“Nuove disposizioni di vigilanza prudenziale per le banche”
La gestione delle utenze amministrative e tecniche: il caso UBIS

Alessandro Ronchi
Senior Security Project Manager

CONTENUTI

Obiettivo:
rafforzare le capacità delle banche e dei gruppi bancari di presidiare i rischi aziendali, creando un quadro normativo organico e coerente con le migliori prassi internazionali e con le raccomandazioni dei principali standard.

- **Il Capitolo 7** definisce un quadro organico di **principi e regole cui deve essere ispirato il sistema dei controlli interni**, che deve risultare completo, adeguato, funzionale e affidabile.
- **Il Capitolo 8** contiene la **disciplina del sistema informativo** che è stata integralmente rivista, anche per recepire le principali evoluzioni emerse nel panorama internazionale.
- **Il Capitolo 9** disciplina la materia della **continuità operativa**, riorganizzando le disposizioni attualmente contenute in diverse fonti.

Riferimenti:
https://www.bancaditalia.it/vigilanza/normativa/norm_bi/circ-reg/vigprud/agg_15_del_02072013

Titolo V - Capitolo 8 - IL SISTEMA INFORMATIVO


BANCA D'ITALIA
EUROSISTEMA

Nuove disposizioni di vigilanza prudenziale per le banche

Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013

Le banche si conformano alle disposizioni contenute nel Capitolo 8 (Il sistema informativo), incluse le raccomandazioni della BCE in materia di sicurezza dei pagamenti in internet, **entro il 1° febbraio 2015 (data di efficacia).**

SEZIONE IV - LA GESTIONE DELLA SICUREZZA INFORMATICA

3. La sicurezza delle informazioni e delle risorse ICT

"Tali misure sono distribuite su diversi strati, <<… >> comprendendo:

- la procedura di **autenticazione per l'accesso alle applicazioni e ai sistemi;** in particolare sono garantiti **l'univoca associazione a ciascun utente delle proprie credenziali di accesso, il presidio della riservatezza dei fattori di autenticazione, l'osservanza degli standard definiti all'interno nonché delle normative applicabili,** ad es. in materia di composizione e gestione della password, di limiti ai tentativi di accesso, di lunghezza di chiavi crittografiche;
- le procedure per lo svolgimento delle operazioni critiche, garantendo il **rispetto dei principi del minimo privilegio e della segregazione dei compiti** (ad es., specifiche procedure di abilitazione e di autenticazione, **controlli di tipo four eyes, o di verifica giornaliera ex post**);
- **il monitoraggio, anche attraverso l'analisi di log e tracce di audit, di accessi, operazioni e altri eventi** al fine di prevenire e gestire gli incidenti di sicurezza informatica; **le attività degli amministratori di sistema e altri utenti privilegiati delle componenti critiche sono sottoposte a stretto controllo;**
- le regole di **tracciabilità delle azioni svolte**, finalizzate a consentire la verifica a posteriori delle operazioni critiche, con l'archiviazione dell'autore, data e ora, contesto operativo e altre caratteristiche salienti della transazione. **Le tracce elettroniche sono conservate per un periodo non inferiore a 24 mesi in archivi non modificabili** o le cui modifiche sono puntualmente registrate."

Caso UBIS: metodo adottato

1. Analisi della **normativa 263 e delle policy aziendali** in essere

2. Analisi dello **stato attuale di compliance** rispetto a quanto previsto dalla normativa:
   - Processi, procedure operative
   - Soluzioni tecniche implementate

3. Identificazione della **soluzione tecnica**

4. **Implementazione** della soluzione tecnica
   - Test funzionali e validazione
   - Passaggio in produzione

5. **Revisione dei processi e delle procedure** interne

Data Access Management:

Compliance alla circolare 263

Circolare 263
Titolo V – Capitolo 8

- **Autenticazione:** univoca associazione a ciascun utente delle proprie credenziali di accesso
- **Minimo privilegio e della 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

