WIKIPEDIA

Identity management

Da Wikipedia, l'enciclopedia libera.

Con **Identity Management (IM)** si intendono i sistemi integrati di tecnologie, criteri e procedure in grado di consentire alle organizzazioni di facilitare - e al tempo stesso controllare - gli accessi degli utenti ad applicazioni e dati critici, proteggendo contestualmente i dati personali da accessi non autorizzati.

Indice

Caratteristiche

Sono molti i software e sistemi che offrono servizi di Identity Management: come la maggior parte dei software ne esistono sia a pagamento che open source. Di qualunque tipo siano, questi sistemi offrono un insieme di servizi, più o meno diversificati, più o meno completi; i principali sono:

- Account Management
- Compliance Management
- Multifactor Authentication
- Single Sign On
- Password Management
- User Activity Monitoring
- Role Management

Account Management

L'**Account management** è un servizio che permette di creare e gestire i profili degli utenti che utilizzano un sistema informatico. Alla creazione di un dato account vengono eventualmente associati(in relazione al *multifactor authentication*) un badge, un'impronta digitale o una qualsiasi altra informazione che, assieme alla password, permettono l'autenticazione. Ad ogni account verranno(generalmente) forniti dei "privilegi", che gli permettono di accedere a parti definite del sistema e/o della rete(*role management*), e quindi fornire servizi personalizzati; inoltre verranno continuamente monitorati al fine di evitare qualsiasi tipo di problema, legale(*compliance management*) o di qualsiasi altra natura.

Compliance Management

Il **Compliance Management** (gestione della conformità) è l'insieme dei processi, interni ad un'organizzazione, volti a monitorare le attività degli utenti, con il fine di garantire sempre il rispetto delle norme vigenti. Questi processi possono essere di diversa natura, ma si dividono principalmente in due categorie:

- ' *I Dieci Comandamenti* ', modello rigoroso che spesso, però, lascia spazio ad un ricorso minimo in caso di trasgressioni
- ' *Gestione della qualità* ', modello che permette di 'adattare'(o fare eccezioni), in casi particolari, le normative in modo di permettere alle aziende di lavorare nelle migliori condizioni possibili

Multifactor Authentication

Il **Multifactor Authentication** è un sistema che combina due o più credenziali per l'identificazione di un utente:

- *qualcosa che so*, ovvero un'informazione che l'utente deve fornire per poter accedere, come una password, un PIN o la risposta ad una domanda
- *qualcosa che ho*, ovvero qualcosa di cui l'utente è materialmente in possesso, come bancomat, scheda SIM, badge, ecc...
- *qualcosa che sono* ,ovvero include l'ambito dei metodi di autenticazione biometrica, come scansione della retina, impronta digitale, riconoscimento vocale o facciale

Come detto prima tutte queste informazioni vengono memorizzate alla creazione del profilo

Single Sign On

Il **Single Sign On** è la caratteristica di effettuare una sola autenticazione per l'utilizzo di più software e/o sistemi, con l'obbiettivo di semplificare la gestione delle password da parte degli utenti e la gestione della sicurezza da parte degli amministratori/sistemisti.

Password Management

Il **Password Management** sono un insieme di sistemi per la gestione delle password: di questi sistemi fanno parte regole e software, che variano a seconda che si tratti di un singolo utente(es.uso domestico/personale) o gruppi di utenti(es. Aziende). Per quanto riguarda l'utilizzo di singoli utenti, si tratta generalmente di programmi che consentono di memorizzare e criptare le proprie password: si parla anche di password wallet. Mentre per l'utilizzo multi-utente si utilizzano software di[1],[2],[3], Single Sign On(di cui parlato in precedenza)

User Activity Monitoring

Con *User Activity Monitoring* si intende l'insieme delle operazioni volte al controllo del comportamento dell'utente; ciò comprende: l'utilizzo delle applicazioni, le finestre e/o software aperte/i, siti visitati, comandi eseguiti e tutto ciò che può riguardare l'utilizzo (proprio o improprio) del terminale.
Questa attività avviene ricorrendo all'utilizzo simultaneo di controllo e allerta in tempo reale in caso di comportamenti anomali da parte di un utente, e della registrazione di tutte le operazioni eseguite dallo stesso in appositi file di[4]. Con l'utilizzo di appositi software questi file, che registrano ogni informazione riguardo l'attività dell'utente, possono assumere validità legale nel caso in cui si verifichino casi di perdita di dati, attacchi al sistema o qualunque evento che porti alla compromissione o furto di informazioni sensibili.

Role Management

Il **Role Management** permette di organizzare delle autorizzazioni che gestiscono quali utenti possono utilizzare o meno le risorse delle applicazioni fornite: si possono quindi aggregare gli utenti in gruppi, ognuno con una serie di privilegi. Questo sistema consente di coordinare un insieme di situazioni, come ad esempio mostrare/nascondere delle

informazioni o, in modo similare, permettere l'accesso a certe parti di applicazioni o di siti web solo ad una parte selezionata di utenti. Potremmo assimilare queste regole, ad esempio, a quelle utilizzate nelle , ACL.
Esempio ACL:

```
access-list 100 deny ip host 192.168.0.5 any
access-list 100 permit tcp any gt 500 host 192.168.4.1
```

Questo tipo di regole possono essere stabilite attraverso diversi linguaggi, come ad esempio C#, ASP.NET o VisualBasic.
Esempio role management C#:

```
Roles.AddUserToRole("MarioRossi", "manager");
string[] userGroup = new string[2];
userGroup[0] = "Technician";
userGroup[1] = "Graduated";
Roles.AddUsersToRole(userGroup, "members");
```

Standard

Gli standard che , ISO (https://www.iso.org/home.html) ha elaborato fin'ora in merito alla gestione delle identità sono i seguenti:

- ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts
- ISO/IEC 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements
- ISO/IEC DIS 24760-3 A Framework for Identity Management—Part 3: Practice
- ISO/IEC 29115 Entity Authentication Assurance
- ISO/IEC 29146 A framework for access management
- ISO/IEC CD 29003 Identity Proofing and Verification
- ISO/IEC 29100 Privacy framework
- ISO/IEC 29101 Privacy Architecture
- ISO/IEC 29134 Privacy Impact Assessment Methodology

Voci correlate

- Autenticazione
- Security Assertion Markup Language

Principali link e fonti

, Kent.edu - What is Password Management (https://www.kent.edu/is/secureit/what-password-management)
, AuditShark.com - What is Compliance Management (https://www.auditshark.com/Education/what-is-compliance-management.aspx)
, Microsoft.com - Role Management (https://msdn.microsoft.com/en-us/library/5k850zwb.aspx)
, Hubspot.com - Account Management (https://blog.hubspot.com/sales/account-management-vs-sales)
, Searchsecurity.techtarget.com - Multi-factor authentication (http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA)

1. **^** , Password Synchronization
2. **^** , Self-service Password Reset
3. **^** , Privileged Password Management
4. **^** , LOG
