Business and Economics Journal
ISSN: 2151-6219

Lazarova, Bus Eco J 2016, 7:3
DOI: 10.4172/2151-6219.1000229

Short Communication Open Access

Managing Access to Cloud Services by Administrators in the Company

Vanya Lazarova*

University of National and World Economy, Sofia, Bulgaria

Abstract

After getting an access to cloud services, the company has to appoint staff to maintain this access. The administrator of cloud services is the employee who supports these operations. In order to perform their job, administrators acquire rights to access user data such as names, addresses, occupations, passwords and so on. The maintenance of user accounts is designed in a manner so that the consumers are protected in a situation like this - the administrators cannot access the user password if the user has changed it during the registration process. However, to carry out his normal activities, the administrator could change the current user password, even if he does not know it. This situation requires additional measures and regulation from the organization and the security department.

Keywords: Cloud services; Administrators; Management

Introduction

Cloud services are increasing every year. More and more companies are using them due to attractive prices and the wide range of highly professional services that suppliers provide. Along with the growth of cloud services, new problems arise. One of them is the access to the user data by authorized personnel - administrators in the company.

The interest in this problem has been growing lately because of the fast increasing the number and the powers of the administrator services. More and more rights are given to the administrators which requires special measures to be taken by the company management to protect their employees' data.

The administrators in the company who manage the access to the cloud services have many opportunities to manipulate user data, passwords and change them with or without permission from the users. The administrators need these rights to perform the work for which they were appointed - to keep an interrupted user access to the cloud services. To preserve user data, however, it is necessary to establish an additional organizational measures. Such measures would guarantee the consumer rights in case of unauthorized changes to the data and passwords by the cloud services administrators.

This article doesn't cover unauthorized access to the company's data in the cloud.

The subject of the article are Microsoft cloud services. Windows Azure Active Directory is a cloud-based platform, an extension of Microsoft Office365. Office365 users need to install the required software and register to receive the necessary license to use cloud services from Microsoft. The administrator functions in the Microsoft Windows Azure Active Directory system have to be identified. Users must know which functions have access to their accounts and the possibilities that are given to the administrators to access the data and the passwords in particular.

Microsoft Windows Azure Active Directory

Microsoft cloud services as all cloud services are subscription services - for them the company has to pay exactly as it pays subscription to the mobile phone operator or other utilities. In the same way as it happens to other services, when choosing a cloud service, the user has to choose subscription plan adjusted to his specific needs - how many data the user wants, how much server space, what kind of software, etc ... There are ready-made plans available, but the companies (users) can create individual plans, according to their specific needs.

Administrators maintain in working condition certain activities, processes and the entire system for access to cloud services. The number and type of the administrators who maintain cloud services have risen in recent years because the number and variety of the activities that must be performed have increased. Some of these activities are: create, configure and manage user accounts to individuals, organizations and employees within an organization; add new users; assigning different levels of user access to various services; synchronize access from different devices; maintain subscription services and custom plans to access these services; implementing and maintaining company data and much more. Administrators have different roles depending on what activities they maintain.

Administrator Role

The administrators of cloud services are also users (just like any other users) but with additional rights. The administrator would have the same permissions to the cloud services that company has subscribed to.

Microsoft's cloud services have many different administrators, divided into roles according to the activities that they support. These roles are (Figure 1): maintenance of the cloud accounts, general maintenance, maintenance of passwords, support for the cloud services and maintenance of the user accounts. It should be noted that a single administrator could perform several roles and might have rights to support various types of activities.

To understand which of these administrators have access to user data and who can manipulate them, the permissions that are inherent in each administrator role have to be considered.

Administrator Permissions

Billing administrator

Activities of this administrator are: purchasing packages for

***Corresponding author:** Vanya Lazarova, University of National and World Economy, Sofia, Bulgaria, Tel: 3592 8195211; E-mail: vlazarova@unwe.bg

Received February 22, 2016; **Accepted** June 25, 2016; **Published** July 05, 2016

Citation: Lazarova V (2016) Managing Access to Cloud Services by Administrators in the Company. Bus Eco J 7: 229. doi:10.4172/2151-6219.1000229

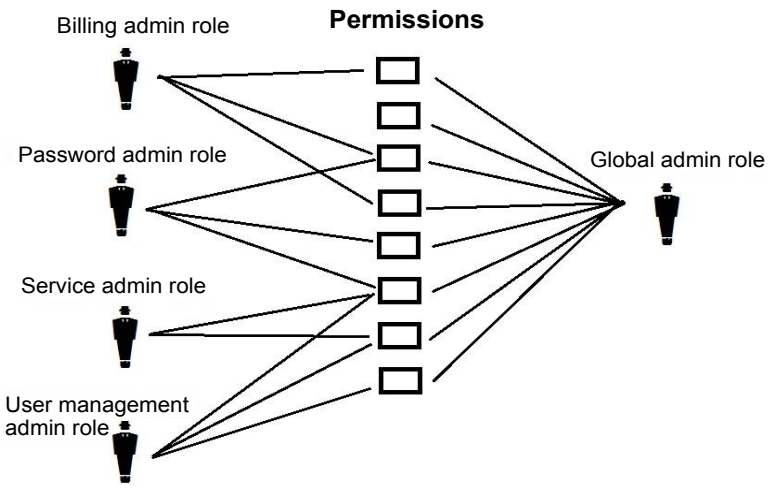

Figure 1: Roles of the administrators of the cloud services and their permissions.

cloud services; managing subscriptions; managing user accounts and carrying out general monitoring of this service. Billing administrators have permissions to view the information of the company and the users; could manage the subscription rights of users and could perform purchase and make payment of the Office365 software. But there are some forbidden activities for billing administrator. He (or she) cannot change passwords of the users; cannot create and manage users, groups and their licensing rights; cannot manage domains; cannot manage the information of the company; cannot assign administrator roles and cannot synchronize data [1].