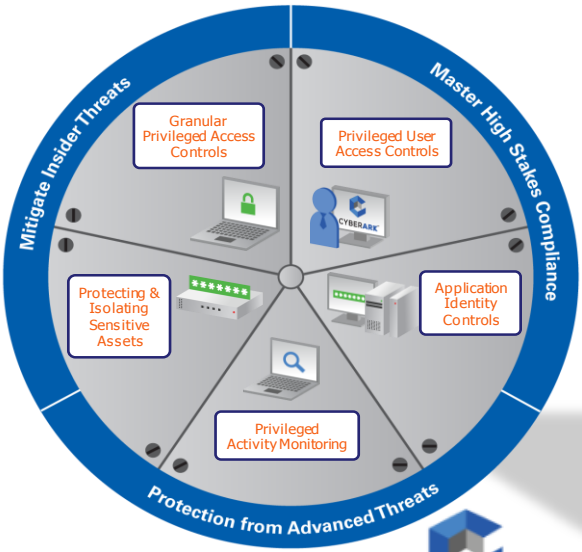
Sistemi

- ***Le credenziali amministrative*** *(root, administrator) sono sottoposte a policy di* ***complessità*** *e* ***ciclo di vita*** *(cambio password)*
- *Possibilità di effettuare il* ***cambio password*** *degli account amministrativi* ***ogni qualvolta questo venga utilizzato da un operatore***
- ***Assegnazione di privilegi minimi agli utenti*** *che utilizzano l'utenza* ***solo per il tempo necessario a svolgere l'attività***
- ***Tracciatura dell'accesso e dell'utilizzo*** *delle credenziali amministrative*
- ***Produzione di report ed invio di log*** *in real-time al SIEM*

Applicazioni

- *Possibilità di effettuare il* ***cambio password*** *delle utenze tecniche in conformità*
- ***Eliminazione delle credenziali da script e/o codice applicativo,*** *disperse sui server applicativi*
- ***Credenziali*** *utilizzate dalle applicazioni non più a conoscenza di* ***sviluppatori ed amministratori delle applicazioni***
- ***Tracciatura dell'accesso e dell'utilizzo*** *delle credenziali amministrative*
- ***Produzione di report ed invio di log*** *in real-time al SIEM*

Tecnologia: CyberArk



La soluzione PIM **CyberArk** permette di:

- **Conservare e gestire centralmente le utenze privilegiate** (root, administrator ecc) presenti sui sistemi e sulle applicazioni
- **Eliminare la conoscenza** delle utenze privilegiate da parte di **sistemisti** e di **gestori** delle applicazioni
- Garantire l'accesso e l'uso delle credenziali solo **quando necessario,** sulla base di criteri di **autorizzazione, segregazione, minimo privilegio**
- Far eseguire in **modalità controllata** comandi o di intere sessioni agli utenti, mediante un **processo autorizzativo da parte di terze parti** (four eyes control)
- Separare il provisioning delle utenze (IAM) dal controllo del loro utilizzo
- **Tracciare l'accesso** e l'utilizzo delle credenziali privilegiate **le azioni eseguite attraverso log, registrazioni video e report**
- Conservare log in **repository cifrati** e inalterabili

La **suite CyberArk** offre quindi una **soluzione integrata** rispondente alle disposizioni della "Circolare 263 Titolo V - Capitolo 8"


BANCA D'ITALIA
EUROSISTEMA

Nuove disposizioni di vigilanza prudenziale per le banche

Caso UBIS: implementazione -1

Installazione piattaforma CyberArk

Implementazione piattaforma CyberArk in configurazione di HA e DR presso la farm UBIS

- Installazione della piattaforma CyberArk con configurazione HA e DR
- Configurazione dei diversi ruoli di accesso ed utilizzo della piattaforma (amministratore, utente, auditor)
- Predisposizione all'invio dei log alla piattaforma esterna (SIEM)

Integrazione di Sistemi ed Utenze amministrative impersonali

Integrazione Utenze amministrative e impersonali sui sistemi

- Censimento dei sistemi coinvolti e degli amministratori dei sistemi
- Integrazione dei sistemi con eventuale sviluppo di soluzioni "custom":
  - Sistemi (Linux, AIX, Windows,…)
  - Database (SQL, Sybase …)
  - …
- Integrazione degli user repository (LDAP, Active Directory) con la piattaforma CyberArk
- Implementazione SoD sugli account:
  - Integrazione utenze amministrative impersonali (root, admin, …)
  - Gestione automatica delle credenziali amministrative secondo policy interne/normativa
  - Raccolta automatica dei log delle attività effettuate ed invio a SIEM

Caso UBIS: implementazione -2

Studio di fattibilità per espansione soluzione ad Applicazioni ed Utenze Tecniche

