

I limiti e le difficoltà di una corretta profilazione degli utenti

The limitations and difficulties of proper user profiling

Giancarlo Butti ♦

♦ Isaca Milano

Sommario

Una delle principali misure di sicurezza che tutti noi utilizziamo tutti i giorni, anche se inconsapevolmente, riguarda l'uso di credenziali di autenticazione composte solitamente da una user id e da una password, l'uso di dispositivi fisici di autenticazione (ad esempio un badge), l'uso di caratteristiche biometriche di una persona (impronte digitali...).

Dopo l'autenticazione, al nostro nominativo viene abbinato un profilo autorizzativo che ci consente di accedere ai soli asset ai quali siamo abilitati.

Ma è proprio così?

Abstract

One of the main security measures that we all use every day, even if unknowingly, involves the use of authentication credentials usually composed of a user id and password, the use of physical authentication devices (e.g. a badges), the use of biometric characteristics of a person (fingerprints...).

After authentication, our call sign is matched with an authorization profile that allows us to access only those assets to which they are enabled.

But is this really the case?

Keyword

Need to know, authentication, authorization

1 - Introduzione

Il principio del need to know (secondo il glossario del NIST - CNSSI 4009-2015: *“Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.”*) viene ripreso in numerose normative, negli standard di sicurezza, nelle buone pratiche...

Il GDPR, ad esempio, introducendo il concetto di minimizzazione sul numero di soggetti che possono accedere ai dati (art. 25.2), richiede implicitamente di applicare questo principio.

Si tratta di una delle due misure di sicurezza obbligatorie previste nel GDPR (l'altra è la 32.4, che prevede la formazione dei soggetti autorizzati al trattamento) che per il resto, lascia ai singoli Titolari la responsabilità di individuare delle idonee misure di sicurezza, dopo aver effettuato una valutazione dei rischi di un trattamento sui diritti e le libertà delle persone fisiche (art. 32 del GDPR).

Un principio quindi assolutamente conosciuto e, “teoricamente”, applicato.

Le virgolette sono d'obbligo in quanto, come si evincerà dal resto dell'articolo, riuscire ad implementare correttamente questo principio, salvo il caso di sistemi informativi poco complessi, è estremamente difficoltoso.

Nemmeno l'uso di strumenti, quali sistemi di identity management, possono aiutare in questa difficile impresa e l'articolo spiegherà le motivazioni di questa difficoltà.

La conseguenza di quanto sopra è che, nella realtà, quasi nessuna organizzazione è conforme alle normative che richiedono una corretta applicazione di questo principio (oltre al GDPR basta citare la Circolare 285 di Banca d'Italia per il mondo bancario, o analoghe normative in altri settori).

2 – I requisiti per una corretta implementazione del principio del need to know

La corretta implementazione del principio del need to know, richiede una serie di prerequisiti, che in sintesi devono permettere di abbinare ad un utente (o ad una utenza) uno o più profili abilitativi, che consentano a quell'utente di accedere alle sole risorse (asset, dati, applicazioni, documenti...) che sono strettamente necessarie per svolgere le attività legate al suo specifico ruolo.

Sono stati introdotti alcuni concetti, quali quello di ruolo, utente, asset, profilo... che si ritiene essere di uso comune e che quindi non richiedono una ulteriore spiegazione.

Quello che si può dedurre dalla frase più sopra è che, per poter procedere a questo abbinamento fra ruolo e risorse, e quindi per poter definire il contenuto di un profilo abilitativo, sia necessaria la conoscenza di una serie di elementi di base fondamentali.

Ad esempio, è necessario avere una mappatura di quelle che sono le risorse alle quali gli utenti devono poter accedere e una mappatura di quelli che sono i ruoli all'interno dell'organizzazione.

In altre parole, il prerequisito per la corretta definizione di un profilo abilitativo, è la disponibilità di una serie di informazioni di base che documentino la realtà della organizzazione e delle sue risorse informatiche (e anche non informatiche, quali i comuni documenti su carta).

3 – I passi per una corretta implementazione del principio del need to know

Come si deve procedere quindi per poter effettuare una corretta implementazione del principio del need to know?

Il processo si può sintetizzare nelle seguenti fasi:

- mappature delle risorse informatiche alle quali è necessario accedere
- mappatura dei soggetti che devono accedere alle risorse e dei loro ruoli
- incrocio fra l'elenco delle risorse disponibili e le risorse alle quali è necessario accedere per svolgere le varie attività da parte dei vari ruoli, creando i relativi profili abilitativi
- gestione della evoluzione degli elementi di cui sopra.

