Sicurezza delle utenze privilegiate

L’esperienza di Cedacri

Michele Rivieri, Responsabile Info Security e Definizione Regole Sicurezza di Cedacri

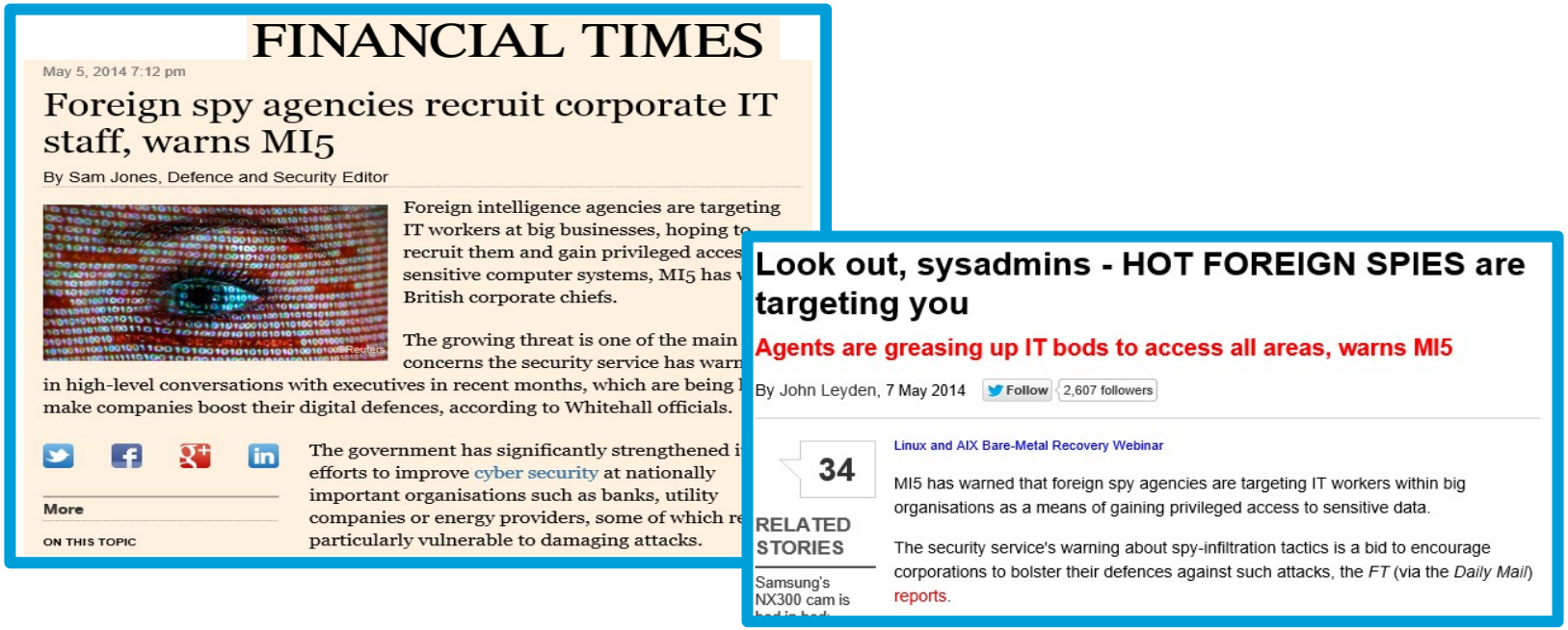
Il Gruppo Cedacri fornisce una gamma completa di servizi a supporto degli operatori bancari e industriali

- 1.400 dipendenti
- > 150 Clienti tra banche, istituzioni finanziarie, aziende industriali e di servizi
- > 256 Mln di fatturato Consolidato di Gruppo
- 2700 sportelli gestiti
- 30.000 Mips di potenza elaborativa Mainframe
- 4.000 Server
- 33.000 utenti utilizzatori del Sistema
- 50 milioni di transazioni gestite giornalmente

Contesto tecnico di riferimento

- Asset strategici per l'erogazione di servizi ad Istituti Bancari
- Infrastruttura server IT interna: server (Windows, Unix/Linux), Database, Mainframe

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'accesso 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 concerns the security service has warned in high-level conversations with executives in recent months, which are being held to make companies boost their digital defences, according to Whitehall officials.

