TESINA – CORSO CYBERSECURITY 2021/2022

Sistemi Office365: Teams Information Barriers

studio proposto da @Avanade

MARIO CUOMO

Sommario

ABSTRACT

Gli obiettivi principali della sicurezza informatica sono principalmente 3: garantire la confidenzialità, integrità e disponibilità dei dati. Tra i vari strumenti messi a disposizione da Microsoft per assicurare la confidenzialità si ha *Information Barries*, appartenente alla suite Microsoft 365 – un set di strumenti per la produttività, gestione aziendale, sicurezza e conformità.

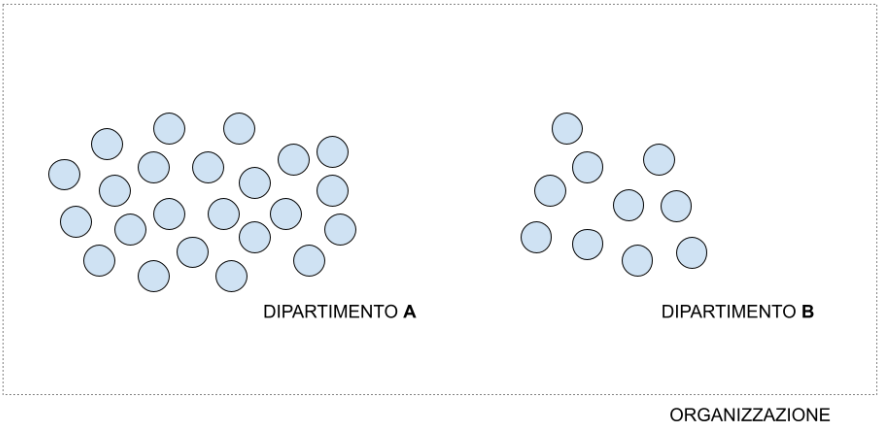
I sistemi informatici acquisiscono una quantità enorme di dati e l'attenzione verso questi è fondamentale. Nel contesto di produttività aziendale per dato si intende qualsiasi risorsa utile a svolgere le proprie attività; molto spesso tali risorse sono condivise in strumenti di collaborazione, come per esempio Microsoft Teams.
Lo scopo di *Information Barries* è quello di fare in modo tale che le risorse siano condivise solamente tra gli aventi diritti di accesso limitandone la diffusione – anche all'interno della stessa organizzazione. L'implementazione delle barriere per le informazioni può essere realizzata sia per motivi legislativi – per esempio la conformità a direttive come può essere il GDPR del 2018 – ma anche per politiche interne aziendali – per esempio limitando la possibilità di comunicazione tra due reparti quali quello dell'amministrazione e quello commerciale.
Information Barriers pemette di proteggere le informazioni all'interno delle organizzazioni ponendo l'attenzione verso la compliance piuttosto che verso l'identità e la sicurezza, definendo chi è autorizzato o no a condividere del contenuto con chi.

Anche se è possibile applicare le barriere di informazione a diversi strumenti, come *SharePoint* e *OneDrive*, il seguente elaborato pone l'attenzione verso la piattaforma *Microsoft Teams*.

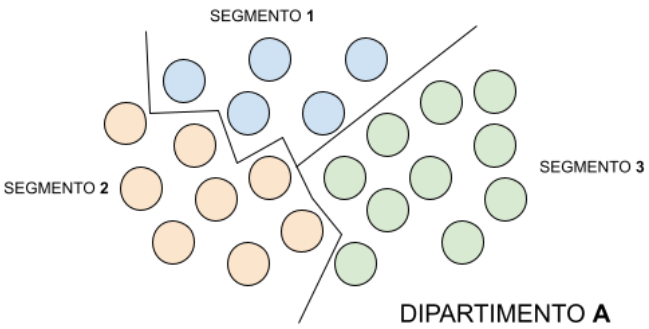
IMPLEMENTAZIONE AD ALTO LIVELLO

Uno dei concetti principali quando si lavora con le barriere di informazioni è quello di *segmento*. Un segmento identifica univocamente un gruppo di utenti.
Identificare i segmenti è un'operazione non banale: un utente può appartenere a uno e uno solo segmento e a ognuno di essi può essere applicato un solo criterio.