3.1 – La mappatura delle risorse informatiche

3.1.1 – La mappatura dei componenti

La mappatura delle risorse informatiche comprende server (fisici o virtuali) nei più diversi ambienti, applicativi, database, apparati di rete, apparati per la sicurezza sia fisica, sia logica, apparati per la fonia, dispositivi mobili, stampanti, multifunzione, NAS, SAN, apparati di digitalizzazione, documenti in formato digitale...

Tali apparati possono operare in ambienti diversificati (produzione, sviluppo, test, formazione, sito di recovery...), on premise o presso qualche fornitore (in cloud o meno).

Quindi è necessario disporre di strumenti che consentano di effettuare e gestire nel tempo una adeguata mappatura che deve essere molto puntuale, analitica e che deve anche mappare le correlazioni esistenti fra i vari elementi.

Ad esempio quali dati siano accessibili dai vari applicativi.

Se infatti i dati presenti in un database sono accessibili, ad esempio, da applicativi diversi, è evidente che è necessario che vi sia una coerenza nei profili abilitativi di tutti questi applicativi.

Analogo è il caso in cui una determinata informazione sia presente in più database o sotto forma di dati e di documenti digitali.

È quindi necessaria una mappatura che documenti la relazione esistente fra database e applicativi.

3.1.2 – La mappatura degli applicativi e delle loro funzioni

Un altro aspetto più articolato e complesso da gestire, ma assolutamente fondamentale, è il disporre non solo di un elenco di tutte applicazioni disponibili, ma anche di tutte le funzioni disponibili per ogni applicazione, di quali siano i dati accessibili da ogni singola funzione, nonché del tipo di operazioni che tale funzione consente di svolgere sui dati.

La complessità appare più chiara se si pensa che applicazioni di uso comune in ambito bancario possono avere centinaia di funzioni e che una banca può utilizzare anche un migliaio di applicazioni.

In una situazione di questo tipo o di analoga complessità, come quelle presenti in molte organizzazioni medio grandi, una mappatura con questo livello di analiticità è difficilmente riscontrabile e richiede la presenza di strumenti di mappatura adeguati che consentano la condivisione di queste informazioni.

Non è infatti sufficiente che tali informazioni siano in possesso del singolo ufficio IT che si occupa della manutenzione di una specifica applicazione ma, ad esempio, devono essere definiti degli standard di nomenclatura e descrizione delle caratteristiche delle singole funzioni.

Se le informazioni contenute in questo repository non sono realmente fruibili da soggetti diversi da chi le ha create, non sarà possibile centralizzare la loro gestione.

Per contro, solo chi ha una visione di insieme può, ad esempio, creare profili coerenti fra più applicazioni, o evitare che lo stesso soggetto possa, inferendo informazioni presenti su più applicativi, ottenere informazioni alle quali non dovrebbe accedere.

Inoltre, in assenza di un repository con tale livello di dettaglio, è impossibile ipotizzare di poter creare dei profili realmente coerenti con un determinato ruolo in quanto, al più, si potrà presupporre che uno specifico ruolo debba accedere ad una determinata applicazione, ma non il dettaglio di cosa potrà fare su quella applicazione.

Altra informazione che sarebbe necessario avere per una corretta profilazione, riguarda la modalità con cui sono costruite sia le alberature relative alle funzioni disponibili su un applicativo, sia la creazione dei profili utente.

In particolare, se tali costrutti sono scritti nel codice dell'applicazione ovvero se sono parametrici.

Nel primo caso, qualunque esigenza implementativa richiederà l'intervento di chi ha scritto l'applicazione (sempre che sia ancora disponibile e che siano disponibili i sorgenti dell'applicazione), mentre nel secondo caso sarà più semplice adattare l'applicazione alle proprie esigenze.

Ne consegue che, in alcuni casi, quello che un profilo autorizzativo teorico richiederebbe, nella pratica potrebbe non essere fattibile, in modo assoluto o in quanto economicamente insostenibile.

Un esempio facile da comprendere riguarda il profilo dedicato alle attività di verifica da parte di un auditor; tale profilo deve permettere di accedere a qualunque informazione, ma solo in consultazione, senza la possibilità di svolgere alcuna azione operativa.

Tale profilo raramente è presente sulle applicazioni e quindi, viene solitamente assegnato all'auditor un profilo il meno invasivo possibile, ma in ogni caso non coerente con il ruolo di auditor e quindi, in ultima analisi, non conforme e non allineato al principio del need to know. Quindi, paradossalmente, per consentire ad un auditor di svolgere il suo lavoro, viene eseguita un'azione che l'auditor dovrebbe segnalare come non conforme.

Allora perché in tali occasioni non viene creato uno specifico profilo per gli auditor?

Le motivazioni sono già state evidenziate in precedenza; potrebbe essere troppo oneroso in termini di tempo o dal punto di vista economico, in particolare se, per poterlo creare, è necessario intervenire sul codice sorgente dell'applicazione, o addirittura impossibile se non si ha a disposizione quest'ultimo o le competenze per poter intervenire.