The government has significantly strengthened its efforts to improve cyber security at nationally important organisations such as banks, utility companies or energy providers, some of which are particularly vulnerable to damaging attacks.

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

RELATED STORIES

Samsung's NX300 cam is

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.

Contesto normativo di riferimento

Normativa in materia di Protezione dei dati personali	Privacy e Amministratori di sistema	Provvedimento del Garante Privacy in materia di circolazione delle informazioni e di tracciamento delle operazioni bancarie	Normative in materia di segreto bancario	Normativa 263/285 Banca d'Italia
▪ Autorizzazione al trattamento dei dati personali ▪ Limitazione al trattamento dei dati personali (liceità, correttezza, pertinenza, …) ▪ Controllo accessi secondo l'approccio del minimo privilegio	▪ Selezione dei soggetti in grado di svolgere compiti amministrativi ▪ Lista aggiornata degli amministratori di sistema ▪ Revisione periodica degli amministratori di sistema ▪ Raccolta e conservazione dei log relativi agli accessi amministrativi (log-in/out)	▪ 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	▪ 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	▪ 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

Requisiti per la gestione delle utenze privilegiate

Utenze privilegiate	Qualsiasi sistema si avvale di utenze 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
Non interferenza coi sistemi	Qualsiasi sistema ed apparato si avvale di utenze privilegiate. Una soluzione di gestione deve operare senza interferire con i sistemi su cui opera
Ricondurre a persone le attività effettuate	Le Utenze Privilegiate possono essere un "blind spot" per i sistemi di monitoraggio, quando non sia possibile ricondurne gli utilizzi ad un singolo operatore.
Conservazione sicura delle credenziali	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.
Limitazione dell'utilizzo delle utenze privilegiate	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

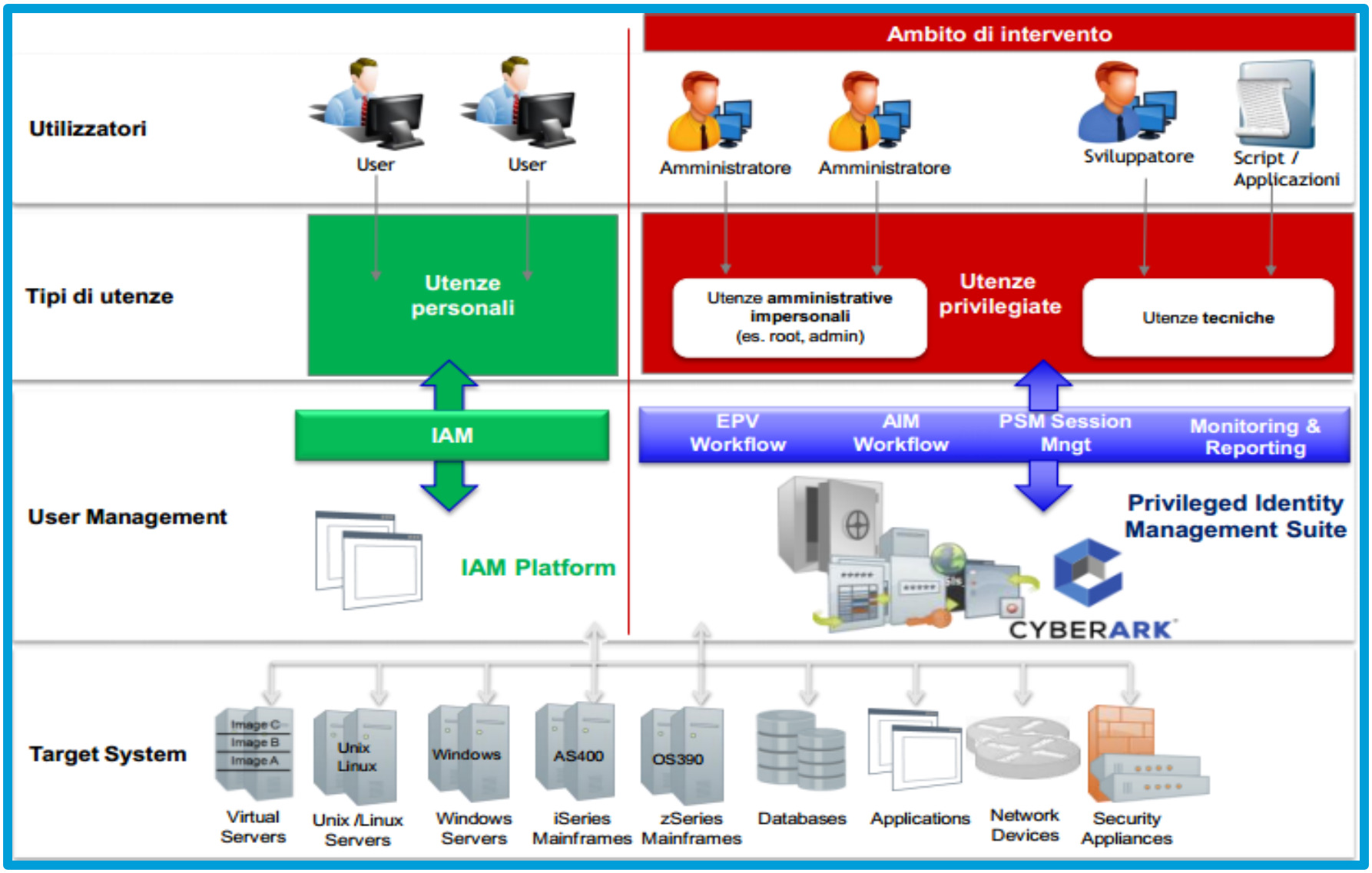
La soluzione ricercata doveva consentire di **gestire le credenziali privilegiate** presenti sui **sistemi** e nelle **applicazioni** raggiungendo i seguenti obiettivi:

