Managing User Access to Cloud Services by Company Administrators

Vanya Lazarova

University of National and World Economy, Sofia, Bulgaria

***Abstract* – The number and power of administrator services has been growing lately. 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 consumers are protected in a situation like this - administrators cannot access anyuser passwords if auser has changed it during the registration process. However, to carry out his normal activities, anadministrator canchange the current user password, even if he does not know it. This situation requires special measures to be taken by company's management to protect their employees' data.**

***Keywords* – cloud services,user access, administrator roles, administrator permissions.**

1. Introduction

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

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

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

This article does notcover unauthorized access to company's data in the cloud. The problems of access tocostumer's data via mobile devices [1] are very serious, and need special attention, which would be too much for this article.

The subject of the article are Microsoft cloud services [2]. Windows Azure Active Directory is a cloud-based platform, an extension of Microsoft Office365. Office365 users need to install required software and register to receive anecessary license to use cloud services from Microsoft [3]. Administrator functions in the Microsoft Windows Azure Active Directory system hasto be identified. Users must know which functions have access to their accounts and whichpermissionsare given to administrators to access data and passwords in particular.

Microsoft cloud services as all cloud services are subscription services - acompany has to pay for them exactly as it pays subscription to amobile phone operator or other utilities. As it is the case with other services, when choosing a cloud service, auser has to choose subscription plan adjusted to his specific needs –quantity of data, server space, kind of software, etc... There are ready-made plans available, but companies (users) can create individual plans, according to their specific needs.

Administrators maintain certain activities in a working condition, processes and the entire system for access to cloud services. The number and type of administrators who maintain cloud services have risen in recent years because the number and variety of activities that must be performed have increased. Some of these activities are: creating, configuringand managinguser accounts to individuals, organizations

DOI: 10.18421/TEM53-06
https://dx.doi.org/10.18421/TEM53-06

Corresponding author: Vanya Lazarova, University of National and World Economy, Sofia, Bulgaria
Email: vlazarova@unwe.bg

© 2016 Vanya Lazarova, published by UIKTEN.
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.
The article is published with Open Access at www.temjournal.com

and employees within an organization; adding new users; assigning different levels of user access to various services; synchronizing access from different devices; maintaining 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.

2. Roles of administrators of cloud services and their permissions

Administrators of cloud services are also users (just like any other users) but with additional rights. Anadministrator would have the same permissions to cloud services that a 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 (Fig. 1): maintenance of cloud accounts, general maintenance, maintenance of passwords, support for cloud services and maintenance of user accounts [4]. It should be noted that a single administrator could perform several roles and might have rights to support various types of activities.

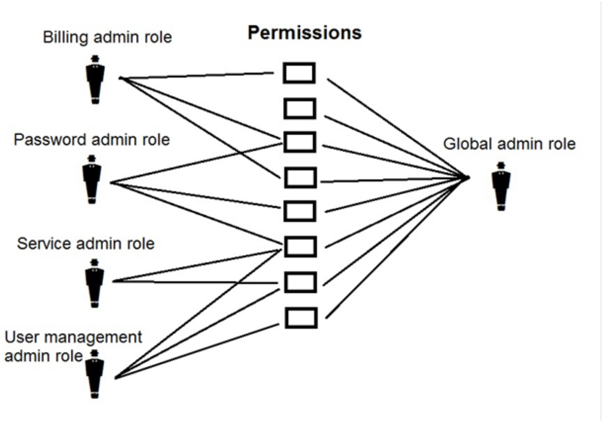


Figure 1.Roles of administrators

To understand which of these administrators have access to user data and who can manipulate them, the permissions (Fig. 2) that are inherent in each administrator role have to be considered.