Va anche considerato il fatto che esistono applicazioni che non dispongono di un processo di autenticazione e autorizzazione, come ad esempio, quelle di produttività individuale, largamente utilizzate in tutte le organizzazioni.

Spesso tali applicazioni sono utilizzate dagli utenti per effettuare particolari elaborazioni, per le quali non sono disponibili applicazioni "ufficiali", e questo introduce un ulteriore elemento di complessità.

In questi casi l'organizzazione deve prevedere presidi di altra natura per mantenere il controllo sull'accesso alle informazioni, sulle possibili elaborazioni delle stesse ed in particolare sulla possibilità, da parte degli utenti, di combinare informazioni provenienti da diverse fonti, anche esterne all'organizzazione.

Il tema è molto complesso ed esula dagli obiettivi di questo articolo, ma evidenzia che il perimetro del sistema informativo da presidiare va oltre la tradizionale sala server (reale o virtuale).

Ulteriore elemento da considerare è il così detto shadow IT, e cioè quelle componenti del sistema informativo che vengono utilizzate dagli utenti e che sono fuori del controllo

dell'organizzazione, o quantomeno dell'IT. Si pensi ad esempio ai servizi di archiviazione e condivisione delle informazioni disponibili on line.

3.1.3 – L'accesso diretto ai dati

Oltre a quanto fino ad ora esposto, è necessario verificare ulteriori aspetti del sistema informativo.

Ad esempio, i dati presenti in un database possono essere acceduti, come in precedenza evidenziato, da più di un'applicazione.

Ma la loro lettura o più in generale il loro trattamento, comprese quindi anche le operazioni di modifica e di cancellazione, potrebbero avvenire anche senza che sia necessario l'uso di un applicativo.

Un semplice foglio Excel consente di creare delle query che interagiscono con una fonte esterna di informazioni, come un database, permettendo a chiunque conosca la struttura del database, la sua collocazione nella rete aziendale e le eventuali credenziali di accesso, di effettuare interrogazioni o manipolazioni dei dati.

Per evitare una simile eventualità è possibile intervenire su più fronti, ma è evidente che chi si occupa di garantire la sicurezza delle risorse informatiche deve avere coscienza di tutte le possibili eventualità.

È inoltre evidente che chi accede direttamente al database con profili amministrativi può similmente procedere ad analoghe attività sui dati.

Anche in questo caso le misure di tutela possono essere numerose, quali la registrazione delle operazioni svolte in log non alterabili da parte di chi ha compiuto le operazioni.

3.1.4 – L'esportazione di dati

Anche il legittimo accesso ai dati può portare ad operazioni non conformi a quanto prevede un determinato ruolo. Ad esempio, una esportazione massiva di dati dai database aziendali e la loro successiva conservazione sul pc dell'utente, potrebbe consentire a quest'ultimo di effettuare successive operazioni di trattamento altrimenti non consentite.

Ad esempio, se i dati sono relativi a dei clienti, è possibile che l'utente che ha proceduto alla loro estrazione, proceda ad una loro profilazione o che inferisca informazioni che non sono nativamente nel database.

Combinando informazioni provenienti da diversi database aziendali, potrebbe creare correlazioni non precedentemente evidenti.

Questo tipo di operazioni potrebbero comportare diverse violazioni, in particolare alla normativa privacy.

Queste tipologie di trattamenti infatti, non vengono rappresentate nelle informative rilasciate agli interessati, o potrebbero essere comunque vietate dalla normativa in assenza di una adeguata base giuridica, come nel caso della profilazione.

3.2 – Mappatura dei soggetti che devono accedere alle risorse e dei loro ruoli

3.2.1 – La mappatura di utenze e di utenti

Il secondo elemento da mappare sono i soggetti che possono accedere alle informazioni.

Al riguardo vanno differenziate le utenze dagli utenti.

Con il termine utenze si intendono le macrocategorie di utenti che si desiderano prendere in considerazione.

Una possibile classificazione è la seguente:

- utenze applicative
 - normali
 - amministratori delle applicazioni
- utenze particolari
 - amministratori di sistema (multiambiente)
 - amministratori di data base
 - amministratori di apparati di rete
 - amministratori di apparati di telefonia
 - amministratori degli apparati relativi alla sicurezza fisica
 - ...
- utenze tecniche.

Nell'esempio riportato vi sono tre macrocategorie di utenze ben distinte. Le prime due riguardano tipologie di utenze riferite a persone fisiche, mentre con utenze tecniche si intendono quelle con le quali, ad esempio, un'applicazione si presenta ad un database per eseguire delle query.