Nei casi più semplici un segmento può essere identificato a partire da una caratteristica intrinseca degli utenti come per esempio l'appartenenza a un dipartimento piuttosto che a un altro.
Le proprietà che possono essere utilizzate sono tutte quelle utilizzate in *Azure Active Directory*, un servizio di gestione delle identità sul cloud di Microsoft.



Operazione più complessa si ha nel caso in cui si voglia effettuare una segmentazione a una grana più fine, per esempio segmentando gli utenti appartenenti allo stesso dipartimento e non avendo una feature discriminante per essi. In tal caso è possibile definire proprietà custom.



Una volta identificati e definiti i segmenti è necessario stabilire il criterio per limitare la comunicazione tra questi.
Si noti come le *policy* sono bidirezionali: se si vuole bloccare la comunicazione tra il segmento 1 e il segmento 2 è necessario definire due criteri per entrambi i flussi di comunicazione da un segmento all'altro.

In genere la definizione e l'attivazione delle policy avviene in due momenti temporali distinti, spesso dopo una accurata revisione dei criteri definiti, in quanto l'attivazione di questi non è immediata ma richiede una manciata di ore.

SCENARIO AZIENDALE DI ESEMPIO

Come scenario aziendale di esempio per i casi d'uso 1 e 2 ho considerato il tenant Office 365 dell'Università degli Studi Roma Tre.

Effettuando una ricerca degli utenti utilizzando Microsoft Teams ho notato che è possibile iniziare una nuova conversazione con qualsiasi categoria di persona che possiede una utenza di Office 365 del tenant dell'ateneo *@[xxx].uniroma3.it*.
Il personale della segreteria per esempio può iniziare una conversazione con un professore in qualsiasi momento. Lo stesso può succedere tra il personale dell'amministrazione e gli studenti.

Si vuole evitare questa situazione in quanto è possibile che utenti non autorizzati entrino in possesso di dati sensibili condivisi erroneamente all'interno della piattaforma Microsoft Teams. Si pensi per esempio un amministratore che voglia condividere un file su Teams a un altro amministratore ma sbaglia l'utenza – inviandolo a uno studente – a causa di una omonimia.

Per semplicità si consideri l'organizzazione così formata:

DIPARTIMENTO	NUMERO DI UTENTI
INGEGNERIA	32
STUDI UMANISTICI	26
AMMINISTRAZIONE	5
SEGRETERIA	2
TESORERIA	4

In modo ancora più semplicistico si consideri di avere come uniche informazioni degli utenti il *nome*, *cognome* e *dipartimento* di appartenenza.

NOME	COGNOME	DIPARTIMENTO
MARIO	ROSSI	INGEGNERIA
LUCA	VERDI	STUDI UMANISTICI
…	…	…

Allo stato attuale ogni utente di ogni dipartimento può iniziare una nuova conversazione con ogni altro utente.
Nel caso d'uso 1 è mostrato come bloccare la comunicazione tra segmenti: gli studenti di *Ingegneria* e di *Studi Umanistici* non potranno interagire con il personale dell'*Amministrazione*.
Nel caso d'uso 2 è mostrato come isolare la comunicazione da e verso l'esterno di un segmento: il personale della *Tesoreria* è in grado di condividere dati solo tra il gruppo stesso.

OPERAZIONE PRELIMINARE – CONNESSIONE AL SECURITY & COMPLIANCE CENTER

L'applicazione di *Information Barries* avviene via script tramite *PowerShell*, una shell di comandi che utilizza l'omonimo linguaggio di scripting basato sul *.NET Common Language Runtime*.

La prima operazione da effettuare è quella di aprire una connessione con il *Centro sicurezza e conformità*.

```
Connect-IPPSSession -UserPrincipalName m.cuomo@tinghios.onmicrosoft.com

Connect-AzureAD -Tenant "tinghios.onmicrosoft.com"
```

Una volta effettuata la connessione è necessario fornire il consenso all'*Infomation Barrier Processor* ad accedere alle informazioni dell'applicazione e del tenant di interesse.

```
$appId="bcf62038-e005-436d-b970-2a472f8c1982"

$sp=Get-AzADServicePrincipal -ServicePrincipalName $appId

if ($sp -eq $null) { New-AzADServicePrincipal -ApplicationId $appId }

Start-Process
"https://login.microsoftonline.com/common/adminconsent?client_id=$appId"
```

Da questo momento è possibile definire segmenti e policy.
I casi d'uso descritti di seguito non riportano la fase di connessione e autenticazione, operazione preliminare in ogni caso.

