# REPORT DELLE AZIONI DA INTRAPRENDERE SULLA GESTIONE DEI CONTROLLI DI ACCESSO

## Introduzione

Questo report descrive le azioni da intraprendere per la raccolta di informazioni necessarie alla conduzione di un risk assessment sulla gestione dei controlli di accesso per un'azienda. L'obiettivo è identificare le persone chiave da intervistare, i tipi di documentazione da rivedere e i test da eseguire per valutare la configurazione dei sistemi IT e la sicurezza delle reti, in linea con le normative NIST SP 800-53.
Elenco delle Persone Chiave da Intervistare e Argomenti di Discussione:

**Responsabile della Sicurezza Informatica (CISO)**
Argomenti di Discussione:

- Politiche di sicurezza attuali
- Protocolli di gestione degli accessi
- Incidenti di sicurezza passati
- Piani di risposta agli incidenti

**Head IT administrator**
Argomenti di Discussione:

- Architettura della rete
- Sistemi di controllo degli accessi fisici e logici
- Backup e disaster recovery
- Processi di aggiornamento dei sistemi

**Amministratore di Sistema**

Argomenti di Discussione:

- Configurazione dei sistemi IT
- Gestione degli account utente e dei permessi
- Monitoraggio e log
- Configurazione degli strumenti di gestione della sicurezza utilizzati

**Responsabile delle Risorse Umane**

Argomenti di Discussione:

- Procedure di onboarding
- Formazione sulla sicurezza per i dipendenti
- Politiche di verifica delle identità
- Gestione delle credenziali dei dipendenti

## Tipi di Documentazione da Rivedere

La documentazione è fondamentale per un piano di risk assessment, permette di acquisire informazioni su processi, sistemi, sicurezza e politiche passate e in uso in azienda.
Per lo scenario in esame andremo a rivedere i seguenti documenti:

- Politiche e Procedure di Sicurezza
- Politiche di gestione degli accessi
- Procedure di autenticazione e autorizzazione
- Linee guida per la gestione delle password
- Piani di risposta agli incidenti
- Documentazione dei Sistemi IT
- Configurazioni e architettura di rete
- Documentazione sui dispositivi di sicurezza (firewall, IDS/IPS, ecc.)
- Report di Audit (interni ed esterni) e Valutazioni Precedenti

## Test da Eseguire per Raccogliere Dati sulla Configurazione dei Sistemi IT e sulla Sicurezza delle Reti

Oltre alle interviste ed alla review della documentazione aziendale, i dati possono essere raccolti da attività di test. I test servono per portare in luce dati che altrimenti non potremmo raccogliere e analizzare, questo perché negli anni le attrezzature e le configurazioni possono cambiare.

Dato l'aggiornamento a nuovi prodotti e nuove configurazioni i sistemi possono esporre vulnerabilità che prima non erano presenti. I test consigliati per questo scenario sono i seguenti:

**Vulnerability Assessment**
Scansione delle vulnerabilità dei sistemi e delle reti per identificare punti deboli e possibili falle di sicurezza.

**Penetration Testing**
Simulazione di attacchi per testare la robustezza dei controlli di accesso, identificando le potenziali vie di compromissione.

**Revisione delle Configurazioni**
Analisi delle configurazioni dei firewall, router e switch per garantire che siano in linea con le pratiche di sicurezza aziendali e conformi alle normative utilizzate per la gestione del rischio aziendale.

**Test di Controllo degli Accessi**
Verifica dei permessi utente e delle policy di accesso per assicurarsi che solo gli utenti autorizzati abbiano accesso alle risorse sensibili. Questo comprende la valutazione dei controlli IAM, MFA ed altre pratiche che l'azienda ha implementato per il controllo degli accessi.

**Analisi dei Log**

Monitoraggio e analisi dei log di accesso e delle attività di sistema per identificare anomalie e comportamenti sospetti.

**Test di Incident Response**

Esecuzione di test sui piani di risposta agli incidenti per verificare l'efficacia e la prontezza del team di sicurezza nel rispondere a potenziali incidenti di sicurezza. Possiamo testare un piano di incident response mettendo in atto procedure controllate di attacco.

## Conclusione

La collaborazione con le persone chiave, la revisione della documentazione rilevante e l'esecuzione di test specifici consentiranno di identificare le aree di rischio e di sviluppare strategie adeguate per mitigare tali rischi ed attuare un ottimo piano di risk assessment.