Quest'ultima categoria di utenze ha delle caratteristiche e delle problematiche particolari, che non sono oggetto di trattazione in questo articolo; in particolare molto spesso dispongono di credenziali di accesso scritte nel codice dell'applicazione e quindi non modificabili.

Le utenze di tipo amministrativo dispongono di privilegi di accesso molto ampio, che consentono di svolgere un insieme molto vasto di operazioni direttamente sui sistemi e sui database, in particolare per la loro gestione.

Nell'ambito delle utenze applicative, spesso esistono utenze con privilegi particolari di tipo amministrativo, intendendo con tale termine utenze dedicate, ad esempio, alla creazione di utenti sull'applicazione stessa, ovvero alla configurazione di altri parametri nell'applicazione.

Le utenze di tipo amministrativo, siano esse legate al singolo applicativo o ad altri asset informatici, seguono un percorso diverso per la loro corretta profilazione, in quanto il loro uso è molto più standardizzato.

Un secondo tipo di raggruppamento degli utenti, li identifica per categoria di appartenenza:

- interni
 - dipendenti
 - lavoro temporaneo
 - stagisti
 - ...
- esterni
 - consulenti
 - ispettori
 - partner
 - outsourcer
 - utenti finali
 - ...

Questo tipo di raggruppamento macro ha la sola finalità di definire politiche di gestione ed accesso comuni ai membri dei vari gruppi.

Ad esempio, si può stabilire che gli utenti esterni non possano accedere direttamente alle risorse informatiche dell'organizzazione, ma possono accedere ai servizi offerti solo tramite un portale web.

3.2.2 – La mappatura dei ruoli aziendali

Le attività all'interno di un'organizzazione sono svolte dal personale che è inquadrato in diverse unità organizzative (uffici). L'ufficio acquisti svolge attività completamente diverse da quelle che sono svolte dall'ufficio risorse umane.

È quindi necessario elencare in modo analitico quali siano le attività svolte dai singoli uffici, differenziando eventualmente ulteriormente queste ultime nel caso in cui i membri di uno stesso ufficio svolgano attività fra loro diverse.

Ad ogni ufficio possono corrispondere quindi uno o più ruoli.

Ad esempio potrebbe essere necessaria una differenziazione fra l'addetto agli acquisti UE e l'addetto agli acquisti extra UE, in quanto svolgono attività diverse e utilizzano dati ed applicazioni diverse, ovvero funzioni diverse sullo stesso applicativo.

Considerando che i profili abilitativi sono solitamente abbinati ai ruoli, la granularità nella definizione dei ruoli è importante, altrimenti si rischia che, ritornando al nostro esempio, se gli addetti all'ufficio acquisti hanno un unico ruolo, possano accedere anche a funzionalità e dati/documenti che non sono strettamente necessari per lo svolgimento della loro attività.

Questo può essere più o meno critico in funzione del ruolo svolto, ma in ogni caso viene violato il principio del need to know.

Sta poi all'organizzazione valutare se gestire questo aspetto aumentando il numero dei ruoli o se procedere a livello informatico con delle abilitazioni specifiche ad personam.

Ad esempio, un unico ruolo per l'ufficio acquisti potrebbe permettere di accedere a dati ed applicazioni di uso comune a tutto l'ufficio, ed abilitazioni ad personam permettere ai singoli operatori di accedere alle specifiche applicazioni legate alla loro attività.

Se si percorre questa seconda ipotesi, va ricordato che le abilitazioni ad personam sono poi difficili da gestire nel tempo.

Solitamente le organizzazioni hanno degli organigrammi o dei funzionigrammi che descrivono sommariamente quali siano i compiti dei vari uffici, ma non arrivano a descrivere con sufficiente dettaglio le singole attività.

Se dal punto della gestione organizzativa questo può essere sufficiente ed evita di aggiornare continuamente la normativa aziendale nel caso di variazioni delle singole attività, per contro non si hanno a disposizione le informazioni necessarie per una corretta definizione dei profili abilitativi.

Per questo motivo si deve procedere ad una più dettagliata mappatura delle singole attività.

3.2.3 – La mappatura delle attività

Per poter definire correttamente un profilo abilitativo è necessario avere da un lato un analitico dettaglio delle risorse informatiche e dall'altro un elenco di quali di queste risorse siano necessarie per svolgere una determinata attività:

- applicazioni
- periferiche o dispositivi particolari (ad esempio scanner)
- informazioni
 - dati
 - documenti informatici
 - documenti analogici (fuori perimetro rispetto questo articolo)
- azioni da compiere sui dati e sui documenti.

Inoltre è necessario censire le singole attività che vengono eseguite da un determinato ruolo.

Il reale problema di quanto appena esposto è che difficilmente un'organizzazione ha una documentazione sufficientemente dettagliata per una tale rappresentazione.