Utenze tecniche privilegiate su applicazioni

- Censimento delle applicazioni aziendali
- Identificazione degli ambienti sui quali le applicazioni operano con le utenze tecniche (es. DB)
- Censimento delle utenze tecniche presenti nel codice applicativo e configurate sugli Application Server
- Integrazione degli user repository (LDAP, Active Directory, OID RACF) nella piattaforma CyberArk
- Migrazione delle applicazioni e riconfigurazione degli Application Server per permettere l'utilizzo delle credenziali centralizzate in CyberArk
- Definizione delle policy di gestione degli account (accesso degli utenti, cambio password, …)
- Raccolta automatica dei log ed invio a piattaforma SIEM

Processi e procedure

Definizione dei processi di utilizzo e monitoraggio delle utenze privilegiate

- Revisione delle modalità di utilizzo delle utenze privilegiate
- Definizione di ruoli e responsabilità: amministratore piattaforma, utilizzatore account, autorizzatore, auditor
- Definizione del processo di richiesta e rilascio delle utenze tecniche e privilegiate
- Tracciatura, monitoraggio e controllo sugli accessi avvenuti e sulle azioni effettuate

Benefici operativi

Segregation of duties - Sicurezza - Compliance

Ambito	Situazione iniziale	Situazione finale
Riservatezza delle credenziali	✗ Credenziali **a conoscenza dei sistemisti** (personale interno o fornitori)	✓ I gestori dei sistemi (personale interno o fornitori) **non sono più a conoscenza** delle credenziali
	✗ Credenziali presenti **in chiaro** nelle **configurazioni locali**	✓ Credenziali **non più presenti** nel codice applicativo ma centralizzate in un **repository cifrato**
Centralizzazione credenziali	✗ Credenziali **distribuite all'interno delle applicazioni** o delle **configurazioni locali**	✓ **Accesso alle utenze privilegiate controllato e autorizzato**
Policy	✗ Non applicate	✓ Applicate e verificate
Cambio della password delle utenze	✗ Attuabile con significativi change applicativi ed impatti sulla produzione	✓ Applicabile senza impatti sulla produzione
Monitoraggio dell'utilizzo delle utenze	✗ Log non presenti	✓ Log presenti in Cyber-Ark ed inviati in tempo reale alla piattaforma SIEM

Risultati ottenuti

Ambito	Descrizione

Sicurezza dell'accesso	• **Protezione dell'accesso ai dati:**
	  ◦ Sicurezza credenziali: mantenute **centralmente** in un **repository cifrato**
	  ◦ Definizione delle **policy di accesso** agli account tecnici da parte del personale
	• **Riduzione delle Frodi interne:**
	  ◦ I gestori dei sistemi (personale interno o fornitori) **non sono più a conoscenza** delle credenziali
	  ◦ **Tracciatura** dell'**utilizzo** delle utenze tecniche e delle **azioni** effettuate

Segregation of duties (SOD)	• **Separazione tra provisioning** delle utenze amministrative sui sistemi (IAM) e il **monitoraggio/controllo** del loro utilizzo • **Separazione dei ruoli tra utilizzatori** delle utenze privilegiate - personale interno o esterno (es. outsourcer) - e ruolo di **controllo/autorizzazione** al loro utilizzo
Regulatory and Compliance	• Applicazione di **password policy** alle utenze privilegiate • Gestione **ciclo di vita** delle utenze privilegiate • Rispetto di **standard e normative:** 263 Banca d'Italia, Garante Privacy Allegato B, Bank Secrecy, BSDG, PCI-DSS

Il Gruppo EXPRIVIA

Fatturato: 132 Milioni €
Dipendenti: 1500

Exprivia SpA è una azienda **italiana**, con **presenza internazionale** in Europa, Sud America e Cina, focalizzata nello **sviluppo** e nell'**implementazione** di soluzioni IT.

EXPRIVIA BANCHE e FINANZA

100 Clienti
30 Milioni fatturato
200 Professionisti

L'offerta "verticale"

- Finanza
- Crediti
- Factoring

L'offerta "trasversale"

- Big Data Intelligence & Analytics
- Customer Experience / Multicanalità
- ICT Security & GRC
- Gestione Operativa

L'offerta di security

Governance Risk Compliance

- Information management
- Compliance
- Business Intelligence
- Security Dashboard
- Business Continuity / DR

Security Infrastructure

- Log management
- Fraud management
- Identity management
- Data loss prevention

Security Operations

- Security Assessment
- Gestione delle infrastrutture
- Monitoraggio dei sistemi di sicurezza

50 Professionisti dedicati alla sicurezza

Consulenza → Integrazione → Esercizio