UniCredit Business Integrated Solutions

official sponsor

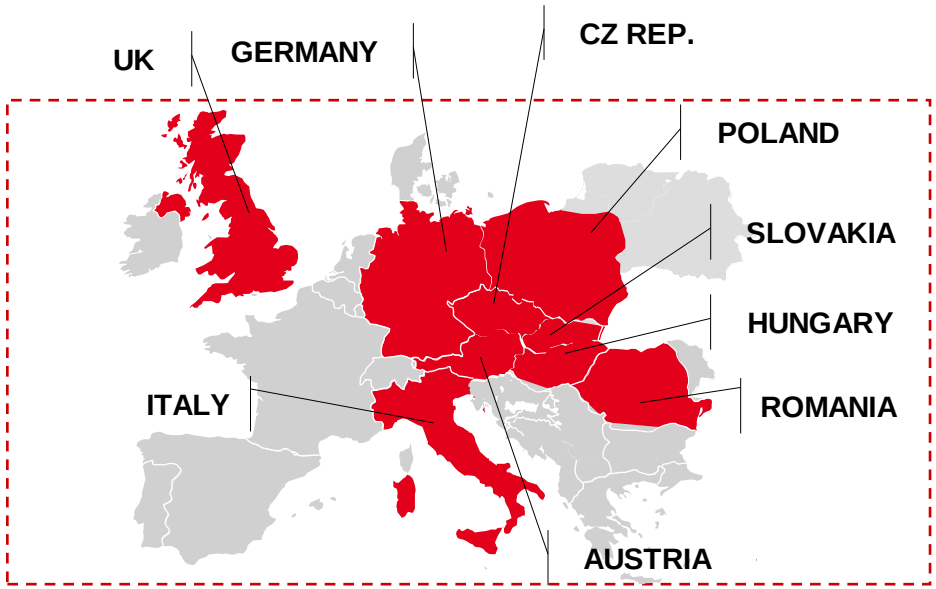
ICT SECURITY SERVICE LINE

La gestione delle utenze amministrative e tecniche: il caso Unicredit Group

Marco Deidda, Head of Data Access Management
UniCredit Business Integrated Solutions – UniCredit Group

Milano, 27 Maggio 2014

UNICREDIT BUSINESS INTEGRATED SOLUTIONS: IDENTITY CARD



- Oltre 10.000 Persone
- 11 paesi*

UniCredit Business Integrated Solutions, la società globale di servizi di Gruppo Unicredit si è sviluppata dal consolidamento di 16 strutture e società di UniCredit dedicate, in particolare, all'erogazione dei servizi di Information e Communication Tecnology (ICT), Back Office e Middle Office, Real Estate, Security e Procurement.

UniCredit Business Integrated Solutions conta oltre 10.000 persone* e coordina le attività in 11 paesi: Austria, Germania, Italia, Polonia, Regno Unito, Repubblica Ceca, Romania, Slovacchia, Ungheria. A New York e Singapore sono presenti 2 branch di UGBS, una Società collegata.

* Perimetro UniCredit Business Integrated Solutions S.C.p.A. e UniCredit Business Integrated Solutions Austria GmbH

Contesto di riferimento: l'evoluzione delle minacce di sicurezza

Le **minacce** di sicurezza hanno subito importanti evoluzioni negli ultimi anni, in linea con l'evoluzione tecnologica (crescente disponibilità di banda e di risorse elaborative, introduzione di dispositivi mobili, …), e sono **sempre più rivolte ad ottenere l'acceso ai dati e ai sistemi aziendali**.

FINANCIAL TIMES

May 5, 2014 7:12 pm

Foreign spy agencies recruit corporate IT staff, warns MI5

By Sam Jones, Defence and Security Editor

Foreign intelligence agencies are targeting IT workers at big businesses, hoping to recruit them and gain privileged access to sensitive computer systems, MI5 has warned British corporate chiefs.

