Student: UP850844

Mitigating corporate information exposure on the web.

Introduction

It can be observed that the web is becoming the default vector for the distribution of data within a corporate environment. Therefore the mitigation of the public exposure of sensitive corporate data on the web is often of paramount concern for many organisations.

Technical Policies

A functioning system for the protection of data and mitigation of information exposure is often dependant on well designed technical policies. One policy that Morrow suggests is to consider how organisations can control the replication of data while using a Bring Your Own Device (BYOD) policy. Through the use of a BYOD policy, organisations can expose themselves to several attack vectors through compromised devices and applications. This especially regards personal devices that have had data logging programs maliciously installed on devices that access sensitive corporate data (Morrow 2012).

Gordon reinforces the importance of organisations being aware of the ways in which employees can inadvertently leak data when they discuss the need for a control system over the movement of files containing corporate data. Gordon comments on the fact that malware signature detection is not completely effective due to the ability to make changes to malware to alter its signature, making detection difficult (Gordon, 2007, p.37). This analysis of the limitations of the different methods to mitigate information exposure demonstrates an understanding that no single method of attempting to secure data is infallible. Such an attitude is reflected throughout the information security industry to the extent that Gordon's recommendations may be evaluated as credible.

Non-technical Policies

Despite the importance of having effective technical policies, ensuring corporations have a clear understanding of the non-technical policies that can be implemented to protect data is essential. Mitnick discusses the efficacy of social engineering (SE) in exposing corporate information through manipulating employees of a targeted company (Mitnick, 2002, p. 247). Gordon reinforces the remarks made by Mitnick through Gordon's considerations on SE where it is discussed that while SE attacks, specifically phishing emails, "rely on ignorance", they are often effective in acquiring private data (Gordon, 2007, p.25).

Additionally, Mitnick suggests data security should be a concern for all employees within a corporation and that nurturing an attitude of enthusiasm regarding an employee's responsibility to secure corporate information prevents employees maliciously exposing data. It can be observed that this suggestion has credibility through Morrow's remarks on how organisations should educate end users on the importance of security, due to data leaks often being caused by insider carelessness (Morrow, 2012). Both Mitnick's and Morrow's sentiments are further emphasised by Williams et al. as they discuss the significance of the role of the individual within the process of securing data, due to the

variability in which employees “engage in systematic evaluation when viewing online communications” (Williams et al., 2017).

Despite both Mitnick and Gordon recognising the significance non-technical policies, Mitnick emphasises the factor of SE to a far greater extent while Gordon focuses on specific implementations of where technical methods can develop the benefits of having an effective non-technical policy. Using both author’s recommendations can generate a comprehensive understanding of the necessary non-technical precautions an organisation may take to mitigate information exposure.

Incident Response

While an understanding of both technical and non-technical methods for preventing information exposure can be critical, a corporation’s response can be the controlling factor in preventing sensitive data exposure in the eventuality of a cyber attack. Anderson suggests that through the use of checklisting and team resource management (TRM) an efficient mechanism can be set up for responding to incidents. Through utilising TRM a flexible approach can be used to optimise human performance through cultivating team-based tools and practices to reduce the response time against attacks compared to traditional command and control approaches (Anderson, 2017). Anderson’s analysis of the advantages of a checklist/TRM system over a traditional command and control approach demonstrates an understanding of the subject which can give credibility to their work.

Anderson’s proposals can be ratified by Hawkins as they comment on the importance of an effective platform for critical communication during an attack, however Hawkins specifically discusses the requirement for multi-modality with a corporation's communication mediums to ensure more effective communication (Hawkins, 2017). This simultaneity of ideas can suggest validity within both Hawkins’ and Anderson’s reflections. However neither Hawkins or Anderson provide discussion on autonomous response systems which is presented by Cazorla et al. as an effective method in providing an effective response to critical system attacks (Cazorla et al., 2015).

Moreover, the NCSC looks at the tasks that can be completed after incidents to gain an understanding of system vulnerabilities. These tasks can reduce the likelihood of further incidents occurring and thus reduce further information exposure. While both Anderson and the NCSC discuss principle ideas on incident response, it could be argued that a more effective document could unify the abstract policies for incident management presented by Anderson as well as recommending detailed tasks an organisation would benefit from completing after an incident of an attack.

Conclusion

Mitnick states how the most effective method of preventing SE attacks is through combined use of security technologies and non-technical policy to ensure employee behavior does not compromise an organisation’s data (Mitnick, 2002, p. 245). This attitude can extrapolate to be equally relevant in instilling a philosophy regarding an effective method of preventing data exposure. Utilising combined techniques within this philosophy can enable a corporation to mitigate any future information exposure on the web.

References

Anderson, K. (2017). Using agility to combat cyber attacks. Journal Of Business Continuity & Emergency Planning, 10(4), 298-307.

Cazorla, L., Alcaraz, C., & Lopez, J. (2015). Awareness and reaction strategies for critical infrastructure protection. Computers And Electrical Engineering, 47299-317. doi:10.1016/j.compeleceng.2015.08.010

Gordon, P. (2007). Data leakage – threats and mitigation. SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation-1931

Hawkins, N. (2017). Feature: Why communication is vital during a cyber-attack. Network Security, 201712-14. doi:10.1016/S1353-4858(17)30028-4

Mitnick, K. D., & Simon, W. L. (2002). The art of deception : Controlling the human element of security. Indianapolis, Indiana : Wiley Publishing, Inc.

Morrow, B. (2012). Feature: BYOD security challenges: control and protect your most sensitive data. Network Security, 20125-8. doi:10.1016/S1353-4858(12)70111-3

NCSC (2016). *10 Steps: Incident Management.* Retrieved from https://www.ncsc.gov.uk/guidance/10-steps-incident-management

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Full length article: Individual differences in susceptibility to online influence: A theoretical review. Computers In Human Behavior, 72412-421. doi:10.1016/j.chb.2017.03.002