- 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 …)

AMBITI DI INTERVENTO

Utenze Amministrative Personali	Utenze Tecniche Applicative
Utenze utilizzate per l'amministrazione dei sistemi (root, administrator)	**Utenze tecniche presenti nel codice applicativo o nei server applicativi**

Ambito di intervento



CEDACRI GROUP

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"
  - Possibilità di gestire dinamicamente l'accesso degli sviluppatori alla produzione solo in caso di necessità e in modo controllato
- Centralizzazione del controllo: costruzione di un servizio interno, gestito dalla Security, per la gestione delle utenze privilegiate, mediante l'utilizzo di un'unica piattaforma
- Creazione di un «asset di sicurezza» de facto

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 (Garante della Privacy, normativa 285 .....) e alle policy interne
- Monitoraggio e reporting: monitoraggio dell'utilizzo delle utenze e reporting per analisi di anomalie e alerting

Infrastrutture gestite

- Cedacri ha realizzato la copertura tramite la soluzione Cyberark di tutti i server di produzione relativi ai suoi servizi interni e al servizio di Full Outsourcing fornito ai suoi clienti (circa 2000 sistemi e 8000 utenze per circa 800 utenti)

- Cedacri sta inoltre fornendo come servizio la copertura a due clienti in facility per un totale di circa 2500 server e 8000 utenze per circa 600 utenti.

- Grazie alla partnership con Cyberark e col partner PuntoIT e alla sua esperienza tecnica e normativa del mondo bancario, Cedacri può offrire il servizio di gestione della sicurezza delle utenze privilegiate a tutti gli istituti che ne abbiano necessità.

Piano di implementazione e next steps

2015

- Scansioni Utenze Privilegiate presenti sui sistemi gestiti
- Deployment infrastruttura Cyberark
- Realizzazione di un Pilota sulle diverse realtà gestite

2016

- Incrementato il perimetro a coprire tutti I sistemi gestiti
- Chiusura dei firewall (accesso esclusivamente tramite PSM) ove richiesto
- Installazione demo Privileged Threat Analysis e Viewfinity
- Installazione viewfinity sui client Cedacri

2017

- Valutazione Implementazione PTA
- Gestione utenze tecniche applicative (AIM)