The growing threat is one of the main cyber concerns th
in high-level conversations with executives in recen
make companies boost their digital defences, accor

The government has s
efforts to improve cyb
important organisatic
companies or energy
particularly vulnerabl

More

ON THIS TOPIC

Look out, sysadmins - HOT FOREIGN SPIES are targeting you

Agents are greasing up IT bods to access all areas, warns MI5

By John Leyden, 7 May 2014 Follow 2,607 followers

34

Linux and AIX Bare-Metal Recovery Webinar

MI5 has warned that foreign spy agencies are targeting IT workers within big organisations as a means of gaining privileged access to sensitive data.

The security service's warning about spy-infiltration tactics is a bid to encourage corporations to bolster their defences against such attacks, the *FT* (via the *Daily Mail*) reports.

RELATED STORIES

Samsung's NX300 cam is

Data Access Management e Segregation Of Duties: il contesto normativo di riferimento

Normativa in materia di Protezione dei dati personali

- *Autorizzazione al trattamento dei dati personali*
- *Limitazione al trattamento dei dati personali (liceità, correttezza, pertinenza, …)*
- *Controllo accessi secondo l'approccio del minimo privilegio*

Privacy e Amministratori di sistema

- *Selezione dei soggetti in grado di svolgere compiti amministrativi (esperienza, capacità e affidabilità)*
- *Lettere di designazione degli amministratori di sistema*
- *Lista aggiornata degli amministratori di sistema*
- *Revisione periodica degli amministratori di sistema*
- *Raccolta e conservazione dei log relativi agli accessi amministrativi (log-in/out)*

Provvedimento del Garante Privacy in materia di circolazione delle informazioni e di tracciamento delle operazioni bancarie

- *Tracciamento delle operazioni bancarie dispositive e di consultazione*
- *Conservazione dei log di tracciamento delle operazioni bancarie*
- *Implementazione di alert su comportamenti anomali delle operazioni di consultazione*
- *Audit interno di controllo e rapporti periodici sulle misure implementate*

Normative in materia di segreto bancario

- *Limitazione all'accesso ai dati bancari da parte di soggetti non sottoposti alla tutela della normativa per il segreto bancario*
- *Autorizzazione preventiva all'accesso ai dati bancari da parte della Banca*
- *Controllo delle utenze privilegiate e di emergenza*

Normativa 263 Banca d'Italia

- *Autenticazione: univoca associazione a ciascun utente delle proprie credenziali di accesso*
- *Minimo privilegio e segregazione dei compiti: specifiche procedure di abilitazione e di autenticazione, controlli di tipo four eyes, o di verifica giornaliera ex post)*
- *Monitoraggio: analisi di log e tracce di audit, di accessi, operazioni e altri eventi*

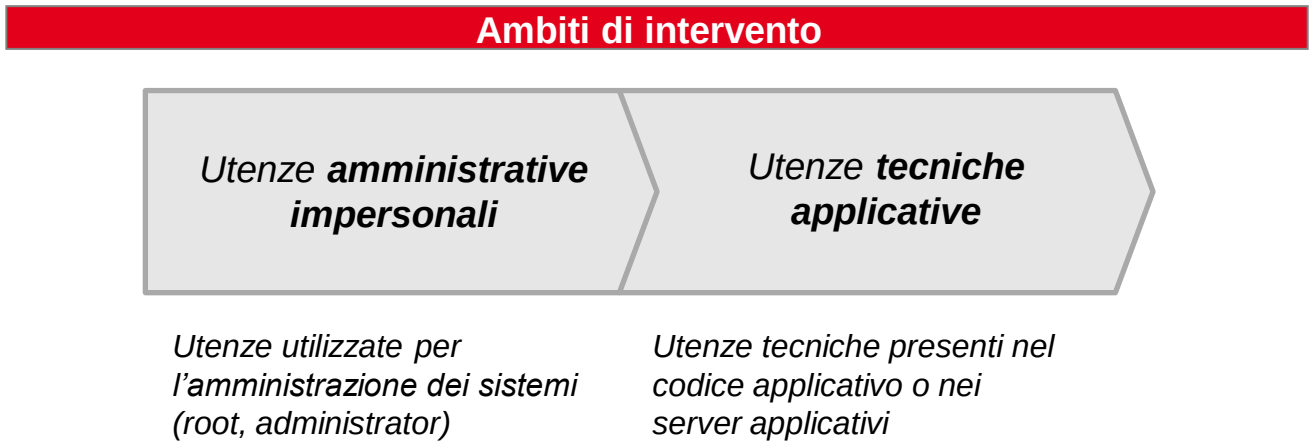
Il controllo dell'accesso finalizzato a limitare e controllare l'accesso ai dati è una priorità anche per il legislatore