CASO D'USO 1 – BLOCCO COMUNICAZIONE VERSO UN GRUPPO INTERNO SPECIFICO

La policy che si vuole implementare in questo caso è molto semplice: gli studenti appartenenti ai dipartimenti di *Ingegneria* e *Studi Umanistici* non possono condividere informazioni con il personale dell'*Amministrazione.* Allo stesso modo l'*Amministrazione* non può iniziare una conversazione con i due dipartimenti.
Si pensi a una politica in cui è necessario contattare la segreteria come proxy tra le due entità.

Il primo passaggio da effettuare è quello di definire i 3 *segmenti* di utenti.
La segmentazione avviene sulla base della proprietà *Department* associata a ogni utente.

```
New-OrganizationSegment -Name "Ingegneria" -UserGroupFilter "Department -eq
'Ingegneria'"

New-OrganizationSegment -Name "StudiUmanistici" -UserGroupFilter "Department
-eq 'Studi Umanistici'"

New-OrganizationSegment -Name "Amministrazione" -UserGroupFilter "Department
-eq 'Amministrazione'"
```

Una volta definiti i segmenti si definiscono i criteri che si vogliono implementare.
I criteri possono essere principalmente di 2 categorie differenti: i criteri *bloccanti* che impediscono la comunicazione tra segmenti e i criteri di tipo *consenti* che permettono la comunicazione solo i segmenti specificati.

In questo caso d'uso sarà utilizzato un criterio di blocco.

```
New-InformationBarrierPolicy -Name "Ingegneria-Amministrazione" -
AssignedSegment "Ingegneria" -SegmentsBlocked "Amministrazione" -State
Inactive
```

Il comando sopra descritto crea un policy di nome `Ingegneria-Amministrazione` assegnata al segmento `Ingegneria`, è di tipo bloccante nei confronti del segmento `Amministrazione`.
La policy è non attiva: non si ha ancora nessun effetto sugli utenti.

Il blocco appena realizzato è *unidirezionale*, blocca la comunicazione da qualsiasi account del dipartimento di *Ingegneria* verso qualsiasi account del dipartimento dell'*Amministrazione*.
Per fare un blocco bidirezionale è necessario definire un secondo criterio, simile al precedente.

```
New-InformationBarrierPolicy -Name "Amministrazione-Ingegneria" -
AssignedSegment "Amministrazione" -SegmentsBlocked "Ingegneria" -State
Inactive
```

Così come è stato fatto per il dipartimento di *Ingegneria*, devono essere creati altri 2 criteri di blocco delle informazioni per quanto riguarda la comunicazione da *Amministrazione* a *Studi Umanistici* e viceversa (chiamati rispettivamente `Amministrazione-StudiUmanistici` e `StudiUmanistici-Amministrazione`).

In modo più elegante e pulito è possibile realizzare il tutto con 3 policy unendo in un unico criterio il blocco della comunicazione che parte dagli utenti dell'*Amministrazione*.
La documentazione ufficiale – docs.microsoft.com/it-it/microsoft-365/compliance/information-barriers-policies – suggerisce di non assegnare più di un criterio a ogni segmento per migliorare l'analisi ed essere più facilmente compliant alle normative interne ed esterne all'organizzazione.

```
New-InformationBarrierPolicy -Name "Amministrazione-
StudiUmanisticiIngegneria" -AssignedSegment "Amministrazione" -
SegmentsBlocked "Ingegneria","StudiUmanistici" -State Inactive
```

La situazione generale è la seguente

DA \ A	INGEGNERIA	STUDI UMANISTICI	AMMINISTRAZIONE	SEGRETERIA	TESORERIA
INGEGNERIA	✓	✗	✗	✓	✓
STUDI UMANISTICI	✓	✓	✗	✓	✓
AMMINISTRAZIONE	✗	✗	✓	✓	✓
SEGRETERIA	✓	✓	✓	✓	✓
TESORERIA	✓	✓	✓	✓	✓

L'attivazione delle policy avviene in modo esplicito dopo la creazione di queste, anche a distanza di tempo.

