Book Review

Securing the cloud: Cloud computer security techniques and tactics

Vic (J.R.) Winkler

Waltham, Massachusetts, 2011, vii + 290pp., \$59.95, ISBN: 978-1597495929 (Paperback).

Security Journal (2014) 27, 338–340. doi:10.1057/sj.2012.16; published online 6 January 2014

In *Securing the Cloud: Cloud Computer Security Techniques and Tactics*, Vic (J.R.) Winkler offers an important book for addressing security issues surrounding the growing use of cloud technology to share and transport files and information. Winkler draws on his 30 plus years of experience working with cyber security in various capacities to provide a detailed framework from which to understand cloud technology, different ways of securing data and networks, and positive and negative aspects of using a cloud. He addresses issues related to cloud computing and cloud services, exploring aspects of architecture, infrastructure, internal and external clouds, security, implementation, and continuous operation. He describes the numerous benefits that result from the pooling of resources, automation and patterns in infrastructure, such as decreased management staff, lower costs, increased start-up operations and opportunities for greater security. Winkler also talks about concerns related to cloud computing, including reliance on single providers, difficulties in migrating applications to the cloud, providers restricting access and failing to fulfill service obligations, and potential threats to security. Throughout the book, Winkler builds on this practical orientation by offering recommendations to cloud providers and subscribers to establish, select or administrate cloud technology.

Securing the Cloud consists of 10 chapters, each addressing different aspects of cloud structure, administration and security. Chapter 1 provides a general overview of cloud computing and security, including terminology, concepts of risk management and architecture, a brief history of different computing methods, and the current changes in computing driven by the expansive adoption of cloud technology. Chapter 2 addresses the general architecture of a cloud computing system. Chapter 3 deals specifically with the issues of security, risk management, and legal requirements for cloud providers and issuers.

Chapters 4 to 8 pertain directly to different aspects of cloud security. Chapter 4 describes the architectural requirements and elements of security architecture, focusing on ways to assess and ensure security in developing a cloud. Chapter 5 addresses data security, including data control, encryption, categorization and storage methods, and transfer to new service providers. Chapter 6 outlines best practices for cloud security, providing a number of important considerations for working with clouds. Chapter 7 and Chapter 8 address internal and external clouds, respectively. Internal clouds are private clouds created for use within an organization, while external clouds are developed and maintained by a central service

provider. These chapters address the structure and implementation of internal clouds and characteristics to consider when selecting an external cloud.

The final part of *Securing the Cloud* deals directly with evaluation and operation of a cloud. Chapter 9 focuses on evaluation of cloud security, offering a preliminary framework for analysis and checklists of questions for practitioners to consider when determining the strengths and weaknesses of their cloud. Chapter 10 discusses issues related to cloud implementation and operation. Winkler concludes with an overview of the main issues covered in the book, including a review of best practices, the benefits of using a cloud, and other resources to consult for professional networking and development.

Winkler provides practitioners with a critical review of the existing professional materials and resources to help establish a safe, secure and reliable cloud. Readers are able to grasp how a cloud functions, the specific elements of its architecture, possible ways security can be compromised, and how to address known problems with cloud computing and services. Diagrams and figures provided throughout the book supplement the text, and illustrate important concepts for readers. There are also many helpful references to external materials that readers can consult for further information, and stories that provide practical tips and sometimes humorous instances where the material being described has been applied. The lists of questions to consider are expansive, and provide good insights into issues a professional may not have considered otherwise. Winkler goes into specific detail while remaining sufficiently broad, providing not so much a list of requirements as an account of the many issues to consider when working with clouds, framing these issues in terms of organizational needs, resources, processes and outcomes. Ultimately, Winkler makes the case that the 'cloud model does force a movement toward a more robust and capable foundation of security services', which provides 'hope that we can regain control over gaps and issues that stem from poorly integrated or *after-thought security*' (pp. 25–26).

Although *Securing the Cloud* provides a decent overview of the topic, there are several limitations in terms of content, layout and presentation. The personal experience of the author represents both the strength and weakness in the writing, offering readers practical insight from years of work in the field, but with limited use of other resources and references. More concentrated effort to incorporate scholarly research (as opposed to personal experience, newspapers, magazines, technical reports and government documents) could add to the credibility of the arguments, particularly to back up claims of best practices, the benefits of cloud computing and the utility of certain security methods over others. The book makes numerous recommendations, perhaps to the point that readers may have difficulties determining what is most applicable to their situation. The book also tends to repeat itself, vexing the reader with pockets of similar material from previous sections. If the goal is to provide an overview to both the non-technically savvy novice and the computing expert, the result is mixed, achieving this goal in some areas and missing the mark in others. There contains a tremendous amount of technical language that will be difficult for new learners to fully understand, and a certain amount of prior background knowledge is expected to fully comprehend the specific details of cloud technology.

Despite these issues, the book should largely satisfy cloud security professionals, engineers and managers in their search for a volume to better prepare them for the changes and challenges that adapting to cloud computing will inevitably bring. *Securing the Cloud* will best serve companies' information technology (IT) professionals and experts interested in cyber security. It also provides interesting perspectives for academic researchers. It does

not constitute a step-by-step process of setting up a cloud, but a framework for what to consider when constructing a cloud. It summarizes and expands the knowledge base of this relatively new and not very well-understood technology. The implications for cyber-security, private and public organizations, government agencies, and individuals are numerous, including guidelines for how to understand the cloud structure to secure files, limit risk exposure and prevent criminal activity. The book expands the current knowledge base for organizational security, IT governance, computing technology, public and private policy, and the application of crime prevention techniques to Internet and computer crime. Although it does not focus exclusively on any of these issues and is written for a specific audience of IT specialists, the book is a useful and informative read for a wider audience of those interested in different computing services for their organization.

Brandon A. Sullivan
Michigan State University,
Michigan, USA