Requisiti per la gestione delle utenze privilegiate

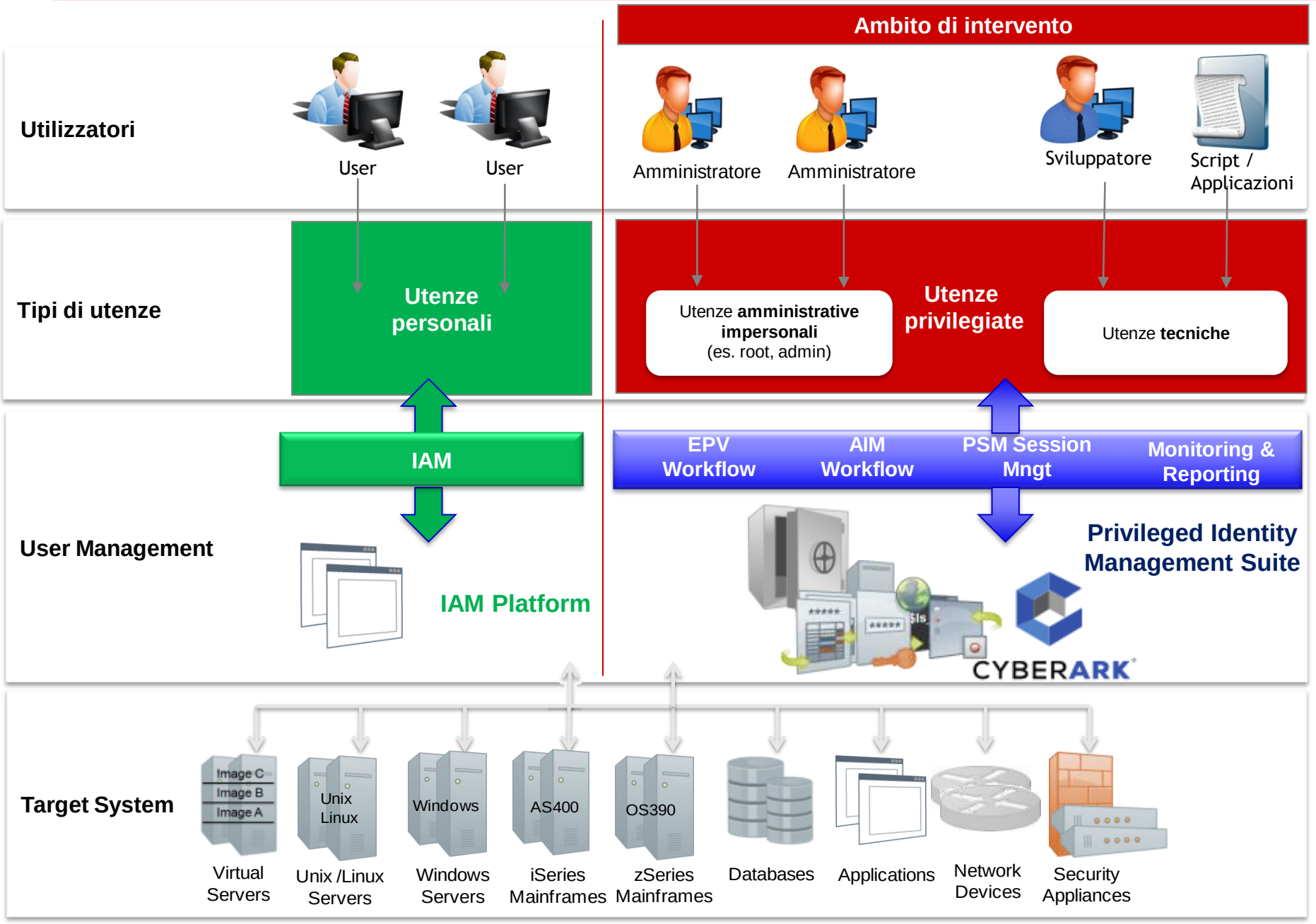
Gestione Utenze Privilegiate	Qualsiasi sistema si avvale di tenze privilegiate predefinite che devono essere gestite in conformità alle normative vigenti. L'elevata numerosità di tali utenze in una organizzazione rende problematica , se non impossibile una gestione manuale delle stesse.
Le Utenze Privilegiate sono presenti in tutte le tipologie di sistema / apparato	Qualsiasi sistema ed apparato si avvale di utenze privilegiate. Una soluzione di gestione deve operare senza interferire con i sistemi su cui opera.
E' necessario poter ricondurre a persone le attività effettuate avvalendosi di Utenze Privilegiate	Le Utenze Privilegiate possono essere un "blind spot" per i sistemi di monitoraggio, quando non sia possibile ricondurne gli utilizzi ad un singolo operatore.
Le credenziali relative ad Utenze Privilegiate devono essere conservate in modalità sicura	Deve essere assicurata la conservazione sicura delle credenziali, tutti i prelevamenti devono essere tracciati ed il personale incaricato della gestione della piattaforma di conservazione non deve poter aver accesso alle credenziali conservate.
Non sempre le Utenze Privilegiate devono essere nella piena disponibilità degli operatori	In numerosi contesti operativi è preferibile che il personale incaricato di attività di maintenance e controllo sui sistemi abbia accesso soltanto a specifiche funzionalità fra quelle disponibili grazie alle utenze privilegiate

