersonation-resistant authentication mechanism is that not all employees will have the technical knowledge to understand complex instructions. Often if the mitigation is too much hassle to setup that it hinders or overwhelms employees then they will not use it, which two-factor authentication combats being both simple to set up and easy to understand. By implementing a hybrid approach of both SMS-based and application-based two-factor authentication, the organisation can ensure that every employee can use the new system even if they do not have a smartphone.

One challenge of the two-factor authentication mechanism is that users must have a personal smartphone or a company smartphone to receive codes via an application. This could be combatted by implementing a simpler SMS-based authentication where users are sent the codes via text message which is supported by almost every mobile phone sold in the last decade. The caveat with this approach is that it is less secure as attackers may be able to intercept SMS messages over insecure cellular networks, however, is still better than no multi-factor authentication at all (Mulliner, et al., 2013). For this reason, it should be made clear to the user that the SMS-based approach is simply there for supporting those without smartphones, as seen in Figure 2.

Application-based two-factor authentication mitigates attacks such as man-in-the-middle attacks by generating the codes on the device from a secret key – however, if a user accidentally leaks their secret key such as their QR code, the two-factor authentication mechanism would be rendered useless. For this reason, users should be asked not to photograph their QR code.

References

Crowd Research Partners, 2018. *2018 Insider Threat Report,* s.l.: Crowd Research Partners.

Davis, J., 2017. *Anthem: Insider theft exposes data of 18,000 Medicare members.* [Online]
Available at: https://www.healthcareitnews.com/news/anthem-insider-theft-exposes-data-18000-medicare-members
[Accessed 2 May 2020].

Horsch, et al., 2016. *Password Policy Markup Language.* [Online]
Available at:
https://www.researchgate.net/publication/309426860_Password_Policy_Markup_Language
[Accessed 2 May 2020].

Mulliner, C., Borgaonkar, R., Stewin, P. & Seifert, J.-P., 2013. SMS-Based One-Time Passwords: Attacks and Defense. In: Heidelberg, ed. *Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA) 2013.* Berlin: Springer, pp. 150-159.

Owen, W. & Shoemaker, E., 2001. *Multi-factor authentication system.* [Online]
Available at: https://patents.google.com/patent/US7373515B2/en
[Accessed 3 May 2020].

United States Department of Justice, 2017. *Tennessee Man Sentenced for Unauthorized Access of Former Employer's Networks.* [Online]
Available at: https://www.justice.gov/opa/pr/tennessee-man-sentenced-unauthorized-access-former-employers-networks
[Accessed 2 May 2020].