Billing Administrator. Activities of this administrator are (Fig. 2): purchasing packages for cloud services; managing subscriptions; managing user accounts and carrying out general monitoring of this service. Billing administrators have permissions to view information of acompany and users; they canmanage subscription rights of users and perform purchases and initiatepayment forthe Office365 software. But there are some forbidden activities that abilling administrator can perform. He (or she) cannot change passwords of users; cannot create and manage users, groups and their licensing rights; cannot manage domains; cannot manage information of acompany; cannot assign administrator roles and cannot synchronize data.

Global Administrator.A Global Administrator has access to all administrative functions. A person who registers to buy Office365 package becomes a global administrator. Only the global administrator is entitled to give different roles to other administrators. There might be more than one global administrator in acompany. The Global Administrator has access to all administrative features, which are (Fig. 3): managing information of a company; managing subscription rights of users; purchasing Office365 products; changing passwords of users; creating and managing users, groups and their licensing rights; managing domains; assigning administrator roles; synchronizing data and activating or deactivating multifactor authentication. There is no activity that global administrator cannot perform.

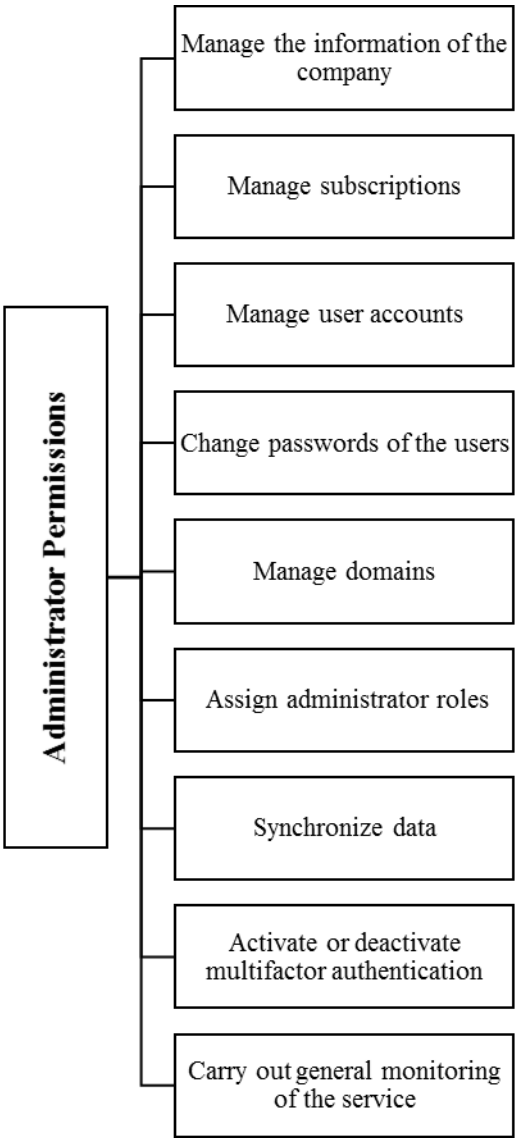

Administrator Permissions
Manage the information of the company
Manage subscriptions
Manage user accounts
Change passwords of the users
Manage domains
Assign administrator roles
Synchronize data
Activate or deactivate multifactor authentication
Carry out general monitoring of the service

Figure 2. Permissions of the administrators

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

Service Administrator. A Service Administrator maintains requests for cloud services and carries out general monitoring of this service. Service Administrators have permissions to manage information of acompany and subscription rights of users. There are some forbidden activities for service administrators [5]. He (or she) cannot reset passwords of users; cannot purchase Office365 products; cannot create and manage users, groups and their licensing rights; cannot manage domains; cannot manage information of acompany; cannot assign administrator roles and cannot synchronize data.

User Management Administrator. A 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 forthe 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 information of acompany and subscription rights of users but they have no permissions to purchase Office365 products; cannot manage domains; cannot manage information of acompany; cannot assign administrator roles; cannot synchronize data and cannot activate or deactivate multifactor authentication.

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, for only one company administrator to perform all activities.

