Part 3. Human-Centred Security

Martin Pavlinov Zhelev

CMP417: Engineering Resilient Systems

BSc (Hons) Ethical Hacking Year 4

2023/2024

Note that the Information contained in this document is for educational purposes.

Contents

1 HUMAN-CENTRED RESILIENCE

1.1 INTRODUCTION

ScottishGlen employees have been receiving phishing emails from a suspected hacktivist group. There are concerns that the employees lack the training to detect malicious emails successfully and thus might open malicious links or attachments that could expose the company's network. As a result, a report was requested recommending methods for improving ScottishGlen's human-centred resilience.

To achieve this, a literature review was conducted to gain insight into phishing attacks, their commonness, how they compromise security, and how to prevent them. Following the literature review, recommendations were made on reducing the risk of such attacks being successful.

1.2 HUMAN-CENTRED RISKS

In their book, Jakobsson and Myers describe phishing as "a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials...". Phishing is commonly performed in an automated fashion through emails that mimic trustworthy organisations and is usually done for financial gain. (Jakobsson and Myers, 2006)

Phishing attacks are one of the significant threats to organisations and individuals. Several types of phishing (email, SMS, voice, and social media) are continuously evolving and have become more challenging to build countermeasures for. Susceptibility to phishing varies based on factors such as age, gender, and education level. Training can reduce the chances of falling prey to phishing; however, even trained individuals can be affected if an attack is sophisticated enough. (Alkhalil et al., 2021)

In 2011, more than half of the incident reports sent to "The United States Computer Emergency Readiness Team" related to phishing (Figure 1). (Gupta et al., 2017)

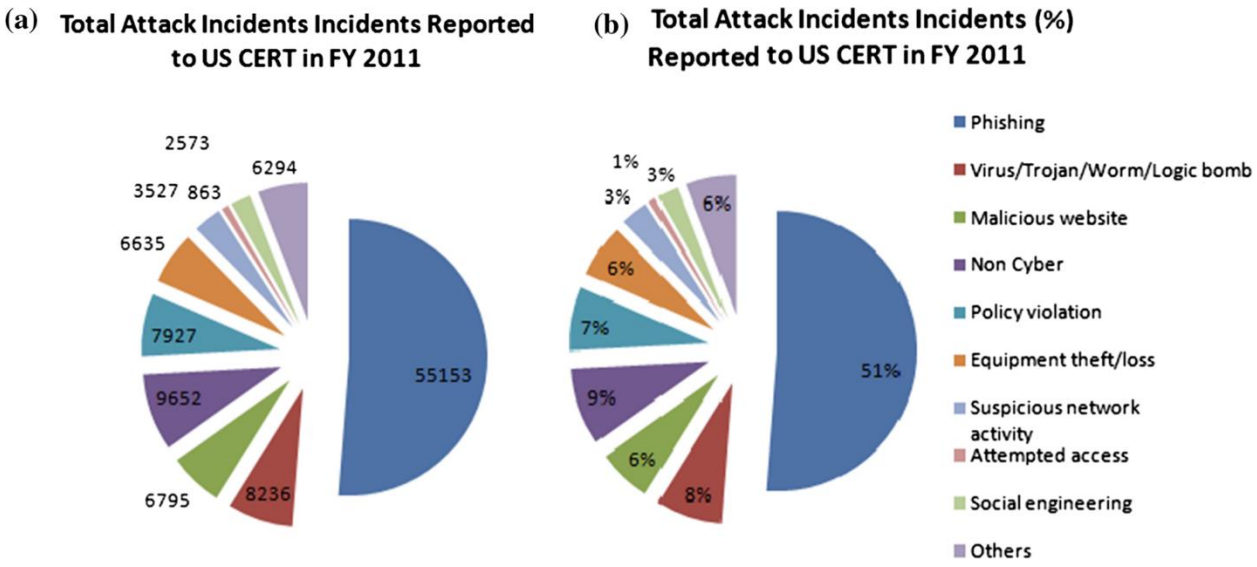

Figure 1. a Summary of total incidents reported to US CERT in FY 2011 and b summary of total incidents (%) reported to US CERT in FY 2011 adapted from (Gupta et al., 2017).

In the UK, more than thirteen million reports of suspicious phishing emails were made by August 2022 to the Suspicious Email Reporting Service (SERS). SERS is a service operated by the National Cyber Security Centre (NSCS) to help people who have received phishing emails. (Office for National Statistics, 2022).