Global administrator

Global Administrator has access to all administrative functions. The person who registers to buy the Office365 package becomes a global administrator. Only global administrator is entitled to give different roles to other administrators. There might be more than one global administrator in the company. Global Administrator has access to all administrative features, which are: manage the information of the company; manage the subscription rights of the users; purchase and payment of the Office365 products; change passwords of the users; create and manage users, groups and their licensing rights; manage domains; manage the information of the company; assign administrator roles; synchronize data and activate or deactivate multifactor authentication. There is no activity that global administrator cannot perform [2].

Password administrator

Password Administrator resets passwords, supports services that have access to the passwords. These administrators can assign passwords to users and other administrators. Password administrators have permissions to view the information of the company and the users; could manage the subscription rights of users. But there are activities that password administrators cannot do: cannot purchase and make payment of the Office365 products; cannot create and manage users, groups and their licensing rights; cannot manage domains; cannot manage the information of the company; cannot assign administrator roles and cannot synchronize data.

Service administrator

Service Administrators maintain requests for the cloud services and carries out general monitoring of this service. Service Administrators have permissions to manage the information of the company and to manage the subscription rights of users. There are some forbidden activities for billing administrator. He (or she) cannot reset passwords of the users; cannot purchase and pay for the Office365 products; cannot create and manage users, groups and their licensing rights; cannot manage domains; cannot manage the information of the company; cannot assign administrator roles and cannot synchronize data.

User management administrator

User Management Administrator resets passwords; creates and manages users; groups and their licensing rights and carries out general monitoring of this service. User Management Administrators have limited rights compared to the other administrators - they cannot set passwords of the global administrator, billing administrator and service administrator; they cannot delete a global administrator or create a new administrator. User Management Administrators have permissions to manage the information of the company and to manage the subscription rights of users but they have no permissions to purchase and pay for the Office365 products; cannot manage domains; cannot manage the information of the company; cannot assign administrator roles; cannot synchronize data and cannot a activate or deactivate multifactor authentication [3].

Each organization may distribute roles between administrators if its size is such that the work is too much for one person. It is technically possible, however, only one company administrator to perform all activities.

To ensure the operation of the cloud services the organization has the choice:

- to assign management of cloud services to organization administrators or
- to rely on a partner - Microsoft Partner – and to use delegated administration.

Microsoft Partner is a company certified by Microsoft to support their products. Microsoft Partner provides services worldwide, has a center that works around the clock and provides reliable maintenance for customers.

The management of the organization - consumer of cloud services has to determine who would maintain the access to the cloud services -

how many administrators are needed, or to entrust the administration of an external partner. There are many factors which have to be considered when determining the choice - number of users in the company, size of exchanging data with the cloud, frequency of access and of course last but not least the price of the service.

Administrators of cloud services in the company

The focus in this article is on the access to the user data by administrators of cloud services in the company. It is needed to determine which of the administrators have the authority to set and modify user data.

According to the roles of the administrators and the rights they have described above, it is clear that the global administrator, the password administrator and user management administrator have all rights to set and change user accounts and passwords.

Passwords can be set as follows: automatic; manual; for each user individually; to set the same password for all users; to set the same password for a group of users.

In the three administrator roles the administrator can gain access to the passwords only during their initial entry into the system. There are commands that could reveal all user data, but without passwords.

The administrator who initiates user access to the cloud services, sets the initial password and the system allows, if the administrator has enabled this feature as soon as the user acquires the password, to change it.

The administrator can use commands to display the status of the user account but there is no command that shows the password. No command through which one can display the current user password. Performing its normal activities, the administrator cannot see the user password if the password is changed.

However it is possible for the administrator to get access to the user data, even if the user has changed password and the new password is not known to the administrator. When performing normal activities, the administrator has to do this. Situations when user has forgotten the password occur often. The administrator has to re-establish the user access to cloud services. It appears possible to change the password of the user, even if it is not known. Administrator has to perform a few simple steps: all user data have to be exported in an external file; the administrator has to enter a new password in this file to replace the current password; the file has to be imported back into the system.

The administrator of the company has an option that helps him to perform the work for which he or she was appointed - to provide user access to cloud services, even in case of problems caused by the users themselves, but this option allows the administrator to access user data, even when the user does not want it.

This situation should be regulated with organizational tools within the company. For example, when the administrator has to change the password he/she must require a written request from the user. After changing the user password the administrator must also provide written notice to the user for the new password. There are other scenarios for this action - request and notice of change to be done by email - but it is clear that there must be some written rules in the company how to deal with such situations.

Conclusion

Within the organization, administrators manage cloud services depending on their role and perform many different activities. The global administrators, the password administrators and the user management administrators have access to the passwords of the users. If the company is not very big, all these activities can be performed by a company administrator. He has access to all user data without their current passwords if users have changed them in the process of registering in the system. There are rights granted to the administrators which are too risky - administrators can change the user password without actually knowing the current password. This and similar risk situations must be regulated within the company using various organizational methods.

If the organization does not create its own rules and restrictions for their implementation, there is a big danger that administrators can acquire too many opportunities for data collection and its undetected distribution as many cases recently were broadcasted in mass media.

References

1. Love C (2016) Assigning administrator roles in Azure Active Directory. Microsoft Azure, Microsoft, 03.
2. Markus V (2016) Understanding resource access in Azure. Microsoft Azure.
3. Jesper O (2016) Administrator roles in Office 365. Microsoft TechNet.