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

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

The management of an organization - consumer of cloud services has to determine who would maintain access to cloud services - how many administrators are needed, or entrust administration of an external partner. There are many factors which have to be considered when determining the choice - number of users in acompany, size of exchanging data with the cloud, frequency of access and of course last but not least important, price of the service.

3. Company administrators of cloud services

The focus in this article is on the access to the user data by administrators of cloud services in acompany. It is needed to determine which administrators have the authority to set and modify user data [6].

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

There are many tools that help administrators to manage their job. PowerShell for Office 365 scripts are one of those tools that canlet us see how this could be done.

Administrators can simultaneously upload many users to a cloud system using previously created information CSV file (Partisipanrs1.csv in the example).

PowerShell script commands [7] are performed consecutively (Table 1):

Table 1.PowerShell scripts for initial user entry

```
Import-Module MSOnline
$credential = get-credential
Connect-MsolService -Credential $credential

Import-Csv Partisipanrs1.csv | ForEach-Object
{ New-MsolUser -UserPrincipalName
$_.UserPrincipalName -FirstName
$_.FirstName -LastName $_.LastName -
DisplayName $_.DisplayName -Title $_.Title -
Password $_.PassWord -Department
$_.Department -Office $_.Office -MobilePhone
$_.MobilePhone -StreetAddress
$_.StreetAddress -City $_.City -State $_.State -
PostalCode $_.PostalCode -Country $_.Country
}
```

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.

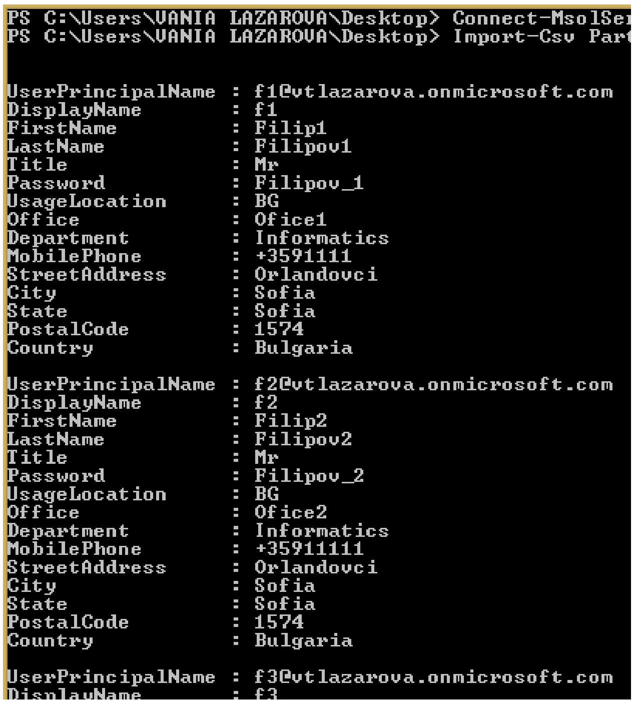
The parameters are set in the script exactly in the same order in which they are in the prepared csv file. The result of execution of the script is a list of users with their names, addresses, occupations, phone numbers and passwords (Fig. 3).

Administrators can access to the passwords only during their initial entry into the system, when executing the script Import-Csv.

There are commands that canreveal all user data, but without passwords.

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

An administrator can use commands to display the status of a user account but there is no command that shows the password. Current user password cannot be displayed, there is no such command. Performing his normal activities, an administrator cannot see user's password if the password has been changed.



```
PS C:\Users\VANIA LAZAROVA\Desktop> Connect-MsolSe
PS C:\Users\VANIA LAZAROVA\Desktop> Import-Csv Par


UserPrincipalName  : f1@vtlazarova.onmicrosoft.com
DisplayName        : f1
FirstName          : Filip1
LastName           : Filipov1
Title              : Mr
Password           : Filipov_1
UsageLocation      : BG
Office             : Ofice1
Department         : Informatics
MobilePhone        : +3591111
StreetAddress      : Orlandovci
City               : Sofia
State              : Sofia
PostalCode         : 1574
Country            : Bulgaria

UserPrincipalName  : f2@vtlazarova.onmicrosoft.com
DisplayName        : f2
FirstName          : Filip2
LastName           : Filipov2
Title              : Mr
Password           : Filipov_2
UsageLocation      : BG
Office             : Ofice2
Department         : Informatics
MobilePhone        : +35911111
StreetAddress      : Orlandovci
City               : Sofia
State              : Sofia
PostalCode         : 1574
Country            : Bulgaria

UserPrincipalName  : f3@vtlazarova.onmicrosoft.com
DisplayName        : f3
```