Solitamente un livello di dettaglio abbastanza vicino a quanto richiesto si ha solo nelle organizzazioni che dispongono di un piano di continuità operativa.

Per realizzarlo infatti è necessario mappare tutte le risorse indispensabili a erogare un processo critico al fine di poterlo replicare presso un'altra sede o da parte di soggetti che normalmente non svolgono quella attività.

In particolare per questa seconda eventualità è necessario disporre di documentazione molto analitica che descriva l'attività passo passo, fino al dettaglio di quali funzioni selezionare dai menu.

3.3 La creazione dei profili abilitativi

Solo disponendo da un lato della mappatura di tutte le risorse informatiche alle quali è necessario accedere (in particolare per quanto riguarda le utenze non amministrative applicazioni, dati e documenti) e dall'altra della mappatura dei ruoli aziendali, è possibile creare dei corretti profili abilitativi, cioè di quell'insieme di regole che consentano ad un determinato ruolo di accedere alle sole applicazioni/funzione, dati, documenti strettamente necessari allo svolgimento di una specifica attività.

Va precisato che possono esserci altri parametri che rendono ancor più granulare la profilazione.

Ad esempio, in ambito bancario, gli addetti delle filiali con lo stesso ruolo svolgono tutti gli stessi compiti e sono quindi abilitati alle stesse applicazioni, tuttavia possono solitamente operare solo sui clienti della filiale di appartenenza.

Sempre in ambito bancario, l'iter deliberativo di un credito viene gestito da soggetti diversi in funzione dell'importo dello stesso.

Abbiamo già accennato nei paragrafi precedenti alle abilitazioni ad personam.

Queste consentono di aggiungere, ad uno specifico utente, abilitazioni che non sono comprese in quelle legate al suo ruolo.

Una esigenza di questo tipo può nascere per diversi motivi, come quella citata nei paragrafi precedenti.

Altro aspetto da considerare è che l'esecuzione delle attività legate ad un determinato ruolo potrebbero determinare l'esigenza di un profilo abilitativo che tecnicamente o economicamente non è possibile implementare, come già evidenziato nei paragrafi precedenti.

Ulteriore elemento da prendere in considerazione, anche questo già ricordato in precedenza, è il garantire la coerenza nell'accesso alle informazioni. Per tale motivo è necessario nella fase di mappatura delle risorse informatiche, avere una chiara rappresentazione della relazione applicazioni, dati, documenti.

Se la stessa informazione è accessibile da applicazioni diverse deve essere mantenuta una coerenza nell'accesso alle stesse.

In altri termini se non ho accesso ad una particolare informazione dall'applicazione A non devo, per coerenza, potervi accedere nemmeno dall'applicazione B.

Evidenzio che si sta parlando di informazioni e non di dati.

La medesima informazione può essere infatti presente in database o documenti diversi.

Sempre per restare in tema bancario, se non è possibile accedere ai dati contenuti nel conto corrente di un collega dall'applicazione conti correnti, non deve essere nemmeno possibile accedere alle stesse informazioni dall'applicazione che gestisce i documenti relativi agli estratti conto.

4 – La realtà aziendale

Il complesso e articolato processo descritto nei paragrafi precedenti, confrontato con la documentazione normalmente riscontrabile presso le organizzazioni, evidenzia quanto la realtà dei fatti sia lontana dalla teoria.

Le organizzazioni non dispongono di tutte le informazioni rappresentate in precedenza.

Molto spesso i profili abilitativi vengono creati per assonanza fra le attività di due diversi uffici. Quando un nuovo ufficio viene creato gli vengono assegnati i profili abilitativi dell'ufficio che svolge le attività più simili, aggiungendo eventuali ulteriori abilitazioni nel caso in cui servano, ma difficilmente preoccupandosi di eliminare quello che non serve.

La difficoltà nel mappare e mantenere aggiornati in tempo reale le informazioni necessarie ad una corretta profilazione, rende di fatto impossibile, salvo che nelle realtà meno complesse, un reale rispetto del principio del need to know.

I limiti e le difficoltà di una corretta profilazione degli utenti

The limitations and difficulties of proper user profiling

G. Butti

Nelle pagine seguenti, si riporta la scheda di sintesi del rapporto di audit ed un esempio delle schede dei processi analizzati (tratte da [1]).

L'esempio riportato descrive un caso teorico di audit effettuato su una organizzazione di medie dimensioni, con un sistema informativo dotato di una ventina di applicazioni, 1000 utenti e 40 profili abilitativi.

Una realtà quindi ne particolarmente semplice, ne particolarmente complessa, che può trovare riscontro, quantomeno per quanto riguarda il numero di applicazioni utilizzate, in molte realtà italiane che abbiano anche un numero di dipendenti molto più limitato.