Per verificare lo stato corrente di tutte le policy definite è possibile utilizzare il seguente comando

```
Get-InformationBarrierPolicy
```

Ogni policy è caratterizzata da un *nome* – specificato in fase di creazione – e da un *GUID* – assegnato dal sistema.
Per rendere effettivamente attivo un criterio si lavora come segue.

```
Set-InformationBarrierPolicy -Identity "Amministrazione-
StudiUmanisticiIngegneria" -State Active
```

La policy sarà applicata per ogni utente dei segmenti coinvolti: ne deriva che se l'organizzazione è molto grande il processo di attivazione può richiedere un tempo anche dell'ordine di una giornata. Viceversa, è possibile bloccare il processo di attivazione di una policy in modo rapido – tempo stimato una mezz'ora.

```
Stop-InformationBarrierPoliciesApplication -Identity <GUID>
```

CASO D'USO 2 – ISOLAMENTO DEGLI UTENTI DI UN GRUPPO RISPETTO L'INTERA ORGANIZZAZIONE

Nel caso d'uso 2 si vuole implementare un criterio bloccante da un segmento verso tutti gli altri. Il segmento che è preso in considerazione è quello del dipartimento della *Tesoreria*: dati sensibili monetari dovrebbero rimanere ben confinati e non divulgati ai non autorizzati.
Gli utenti della *Tesoreria* potranno comunicare solamente tra di loro.

Per prima cosa si crea un segmento, come visto nel caso d'uso 1

```
New-OrganizationSegment -Name "Tesoreria" -UserGroupFilter "Department -eq
'Tesoreria'"
```

Per realizzare l'isolamento degli utenti del segmento verso tutti gli altri utenti si può procedere in due modi. Il primo consiste nel creare $n-1$ policy (se n sono i numeri di segmenti individuati): tale strategia è molto onerosa in termini di tempo e va contro al principio fondante tale per cui a ogni segmento deve essere applicato una solo criterio. L'individuazione di un nuovo segmento comporta le modifica dei criteri già definiti.
Il secondo modo per realizzare un isolamento di questo genere è l'utilizzo di una policy di tipo *acconsenti*: quando si realizza una tale policy si dichiarano solo i segmenti con i quali è consentita la comunicazione (che in questo caso non ce ne sono, se non il segmento stesso).

```
New-InformationBarrierPolicy -Name "Tesoreria-to-Tesoreria" -AssignedSegment
"Tesoreria" -SegmentsAllowed " Tesoreria" -State Inactive
```

La situazione generale è la seguente

A / DA	INGEGNERIA	STUDI UMANISTICI	AMMINISTRAZIONE	SEGRETERIA	TESORERIA
INGEGNERIA	✓	✓	✓	✓	✗
STUDI UMANISTICI	✓	✓	✓	✓	✗
AMMINISTRAZIONE	✓	✓	✓	✓	✗
SEGRETERIA	✓	✓	✓	✓	✗
TESORERIA	✗	✗	✗	✗	✓

Valgono gli stessi accorgimenti visti per il caso 1 riguardo l'attivazione della policy e le tempistiche previste.

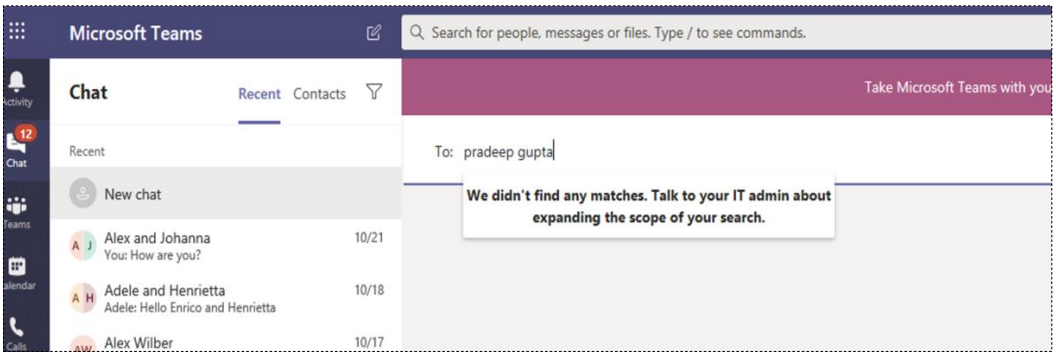
EFFETTI DELL'APPLICAZIONE DI INFORMATION BARRIERS