Obiettivi della soluzione

- La soluzione ricercata doveva consentire di **gestire le credenziali privilegiate** presenti sui **sistemi** e nelle **applicazioni** raggiungendo i seguenti obiettivi:
  - *Segregation of duties (SOD)*
  - *Sicurezza e protezione dalle frodi interne*
  - *Compliance alle normative e alle policy interne (Normativa 263 Banca d'Italia, Garante Privacy Allegato B, PCI-DSS …)*



Ambito di intervento



Piano di implementazione

2012

Analisi e scelta tecnologica

- **Definizione degli obiettivi e dell'ambito di intervento**
- **Definizione dei processi e delle procedure di accesso ai dati e tracciatura**
- **Scelta tecnologica ed installazione della piattaforma**
- **Definizione dei processi e delle procedure di accesso ai dati e tracciatura**

2013

Utenze amministrative e personali sui sistemi

- **Verifiche di compliance della soluzione alla normativa 263**
- **Integrazione di oltre 7000 sistemi :**
  - Sistemi UNIX
  - Sistemi Windows
  - Server Management Console
- **400 Database SQL**
- **Oltre 150 singoli utilizzatori della piattaforma CyberArk**

2014

Utenze amministrative e personali sui sistemi

- **Estensione della soluzione su altri sistemi (Sybase, ESX, …)**

Utenze tecniche privilegiate su applicazioni

- **Studio di fattibilità per l'implementazione della soluzione sulle applicazioni Websphere**

Risultati ottenuti

GOVERNANCE

- ***Controllo dei fornitori:*** *monitoraggio dell'accesso ai sistemi da parte di fornitori esterni o terze parti*
- ***Segregation of duties:*** *separazione tra il ruolo di "utilizzatore" delle utenze tecniche e privilegiate e il "controllore"*
- ***Centralizzazione del controllo:*** *costruzione di un servizio interno, gestito dalla Security, per la gestione delle utenze privilegiate, mediante l'utilizzo di un'unica piattaforma*

SICUREZZA

- ***Sicurezza dell'accesso:*** *credenziali mantenute centralmente in un repository cifrato con policy di accesso da parte del personale*
- ***Prevenzione delle frodi:*** *autorizzazione all'utilizzo delle utenze privilegiate e tracciatura delle azioni effettuate*

COMPLIANCE

- ***Normative e policy:*** *raggiungimento della conformità alle normative (Circolare Banca d'Italia 263, Garante della privacy, PCI-DSS) e alle policy interne*
- ***Monitoraggio e reporting:*** *monitoraggio dell'utilizzo delle utenze e reporting per analisi di anomalie e alerting*