Si evidenzia che l'organizzazione rappresentata nell'esempio, costituisce di per sé stessa una eccellenza, in quanto è dotata di una serie di documenti e procedure che vanno ben oltre rispetto a quanto disponibile nella media delle organizzazioni (si veda al riguardo la Scheda processo).

I rilievi riportati, sebbene ipotetici, possono facilmente trovare riscontro in qualunque realtà.

RAPPORTO DI AUDIT	
N° 0004/2019/ACFE	
SOCIETÀ: ACFE SPA	
PERIODO DI EFFETTUAZIONE DELL'AUDIT	dal 10/02/2019 al 30/04/2019
Capo team	Luigi Rossi
Team	Mario Negri
Responsabile dell'ufficio	Bianchi Attilio
Responsabile dell'Audit	Carlo Rossi
VALUTAZIONE COMPLESSIVA	Parzialmente adeguato
PRECEDENTI ATTIVITÀ DI VERIFICA	
Audit sulle misure minime di sicurezza del 2016	<i>Parzialmente adeguato</i>
Follow up sulle mm di sicurezza del 2011	<i>Parzialmente non adeguato</i>
Audit sulle misure minime di sicurezza del 2010	<i>Non adeguato</i>
OBIETTIVI DELL'AUDIT	
<p>La verifica, inclusa nel programma di audit del 2019, è stata effettuata dal Titolare con lo scopo di verificare il rispetto delle prescrizioni normative in ambito privacy, in riferimento agli artt. 25 e 32; in particolare:</p> <ul style="list-style-type: none"> • le procedure poste in essere dall'azienda al fine di garantire il rispetto del principio di minimizzazione, relativamente all'accessibilità ai dati personali • la definizione di uffici, ruoli organizzativi, profili autorizzativi per l'accesso agli asset aziendali, con particolare riferimento ai dati personali • le relative implementazioni sul sistema informativo. <p>In considerazione del fatto che i dati personali sono un sottoinsieme delle informazioni gestite dall'azienda, nella valutazione dei profili e delle misure tecniche ed organizzative in atto sono state prese in considerazione anche le indicazioni fornite dal Modello organizzativo redatto ai sensi del D.lgs. 231/2001 e delle indicazioni fornite dal Codice della proprietà industriale in merito alle informazioni commerciali riservate.</p>	
ESCLUSIONI	
<p>La verifica non comprende:</p> <ul style="list-style-type: none"> • le utenze tecniche • le utenze amministrative • le utenze assegnate ai clienti per l'accesso alla piattaforma on line • gli strumenti per l'accesso da remoto al sistema informativo aziendale 	
SCHEDE PROCESSI E VALUTAZIONI	
Gestione del personale	<i>Parzialmente adeguato</i>
Definizione dei ruoli e dei profili	<i>Parzialmente non adeguato</i>
Implementazione e gestione dei profili	<i>Parzialmente adeguato</i>

SINTESI DEI RISULTATI

L'attività di audit ha riguardato:

- la verifica delle policy e procedure relative alla:
 - gestione delle strutture organizzative (nuovi uffici, accorpamenti, eliminazione...)
 - definizione di mansionari per le strutture con un livello di dettaglio sufficiente a individuare attività, strumenti, documenti, dati, flussi in ingresso e flussi in uscita
 - definizione dei ruoli
 - definizione dei profili autorizzativi
 - abbinamento ruoli/profili
 - gestione degli utenti (censimento iniziale, variazione di ruolo, assenze prolungate, cessazione del rapporto...)
- la gestione degli utenti ed il loro censimento sul sistema informativo
- l'implementazione e gestione dei profili sul sistema informativo.

L'attività di audit ha ricompreso la verifica degli aspetti formali, operativi ed i relativi controlli.

L'audit ha rilevato:

- le procedure in essere non consentono una mappatura sufficientemente dettagliata delle attività svolte dai singoli uffici
- manca una specifica procedura in merito all'attribuzione delle autorizzazioni ad personam
- la definizione dei profili abilitativi viene effettuata senza un reale censimento delle singole funzioni disponibili sulle applicazioni
- il censimento dei profili abilitativi sul catalogo dei profili viene effettuato senza regole condivise
- la descrizione dei profili abilitativi nel catalogo non consente di capire nel dettaglio quali siano le reali autorizzazioni abbinata al singolo profilo
- non risultano censite le abilitazioni ad personam
- non vi è una corrispondenza univoca fra i ruoli definiti nella procedura del personale e quelli nelle procedure che gestiscono la sicurezza.

Sono stati inoltre riscontrati dall'analisi di 100 utenti (10% del totale):

- 3 utenti con l'attribuzione di un ruolo sul sistema informativo del personale non corrispondente all'ufficio di appartenenza
- 1 utente ancora censito come operativo anche se risulta essere dimissionario da 15 giorni precedente l'attività di verifica
- 2 utenti con autorizzazione ad personam non in linea con il loro attuale ruolo, ma compatibili con il precedente ruolo
- 1 utente con attribuzione di un profilo autorizzativo non in linea con il ruolo.