In 2016, losses from financial fraud caused by phishing in the UK totalled 768.8 million pounds. However, financial losses are not the only impact of phishing. If a phishing attack is successful, it can also cause serious reputational damage to companies, which can lead to customer loss. (Alkhalil et al., 2021)

Lack of awareness causes phishing attacks, so training the staff and implementing tools for automatically removing malicious emails are extremely important. No matter the solution, it must be constantly updated to keep up with the latest phishing developments. (Gupta et al., 2017)

Social engineering, which is a technique commonly used for phishing attacks, “depends on modern preventive tools and the security systems in place, as well as the availability of trained and skilled personnel dealing with sensitive data in organisations.” (Aldawood and Skinner, 2019). Despite that, many organisations do not prioritise training due to a lack of budget. (Aldawood and Skinner, 2019)

1.3 HUMAN-CENTRED RECOMMENDATIONS

The following recommendations should be implemented to reduce the risk and effects of phishing attacks.

1.3.1 Regular Awareness Training

Regular training on phishing attacks and how to identify them should be given to all employees. Alongside this, all employees need to be trained to report anything they determine to be suspicious to members of the IT team at Scottish Glens for review.

To keep the training costs low and the training engaging for all staff, the recommendation found in the paper by Aldawood should be followed. According to them, an assessment test should be given to all employees to determine their level of awareness. After deciding their level, the high-risk employees need to receive a lengthier training session, while low-risk employees are provided with a shorter training session that focuses on their specific weaknesses. (Aldawood and Skinner, 2019)

1.3.2 Email Filtering

As discussed in the paper by Gupta et al., incoming emails need to be passed through a phishing detection system to automatically remove any detected phishing attempts before they reach the mailbox. This solution will need to be regularly updated to ensure its ability to detect the latest attacks. (Gupta et al., 2017)

1.3.3 Phishing Tests

Further phishing tests should be conducted to train the staff. As discussed by the IT company IBM, this type of testing should be performed regularly. It should also resemble realistic phishing attempts, with that only difference being that if a user falls prey to it, there is no effect on the organisation. (IBM, 2024)

1.3.4 Strong Password Policy and Management

All employees should use Password Managers to implement strong, randomly generated passwords that are never reused. As discussed by Alkhalil et al., if an attack is sophisticated enough, even trained individuals can be affected, including all employees. By having a strong password policy in place, an attacker would not be able to use the obtained password to access multiple services. (Alkhalil et al., 2021)

1.3.5 No Blame Culture

As Kwak et al.'s paper discusses, people are scared to report phishing attacks because they fear punishment and ridicule. (Kwak et al., 2020). Because of this, no employees should be blamed if they fall prey to a phishing attack, and they should be frequently encouraged to admit if they have made a mistake. This would allow the IT team to take appropriate actions sooner to reduce the harm of the phishing attack.

2 AUTHENTICATION MECHANISM DESIGN

2.1 INTRODUCTION

Another risk ScottishGlenn faces is the lack of authentication in their internal network. As a result, the researcher has been asked to identify a suitable authentication mechanism that balances security and usability.

Similarly to before, a literature review was conducted this time to gain insight into the importance of authentication mechanisms, their different types, and which one is the most effective. Following this, a recommendation will be made on which authentication mechanism to implement.

2.2 AUTHENTICATION MECHANISMS LITERATURE REVIEW

Authentication is “the process by which a person or system verifies that they are who they say they are”. Authentication can be single-factor, two-factor or multi-factor (Barney et al., 2023). Each authentication factor can be “Something you know”, “Something you have”, or “Something you are”.

The first, “Something you know,” usually involves using a password or a PIN and is considered the weakest because it can be provided through guessing, brute force, or theft. (Idrus et al., 2013). Alongside this negative, passwords are also unsuitable for people with dyslexia, as found in the paper by Renaud et al. (Renaud et al., 2021)

The second, “Something you have”, typically involves using a physical object like a smart card or a mobile device. (Lal et al., 2016). This method, while good if implemented on its own, can allow access through theft or device cloning techniques.

The third, “Something you are”, uses biometric identification, such as fingerprints or facial recognition, and is considered the strongest since it is much more difficult to steal or replicate biometrics. However, this factor is still prone to false negative and false positive results, which could allow an authorised user to gain access. Because of this, Lal et al. recommend the use of multifactor authentication (MFA). (Lal et al., 2016)

Two-factor authentication (2FA) is a type of MFA. During 2FA, the user typically has to authenticate with something they know and something they have. Typically, this is done using a password (something they know) and a cellphone (something they have).

