Chapter 2

Cloud Computing Security:
Abuse and Nefarious Use of Cloud Computing

Marwan Omar
Nawroz University, Iraq

ABSTRACT

The focus of this chapter is to highlight and address security challenges associated with the use and adoption of cloud computing. The chapter will describe how cloud computing has become an emerging and promising computing model that provides on-demand computing services which eliminates the need of bearing operational costs associated with deploying servers and software applications. As with any technology, cloud computing presents its adopters with security and privacy concerns that arise from exposing sensitive business information to unauthorized access. Also, this chapter will explore and investigate the scope and magnitude of one of the top cloud computing security threats "abuse and nefarious use of cloud computing" and present some of the attacks specific to this top threat as it represents a major barrier for decision makers to adopting cloud computing model. Finally, this chapter aims to serve as an introductory research effort to warrant more extensive research into this top threat and help researchers make recommendations to business organizations as to whether or not their data are vulnerable to such threat when deciding to join the cloud.

INTRODUCTION

Cloud computing is one of the revolutionary technologies that is expected to dominate and reshape the information technology industry in the near future (Rashmi, Sahoo, &.Mehfuz, 2013). This emerging computing technology provides highly scalable computing resources (e.g. information, applications, and transactions) in a way that is accessible, flexible, on-demand, and at a low cost (Eludiora, Abion, Oluwatope, Oluwaranti, Onime, &Kehinde, (2011); it provides unique opportunities for organizations to run business with efficacy and efficiency by allowing businesses to run their applications on a shared data center thus eliminating the need for servers, storage, processing power, upgrades, and technical teams. Furthermore; in cloud computing model, business organizations do not need to purchase any software products or services to run business because they can simply

DOI: 10.4018/978-1-4666-8387-7.ch002

subscribe to the applications in the cloud; those applications normally are scalable and reliable and ultimately allow business leaders to focus on their core business functions to enhance performance and increase profitability (Alam, Doja, Alam, & Malhotra (2013)).

Many organizations have become interested in the cloud computing concept due to many compelling benefits presented by this emerging computing paradigm (Aslam, Ullah, & Ansari (2010). Cloud computing vendors are offering scalable services and applications via centralized data centers utilizing thousands of server computers which provide easy access to computing resources anytime and anywhere (Aslam,Ullah, & Ansari (2010); the capability of cloud computing to quickly scale and provide access to computing services and resources anytime and anywhere, allowing organizations to quickly respond to changing business needs without the expenditures of time, space, money, personnel, and other resources needed for traditional infrastructures for example, New York newspaper organization were able to convert 11 million scanned and archived hard copies into pdf files in 24 hours by renting 100 servers from amazaon's cloud services at a cost to the organization was approximately $250. alternative methods for the conversion would have required cost and taken weeks or even months to complete. (Mongan, 2011).

While cloud computing offers enormous potential for reducing costs and increasing an organization's ability to quickly scale computing resources to respond to changing needs, there are risks associated with cloud computing (Alshammari, (2014)). Specifically, cloud computing may mean that an organization relinquishes control, resulting in exposure to breaches in confidentiality, losses in data integrity and availability. However; as with any technology, cloud computing has its own disadvantages such as releasing control of maintaining confidentiality, integrity, and availability of sensitive business data. In general, most cloud computing consumers want to be assured that cloud providers have effective security policies and controls in place to comply with data protection standards and meet regulatory compliance requirements prior to making a decision to migrate their data or applications to the cloud.

BACKGROUND

Cloud Deployment Models

According to cloud security alliance (2009) there are three cloud deployment models regardless of the service model adopted (SaaS, PaaS, and IaaS):

Public cloud: this is also called external cloud sometimes and it basically involves an organization that sells readily available cloud services to the general public. Business organizations with sensitive corporate data are reluctant to adopt this model because it increases the threat of exposing confidential data to unauthorized access by third parties and potential cyber criminals. The advantage of using the public cloud is that an organization itself does not have to manage the cloud computing infrastructure nor maintain operational activities. The disadvantage of utilizing the services from a public cloud provider is that it is entirely dependent upon another business entity that is offering resources through public cloud (Baber & Chauhan, 2011).

Private cloud: also referred to as internal cloud which means that cloud infrastructure and services are explicitly made available for a single organization. This deployment model can be located on premise or off site as it can also be managed by the organization itself or can be outsourced to a third party. Privately-hosted cloud services tend to be more costly but safer than other deployment models because organizations can retain control of their sensitive data and applications and implement their own security measures. The advantage for maintaining the private cloud is that an organization can retain full control of all the computing resources (e.g. applications, data, and systems)