Sono stati riscontrati dall'analisi di 20 profili (50% del totale):

I limiti e le difficoltà di una corretta profilazione degli utenti

The limitations and difficulties of proper user profiling

G. Butti

- 2 profili con autorizzazioni eccessive rispetto alle esigenze del ruolo al quale sono abbinati
- 3 profili con autorizzazione relative ad applicazioni non più in uso presso l'azienda
- 2 profili che presentano incoerenze rispetto all'accesso ai medesimi dati da parte di applicazioni diverse.

Sono stati riscontrati dall'analisi di 10 applicativi (50% del totale):

- 3 applicativi non consentono la puntuale implementazione dei profili applicativi così come definito nel catalogo dei profili
- 2 applicativi presentano degli scostamenti fra i profili implementati e quanto presente nel catalogo dei profili.

Le criticità sopra esposte espongono l'azienda a:

- rischi legali, legati al mancato rispetto delle prescrizioni della normativa privacy, con particolare riferimento agli art. 25 e 32 del GDPR
- rischi operativi, legati alla richiesta di risarcimenti danni in virtù dell'art. 82 del GDPR
- mancata applicabilità delle tutele previste dal Codice della proprietà industriale

NORMATIVA ESTERNA DI RIFERIMENTO

D.lgs. 196/03

D.lgs. 231/2001

Codice penale – reati informatici

Codice della proprietà industriale

GDPR

NORMATIVA INTERNA DI RIFERIMENTO

Declinata nelle singole schede processi

SCHEDA PROCESSO	
PROCESSO ANALIZZATO	Definizione dei ruoli e dei profili
VALUTAZIONE	Parzialmente non adeguato
PERIODO DI VERIFICA	Dal 01/03/2019 al 20/03/2019
DESCRIZIONE DEL PROCESSO	
<p>L'ufficio Organizzazione, in base alle informazioni in suo possesso sulle attività svolte dai vari uffici, il catalogo degli applicativi ed il catalogo dei dati, definisce:</p> <ul style="list-style-type: none"> • i ruoli aziendali • i profili applicativi • l'abbinamento fra ruoli e profili applicativi. 	
MODALITA' DI SVOLGIMENTO DELL'AUDIT	
<p>La verifica è stata effettuata attraverso l'analisi della documentazione recuperata nel corso dell'attività di audit.</p> <p>Tale documentazione ha ricompreso:</p> <ul style="list-style-type: none"> • policy sul trattamento dei dati personali • procedura per la classificazione delle informazioni • manuale della sicurezza aziendale • procedure per la definizione dei ruoli • procedura per la definizione dei profili • modulistica relativa alla richiesta/modifica/cancellazione dei profili • catalogo dei profili • catalogo delle applicazioni • mansionario • organigramma aziendale • registri delle attività di trattamento • informative rilasciate agli interessati • modello organizzativo 231/2001 • codice etico • disciplinare sull'uso degli strumenti aziendali. <p>L'intervista dei responsabili degli uffici:</p> <ul style="list-style-type: none"> • organizzazione • acquisti • marketing • assistenza alla clientela. <p>La selezione degli uffici da intervistare è stata effettuata considerando quelli con il maggior numero di soggetti interessati.</p>	
CONTROLLI EFFETTUATI E RILIEVI	

I limiti e le difficoltà di una corretta profilazione degli utenti

The limitations and difficulties of proper user profiling

G. Butti

Mansionario	
Rilievo	Le procedure in essere non consentono una mappatura sufficientemente dettagliata delle attività svolte dai singoli uffici. Il livello di dettaglio non consente di definire in particolare quali siano gli strumenti, le informazioni ed i dati necessari per lo svolgimento delle singole attività. Questo non consente una corretta attribuzione definizione dei profili autorizzativi.
Suggerimenti	È necessario aumentare il livello di dettaglio della mappatura.
Valutazione	Medio
Catalogo profili	
Rilievo	Il censimento dei profili abilitativi sul catalogo dei profili viene effettuato senza regole condivise. La descrizione dei profili abilitativi nel catalogo non consente di capire nel dettaglio quali siano le reali autorizzazioni abbinata al singolo profilo. Non risultano censite le abilitazioni ad personam.
Suggerimenti	È necessario censire le abilitazioni ad personam, aumentare il livello di dettaglio nella descrizione dei profili anche attraverso l'uso di una naming convention e definire una procedura per la gestione del catalogo.
Valutazione	Medio
Catalogo applicazioni	
Rilievo	La definizione dei profili abilitativi viene effettuata senza un reale censimento delle singole funzioni disponibili sulle applicazioni
Suggerimenti	È necessario procedere ad una mappatura di dettaglio delle funzioni disponibili sui vari applicativi.
Valutazione	Alto
Procedure	
Rilievo	Manca una specifica procedura in merito all'attribuzione delle autorizzazioni ad personam.
Suggerimenti	Va definita una specifica procedura per l'attribuzione delle autorizzazioni ad personam, per il loro censimento e per la loro gestione nel tempo.
Valutazione	Medio

5 – Garantire l’aggiornamento delle informazioni

La difficoltà nell’effettuare le mappature presentate nei paragrafi precedenti è accompagnata da una ancor più difficile attività di manutenzione delle stesse.

