BYOD and Governance of the Personal Cloud

Stuart Dillon, University of Waikato Management School, Hamilton, New Zealand
Florian Stahl, European Research Center for Information Systems, University of Münster, Münster, Germany
Gottfried Vossen, University of Waikato Management School, Hamilton, New Zealand & European Research Center for Information Systems, University of Münster, Münster, Germany

ABSTRACT

Cloud services are increasingly being used for a variety of purposes, including e-mail, social networking, music streaming, calendar management, file storage etc. In recent times the evolution of cloud services from private applications to corporate usage has been observed. This has led to the question of how private and business cloud services can be dual-accessed through a single device, in particular a mobile device that is used as part of a BYOD (Bring Your Own Device) policy. This paper considers the issues that arise from a consolidation of private and professional applications when accessed from a single device and introduces the term “personal cloud” to characterise such situations. It also presents an approach to cloud governance from a business perspective focusing in particular on security tokens, hardware keys and smart containers.

Keywords: Bring Your Own Device (BYOD), Cloud Computing, Cloud Governance, COPE, Personal Cloud

1. INTRODUCTION

Cloud services are increasingly being used for a variety of purposes, including e-mail, social networking, music and video streaming, calendar and portfolio management, file storage etc. Cloud computing is not new; indeed cloud services for non-business uses have existed for many years. However we have observed in recent times the evolution of private cloud services to corporate/business applications, many of which overlap business and private domains. An online calendar for example will typically show both private and professional appointments, and the employee may want to be able to access company files through a personal device, and vice versa. This paper studies the issues that arise from such a merge of private and professional applications on a single device, introduces the term “personal cloud” for such scenarios, and presents an approach to govern such clouds from a company perspective.

With increasing market penetration of (mobile and) smart devices such as smartphones, tablets, or laptops and owing to the ubiquitous (“always-on,”) nature of these devices, meaning

DOI: 10.4018/IJCAC.2015040102
that they have continuous and uninterrupted Internet access, private applications such as social networks and e-mail will more and more reside on the same device as corporate documents or applications such as company spreadsheets or proprietary software. Most commonly, both types of services are used interchangeably in both business and private environments, e.g., employees usually have a private and a corporate e-mail address, but both are accessed through a common interface or even using the same e-mail application. This observation is supported by the BYOD (“bring your own device”) development, where companies are allowing their employees to use their personal devices at work or for work-related purposes (Scarfo, 2012). Of the many benefits BYOD offers (both to organisations and their employees), and increase in flexibility and efficiency as well as the ability to work at anytime from anywhere are considered key (Morrow, 2012). The underlying philosophy of BYOD is in line with Mark Zuckerberg’s philosophy, implemented in Facebook, that every person has only one identity (as opposed to a private and a professional one). Indeed, in an interview with David Kirkpatrick for his book, “The Facebook Effect,” Zuckerberg is cited as saying “The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly. Having two identities for yourself is an example of a lack of integrity.” (Zimmer, 2010)

Even though this statement is controversial from a privacy point of view, the lack of integrity is particularly pertinent, especially from a technological perspective. By way of an example, consider the daily routine of a typical knowledge worker (e.g., a bank employee). While having breakfast she wants to check on her private and business e-mails. Today, it is very likely that she will do this on her smartphone, tablet, or on the rather new combination “phablet” (portmanteau from phone and tablet) using two different Web services, each with individual login. Also, a third and fourth application will be needed for calendar and (quality) news, all of which with potentially different credentials. In her office, after plugging her laptop into a docking station, she will access proprietary banking software, the same e-mail and calendar services, only via a different interface. She is likely to store some files on a company cloud storage solution. Heading for a customer presentation she grabs her laptop again which is obviously able to access the aforementioned cloud storage. Many interesting scenarios emerge from this setting: During a meeting, relevant company performance figures can be accessed; on the way home a presentation can be finalized on the train; during her lunch break a quick look can be taken at photos from a relative’s vacation; during a free moment, the remainder of last night’s movie can be watched. While this may still be viewed within the realms of science fiction to some, it is only the beginning of what will soon be everyday manifestations of our 24/7 hyper-connected world in which the distinction between private and professional life is vastly blurred (Schmidt and Cohen, 2013). In other words, people will soon be living in their “personal” cloud, a term that was first mentioned in a 2011 Forrester report in 2011 and also picked up by the Web blog readwriteweb.com around the same time.

A study reported in BITKOM (2013), the German Federal Association for Information Economy, Telecommunication and New Media (Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V., abbreviated BITKOM) shows that 43% of German IT and telecommunication companies allow their employees to connect their own devices to the company network. Almost 60% of these companies have established specific rules for this, 81% expect an increase in employee satisfaction, 74% expect increased productivity, while roughly 40% believe they will be perceived as a modern employer. On the other hand, 53% of the companies that were interviewed for this study declined the use of private devices in the workplace, mostly due to increased maintenance and security costs in the presence of a large variety of devices, differing operating systems, with all kinds of application
www.igi-global.com/article/security-issues-cloud-computing/58057?camid=4v1a