Si è visto come bloccare la condivisione e la comunicazione tra segmenti ma non si è specificato esplicitamente cosa questo comporti.
Tra gli effetti di *Information Barriers* sui vari strumenti *SharePoint Online* e *OneDrive for Business* il focus di questo elaborato è sulla piattaforma *Microsoft Teams*.

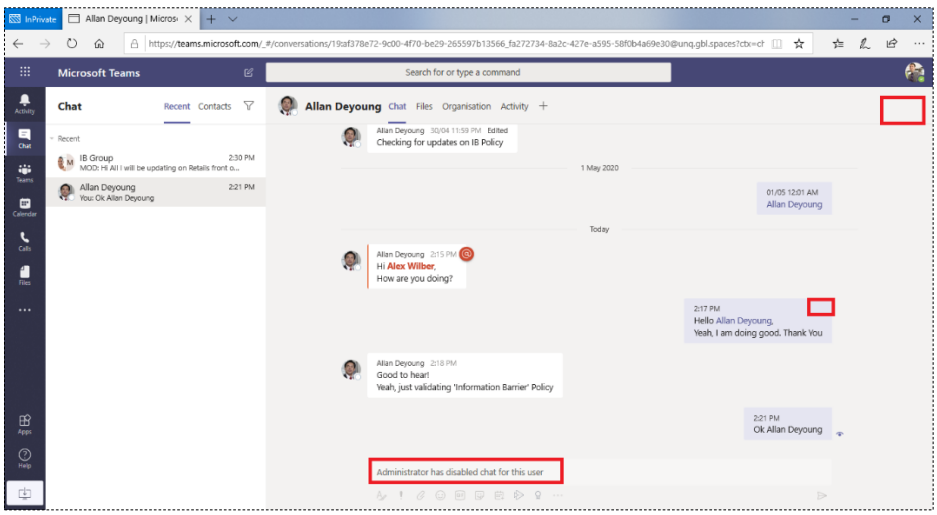
Considerando una policy bloccante tra il segmento *A* e il segmento *B,* esempi di blocchi che possono avvenire sono i seguenti:

- Un utente a del segmento *A* vuole iniziare una conversazione con un utente b del segmento *B*.
  Quando l'utente a ricerca il nome dell'utente b in *Microsof Teams* tale utente non è trovato. Non si è avvertiti esplicitamente dell'esecuzione di *Information Barriers* ma si è invitati a contattare l'amministratore per provare ad espandere il dominio di ricerca.

  Lo stesso avviene quando a prova ad aggiungere b a un team.



- Se in precedenza non era definito nessun criterio tra i segmenti, è probabile che un utente a del segmento *A* abbia comunicato in precedenza con un utente b del segmento *B.*
  Dal momento in cui si attiva la policy la chat (messaggi, chiamate, video chiamate e condivisione schermo) tra i due è disabilitata.



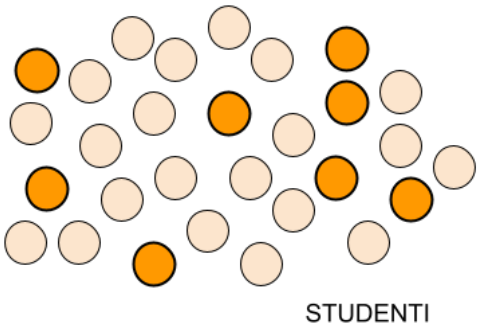
CASO D'USO 3 – SEGMENTAZIONE DEGLI UTENTI UTILIZZANDO FEATURES DI SUPPORTO

Una delle maggiori complessità quando si lavora con le barriere delle informazioni è il vincolo che un utente può appartenere al più a un segmento.
In realtà più che un vincolo è una forte raccomandazione: si immagini la situazione in cui un utente appartiene a due segmenti differenti (segmento *A* e segmento *B*). I segmenti in questione hanno due politiche contrasti nei confronti di un terzo segmento *C*: *A* può comunicare con C, *B* non può comunicare con *C*.
Dato che non è definita univocamente la policy per l'utente si potrebbe avere un comportamento anomalo nella comunicazione.