Possono infatti essere acquisite nuove applicazioni, dismesse altre, modificate con nuove funzionalità quelle esistenti...

Lo stesso dicasi di ogni altro asset.

Può cambiare la struttura organizzativa dell’azienda, con nuovi uffici e accorpamenti, che modificano i compiti assegnati...

Analogamente va gestito il personale, con nuovi ingressi, uscite, assenze di lungo periodo, cambio di ufficio o di ruolo.

Un insieme molto corposo di eventi che vanno censiti e gestiti centralmente, in quanto senza una regia centralizzata, il rischio di perdere quella coerenza che si è faticosamente creata è molto alto.

6 – Non solo profili

Anche ipotizzando di avere creato dei corretti profili abilitativi, ci si scontra con un altro aspetto quasi sempre trascurato: la distinzione fra accesso lecito ed accesso legittimo ad una informazione.

Qual è il significato di tali termini ed in cosa differiscono?

Un utente accede lecitamente ai dati (termine mutuato dalla normativa privacy), non solo se è autorizzato a farlo in base al suo profilo abilitativo, ma anche se tale accesso è giustificato da esigenza lavorative.

Ad esempio, un auditor che possa accedere ai dati degli stipendi dei dipendenti per esigenze di servizio, non può accedere agli stessi dati per pura curiosità.

Quindi l’accesso ad una specifica informazione è legittimo se previsto dal proprio profilo abilitativo, ma è lecito solo se avviene per svolgere l’attività per la quale quella autorizzazione è stata concessa.

Negli altri casi l'accesso è illecito e come tale, costituisce una violazione di dati personali (artt. 33, 34 e 83 del GDPR), sanzionato dalla normativa privacy dal punto di vista amministrativo.

Fra gli altri, se i soggetti i cui dati sono stati illecitamente consultati subiscono un danno, ad esempio perché un capo ufficio accede illecitamente ai dati relativi agli stipendi dei colleghi al fine di decidere chi premiare, può chiedere un risarcimento danni ai sensi dell'art. 82 del GDPR.

Come evitare tutto questo?

Il problema è stato affrontato diversi anni fa dall'Autorità Garante per la protezione dei dati personali, che ha proposto una possibile soluzione nel provvedimento *Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011*.

Tale provvedimento ha introdotto l'obbligo di registrare tutte le operazioni di accesso e trattamento dei dati bancari da parte dei collaboratori di una banca, attraverso la registrazione in appositi log delle azioni effettuate dagli stessi.

Infatti, essendo impossibile o molto oneroso in termini organizzativi e tecnici, distinguere in via preventiva un accesso lecito da un accesso solo legittimo, la soluzione proposta prevede la possibilità di verificare a posteriore, mediante appunto l'analisi "intelligente" dei log, la liceità delle azioni effettuate.

È evidente che la registrazione dei log, per essere in linea con le prescrizioni del GDPR (art. 25.2), dovrebbe essere effettuata da qualunque titolare, previo accordo sindacale o autorizzazione dell'ispettorato del lavoro (art. 4 della legge 300/70).

7 – Conclusioni

La quantità di informazioni necessarie per effettuare una corretta profilazione degli utenti rende di fatto possibile tale pratica solo in realtà particolarmente poco complesse.

L'utilizzo di strumenti di identity management nelle realtà più complesse, e la relativa automazione di parte del processo di gestione, può portare ad un falso senso di corretto presidio della tematica, ma in realtà, in assenza delle informazioni descritte in particolare nel paragrafo 3, la configurazione di tali sistemi si rileva imprecisa.

Le organizzazioni devono quindi necessariamente dotarsi di strumenti che consentano di mappare e gestire nel tempo, possibilmente in modalità il più possibile automatizzata, le informazioni propedeutiche ad una corretta gestione dei profili aziendali e degli altri elementi indispensabili per gestire correttamente il principio del need to know.

8 - Bibliografia

[1] Butti G., Perugini M.R. , “Audit e GDPR”, Franco Angeli, 2017

[2] Autorità Garante per la protezione dei dati personali, “Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie”, 2011