There are several forms of 2FA using cell phones. The least secure is 2FA with text codes because it is easy for cybercriminals to intercept one-time passcode messages. One of the most secure 2FA methods is using an Authenticator app such as Microsoft Authenticator, which

allows the user to authenticate with their phone's existing authentication method (biometrics, password, etc.). Another secure 2FA method is security keys, which provide an alternative for people that do not want to use their mobile device for authentication. (Trevino, 2023)

2.3 AUTHENTICATION MECHANISMS RECOMMENDATIONS

It is recommended that ScottishGlen implement MFA to improve the security of its internal web application. With MFA, malicious actors cannot infiltrate the system just by having access to the users' credentials.

For the use case at ScottishGlen, the best authentication method that should be implemented is 2FA, which uses an authenticator app on the employee's devices and a strong password. For the password to be considered strong, it should pass the following requirements:

- At least 12 characters long
- Contains uppercase and lowercase letters.
- Includes numbers and special characters (e.g., @, #, $)
- Does not contain common words or sequences.
- Optionally is generated by a password manager.

Implementing an authenticator app as a second authentication factor alongside a strong password has two benefits. First, it allows users to use their mobile phone's existing authentication method (biometrics, password, etc.), which satisfies the "Something you are" and "Something you have" authentication factors. Second, if their credentials are compromised, the user will be notified by the 2FA notification they receive from the authenticator app.

A potential issue of this implementation is that users might get irritated having to authenticate themselves through the app on their device, however through the use of SSO and the ability to remember a certain device used during login this should be avoided. Alongside this some users might be unhappy to install an authenticator app on their personal device. To mitigate this, those users should be assigned a company device or provided an alternative 2FA method such as a security key.

In Figure 2, you can see a wireframe of a mock login page for the login system. This visual representation of the login page is included to show that a simple login page, containing the company's logo and name, will be more than sufficient for the internal use case of this solution.

Figure 2: Login page Wireframe.

3 CONCLUSION

By implementing the recommendations in this report, the security of ScottishGlen's can be improved. All the recommendations were made following an in-depth literature review of academic and industry sources.

The recommended strategies for human centred resilience include regular training tailored to the employee's risk level, implementation of email filtering systems, periodic phishing tests and no blame culture.

Additionally, to strengthen the authentication mechanisms in the internal web application the researcher recommends an implementation of 2FA. The suggested implementation in the form of strong password and an authenticator app on the user's devices would ensure that even if credentials are compromised, the damage is minimal.

By implementing the recommendations in this report, the security of ScottishGlen's can be improved. This would reduce the likelihood and impact of a successful cyber attacks.

4 REFERENCES

Aldawood, H. and Skinner, G. (2019) 'Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues', *Future Internet*, 11(3), p.73.

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021) 'Phishing Attacks: A Recent Comprehensive Study and a New Anatomy', *Frontiers in Computer Science*, 3.

Barney, N., Shacklett, M.E. and Rosencrance, L. (2023) *What is Authentication? | Definition from TechTarget*. Available at: https://www.techtarget.com/searchsecurity/definition/authentication (Accessed: 5 May 2024).

Gupta, B.B., Tewari, A., Jain, A.K. and Agrawal, D.P. (2017) 'Fighting against phishing attacks: state of the art and future challenges', *Neural Computing and Applications*, 28, pp.3629-54.

IBM (2024) *What is a phishing simulation?* Available at: https://www.ibm.com/blog/phishing-simulation/ (Accessed: 5 May 2024).

Idrus, S.Z.S., Cherrier, E., Rosenberger, C. and Schwarzmann, J.-J. (2013) 'A Review on Authentication Methods', *Australian Journal of Basic and Applied Sciences*, 7(5), pp.95-107.

Jakobsson, M. and Myers, S. (2006) *Phishing and countermeasures: understanding*. New Jersay: John Wiley and Sons.

Kwak, Y., Lee, S., Damiano, A. and Vishwanath, A. (2020) 'Why do users not report spear phishing emails?', *Telematics and Informatics*, 48, p.101343.

Lal, N.A., Prasad, S. and Farik, M. (2016) 'A Review Of Authentication Methods', *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, 5(11), pp.246-49.

Office for National Statistics (2022) *Phishing attacks – who is most at risk? - Office for National Statistics*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/phishingattackswhoismostatrisk/2022-09-26 (Accessed: 5 May 2024).

Renaud, K., Jognson, G. and Ophoff, J. (2021) 'Accessible authentication: dyslexia and password strategies', *Information & Computer Security*, 29(4), pp.604-24.

Trevino, A. (2023) *2FA vs MFA: What's the Difference?* Available at: https://www.keepersecurity.com/blog/2023/05/08/2fa-vs-mfa-whats-the-difference/ (Accessed: 5 May 2024).