SECURING THE TECHNOLOGY CHANGE AGENDA

UNDERSTANDING AND MANAGING THE SECURITY RISK OF TECHNOLOGY CHANGE INITIATIVES

Securus Global, March 2014

ABSTRACT

Businesses are increasingly seeking to leverage new technologies such as mobile and cloud to enable strategic initiatives, realise business efficiencies, support a flexible, productive workforce and facilitate innovation.

Although these initiatives provide many business benefits, the rapidly evolving technology landscape can also introduce significant security risks that threaten the confidentiality, integrity or availability of sensitive corporate information. In the modern, connected age such compromises can have a significant negative impact to corporate reputation and business performance.

Understanding, identifying and mitigating the security risks inherent in the use of such technology is necessary to allow businesses to realise the benefits of investment in new technology initiatives while maintaining their desired security posture.

Introduction

This case study examines a recent engagement where Securus Global advised a large, ASX 20 listed company with the security management of an initiative to enable the distribution and communication of papers, notes and meeting processes for both board and committee meetings to mobile devices. This was to be implemented using an iPad application and supporting Microsoft web technologies.

Given the highly sensitive and business critical nature of the information handled by the iPad application it was imperative that the business and security risks were understood, identified and mitigated and the application and supporting systems were adequately assessed and secured.

Problem Definition

Several core security challenges must be overcome when implementing any new technology initiative to handle highly sensitive information:

1. Understanding and modelling the threat landscape and the risks inherent in adopting the technologies in the business;
2. Developing and implementing pragmatic and effective mitigation strategies against those threats and risks;
3. Identifying security vulnerabilities in the applications and supporting technologies used;
4. Remediating security vulnerabilities identified to improve security to an acceptable standard without impacting the business benefits or usability of the application or technology; and
5. Ensuring the technical and operations teams have the appropriate skills and experience to remediate the security vulnerabilities identified.

Analysis

Although the business benefits of the project were clear, there are many risks associated with enabling access to such confidential and strategic information through a mobile application.

The threat and risk profile of this project was multi-faceted and more complicated than a typical mobile application that would primarily face threat agents of various skills motivated purely by financial gain. The application was to be used by directors and the executive for highly sensitive corporate information. Given the profile of the company and the highly competitive industries in which it operates it is likely that the threat agents would be skilled, well resourced and motivated beyond immediate financial gain.

In addition to external threats, the application faces security threats from insiders ranging from those with deliberately malicious intent to those who are simply negligent. While nothing new, these threats are taking new forms with these modern, connected technologies.

Should security weaknesses be identified and exploited by parities with malicious intent it may expose the company and its partners to significant reputational and business losses.

After modelling the threat landscape and security risks associated with the initiative, Securus Global performed a technical security assessment of the application and supporting technologies.

The assessment of the project identified several serious security issues that stemmed from fundamental flaws in the design and implementation of the iPad application's key security controls that put at risk the confidentiality, integrity and admissibility of the company board papers, meeting notes and annotations.

The design and implementation of the application and supporting technologies compromised the confidentiality and integrity of board papers and board meeting records and did not satisfy the legal and compliance requirements of a board of directors and the company under the Corporations Act. The areas of concern relate to e-discovery, control over content and the safeguarding of business intelligence.

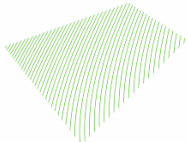
Given the speed at which the application was compromised, the fundamental nature of the issues and the sensitivity of the information in the application the findings were escalated quickly throughout company management, the executive and even the board of directors. In an address to the 800 strong IT staff at the company the GM of Infrastructure directly cited the assessment and the issues identified in response to the question "what keeps you up at night?"

The escalation of the security issues highlighted the importance of effective stakeholder management when discussing and managing security risks during a technical project. It's imperative that communication of security issues be appropriately tailored to each stakeholder group.

Solution

The vulnerabilities identified in the application were primarily due to the fundamental design and implementation of key application components that did not conform to application security best practices and standards. Although some of the vulnerabilities identified may be remediated with "quick fixes", the most critical required a fundamental redesign and rewrite of certain components of the application.

Given the fundamental nature of the vulnerabilities identified, Securus Global proposed that further exploitation of the application would provide minimal benefit to the company and that the focus of the remainder of the engagement should be dedicated to advising and assisting the development team with remediation of the specific issues identified as well as core iOS secure



development practices to further strengthen the fundamental security controls in the application to provide for a stronger foundation with which to build the application in the future.

The company agreed with this approach and Securus Global reached out to the development team to provide secure development advice. Once the suggested improvements had been implemented, Securus Global reassessed the application to find that the security of the application had been significantly improved and was now in line with the expectations of the company and befitting the sensitive nature of the information handled by the application.

In addition to technical remediation Securus Global recommended the company implement policies, frameworks and processes governing the end-to-end use of the application and mobile devices within the organisation and the board.

Business benefits

Technology initiatives such as this board papers application can provide significant benefit to the business in reduced costs, improved productivity and greater flexibility. However, poorly secured implementations can pose a significant risk to an organisation that, if realised, will offset these benefits.

Security assessment by an experienced team of professionals ensured that the company was able to implement the application with the confidence that financial, reputational and legal risks to both the company and the individual directors was appropriately managed with pragmatic security solutions that enabled, rather than hindered, the realisation of the business benefits.

Summary

New, innovative technologies are being adopted by businesses at a rapid pace as they seek to benefit from the advantages they can provide. These technologies, like all technology, can introduce significant security risks that may be exploited by malicious and opportunistic parties. It is important for businesses to understand the threats associated with mobile applications and how to develop and implement them in a secure manner.

More Information

Please reach out if you would like more information on how to effective manage the security implications of the technical change agenda of your organisation.

T: +61 (0) 2 9283 0255
E: info@securusglobal.com
www.securusglobal.com