Figure 3.Complete user information

However, it is possible for an administrator to get access to user data, even if auser has changed password and the new password is not known to the administrator [6]. When performing normal activities, an administrator has to do this. Users often forget their passwords. An administrator has to re-establish user's access to cloud services. It is possible to change the password of auser, even if it is not known. An administrator has to perform a few simple steps: all user data have to be exported toan external file; an 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.

An administrator has to output user data to an external file, in the example (Table 2) the name of this file is 111.csv, then has to load on a single variable ($ PASS) new password invented by him (DDDD_4444) and then has to reimport the same file into the system [8].

Table 2.PowerShell scripts change password

```
Get-MsolUser | Where { $_.UserPrincipalName
-eq "d4@vtlazarova.onmicrosoft.com" } | select
UserPrincipalName | Export-Csv 111.csv –
NoTypeInformation

$PASS = 'DDDD_4444'

Import-Csv 111.csv | % {Set-
MsolUserPassword -userPrincipalName
$_.UserPrincipalName -NewPassword $PASS -
ForceChangePassword $True}
```

It is clear that through some simple steps user passwords can be changed and user would not know.

An administrator of acompany has an option that helps him perform 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 auser does not want it.

This situation should be regulated with organizational tools within a company. For example, when an administrator has to change a password he/she must require a written request from a 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 acompany how to deal with such situations.

4. Conclusion

Within an organization, administrators manage cloud services depending on their role and perform many different activities. Global administrators, password administrators and user management administrators have access to passwords of users. If acompany 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 administrators which are too risky - administrators can change user passwords without actually knowing the current password. This and similar risk situations must be regulated within a company using various organizational methods.

If an 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]. Clarke, N. L., & Furnell, S. M. (2007). Advanced user authentication for mobile devices. *computers & security*, *26*(2), 109-119.

[2]. C. Love, "Microsoft Azure," Microsoft, 03 2016. [Online]. Available: https://azure.microsoft.com/en-us/documentation/articles/active-directory-assign-admin-roles/.

[3]. Markus Vilcinskas, "Microsoft Azure," [Online]. Available: https://azure.microsoft.com/en-us/documentation/articles/active-directory-understanding-resource-access/. [Accessed 02 06 2016].

[4]. Gremban, Kelly. (2016, 07 12). Roles in Azure AD Privileged Identity Management. Retrieved from Microsoft Azure: https://azure.microsoft.com/en-us/documentation/articles/active-directory-privileged-identity-management-roles/.

[5]. Thomas Lin, "Microsoft Azure," Microsoft, 03 2016. [Online]. Available:https://azure.microsoft.com/en-us/documentation/articles/billing-add-change-azure-subscription-administrator/ . [Accessed 12 07 2016].

[6]. Jesper Osgaard,, „Microsoft TechNet," [Online]. Available: https://blogs.technet.microsoft.com/lystavlen/2012/04/10/administrator-roles-in-office-365/ . [Accessed 02 06 2016].

[7]. "Script Samples," [Online]. Available: http://powershell.office.com/script-samples/importing-users-detailed. [Accessed 04 06 2016].

[8]. "Script Samples," [Online]. Available: http://powershell.office.com/script-samples/bulk-set-passwords-for-users. [Accessed 12 07 2016].