Laddove non è possibile rispettare il vincolo della segmentazione utilizzando le caratteristiche intrinseche dell'utente – sede geografica, dipartimento, etc – si può ricorrere all'applicazione di features personalizzate ad hoc.

Il caso d'uso 3 considera il seguente scenario: si vuole raggruppare una élite di studenti di *Ingegneria* e *Studi Umanistici* per un progetto privato. Si vogliono mantenere le utenze già esistenti con la policy che gli utenti élite siano isolati dai restanti studenti.
È possibile segmentare gli utenti utilizzando uno dei 14 attributi personalizzati messi a disposizione per ogni utenza in *Azure Active Directive*.
Per aggiungere gli *extensive attributes* si può utilizzare PowerShell come segue.

```
Set-ADUser C.<identificativoUtente> -Add @{extensionAttribute1 = <valore>}
```



A questo punto si possono creare i segmenti utilizzando come discriminante la nuova feature e successivamente si possono impostare le *barrier policies* – nel caso specifico di tipo *allowed* che permettono la sola comunicazione tra i membri interni e non verso quelli esterni (così come visto per il caso d'uso 2).

INFORMATION BARRIERS PER ONEDRIVE E SHAREPOINT

Microsoft Teams non è l'unico strumento su cui si ripercuote applicazione di *Information Barriers*; altre due applicazioni sono OneDrive e SharePoint: principalmente due strumenti per gestire documenti in cloud. La differenza sostanziale è dovuta dal fatto che il primo – anche nella sua versione *for Business* – ha il focus per lo storage di documenti personali, mentre il secondo pone l'accento per la condivisione e il lavoro di gruppo anche attraverso la realizzazione di siti web (*intra* ed *extra net*).

SHAREPOINT

Applicando i criteri per le barriere delle informazioni a dei segmenti si può far in modo di isolare siti web, negando la possibilità di aggiungere utenti al sito e togliendo la possibilità di visionarlo – completamente o in parte – a utenti non autorizzati.

Si hanno 4 modalità di *Information Barrier* che si possono applicare ai siti di *SharePoint*:

- OPEN
  è la modalità di default, senza restrizioni.
  Un utente può condividere i contenuti sulla base delle proprie barriere: se l'utente appartiene a un segmento *A* e tale segmento non può comunicare col segmento *B*, allora l'utente non sarà in grado di condividere il contenuto con un utente di quel segmento.

- OWNER MODERATE
  con questa modalità il contenuto del sito web può essere condiviso solo tra i membri del sito stesso.
  Solo il moderatore ha la possibilità di condividerlo esternamente – rispettando comunque i vincoli imposti dalle barriere delle informazioni.

- IMPLICIT
  la modalità *implicit* è impostata di default quando si assegna un sito a un team di *Microsoft Teams.* Questo implica che il sito può essere condiviso – così come il suo contenuto – solo tra gli utenti del team stesso.
  Un nuovo utente può essere aggiunto al sito tramite il portale di *Microsoft Teams.*

- EXPLICIT
  la modalità *explicit* è impostata di default quando si assegna un sito a un segmento.
  Il sito e il contenuto possono essere condivisi solo tra gli utenti del segmento.
  Un nuovo utente può essere aggiunto al sito solo se appartiene al segmento associato.

RISORSE ESTERNE & RIFERIMENTI

Il materiale utilizzato per realizzare l'elaborato deriva in gran parte dalla documentazione ufficiale di Microsoft 365 - *https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers* e dalla mini-guida di Microsoft Learn - *https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers*.

I casi d'uso presentati traggono ispirazione dalla realtà universitaria di interesse @Roma Tre.

I PowerShell script sono disponibili nel seguente repository GitHub