PHANTOM SRL

**Presented By :**
Iannone Luca
Pignatello Giuseppe
D'Ottavio Alessio

# RISK COMUNICATION

www.phantomatici.com

# INDICE

# TRACCIA

EPICODE

**Risk management**
Esercizio

Un'azienda ha richiesto la raccolta di informazione per la conduzione di un risk assessment. Lo scenario da valutare è la gestione dei controlli di accesso.

- Prepara un elenco di persone chiave da intervistare nell'azienda e i potenziali argomenti di discussione per ciascuna di esse.
- Identifica i tipi di documentazione che dovresti rivedere per raccogliere informazioni su processi, sistemi e controlli di sicurezza.
- Descrivi i test che potresti eseguire per raccogliere dati sulla configurazione dei sistemi IT e sulla sicurezza delle reti.

Ricordatevi delle risorse utilizzate nell'esercizio di ieri e del materiale relativo ai controlli.

# ELENCO DELLE PERSONE CHIAVE DA INTERVISTARE:

## Responsabile della sicurezza informatica (CISO):

Approccio generale alla sicurezza informatica dell'azienda,
Politiche e procedure relative alla gestione dei controlli di accesso,
Visione sulle minacce e le vulnerabilità attuali e
Strategie di difesa e risposta agli incidenti.
E' bene consultare il CISO prima di condurre un risk assessment perchè conosce in linea generale tutto il contesto di sicurezza informatica all'interno dell'azienda. Le informazioni che si possono ricavare da questa figura sono preziose e consentono di condurre al meglio il risk assessment.

## Digital Risk Manager:

Valutazione e gestione dei rischi digitali dell'azienda,
Identificazione delle potenziali minacce e vulnerabilità e
Sviluppo di strategie per mitigare i rischi legati alla gestione dei controlli di accesso.
Questa figura è indispensabile per lo sviluppo di un risk assessment, è uno specialista del rischio e può condividere informazioni e consigli fondamentali al fine di rendere il risk assessment il più completo possibile.

## Responsabile HR:

Processo di onboarding e offboarding dei dipendenti,
Politiche di accesso basate sui ruoli e sui privilegi e
Procedure di gestione delle credenziali degli utenti.
Il responsabile HR conosce informazioni preziose per l'onboarding e offboarding dei dipendenti, quindi è a stretto contatto con il controllo degli accessi.

## Team di SOC Analyst (Security Operations Center):

Analisi degli eventi di sicurezza e risposta agli incidenti,
Monitoraggio degli accessi e delle attività sospette e
Segnalazione delle violazioni dei controlli di accesso.
Il team di SOC Analyst è l'organo più a stretto contatto con il monitoraggio degli accessi e non solo. Le informazioni che si possono ricavare sono indispensabili.

## Team di NOC Analyst (Network Operations Center):

Monitoraggio della rete e dei dispositivi di sicurezza,
Identificazione delle anomalie di traffico e dei possibili attacchi e
Collaborazione con il team di sicurezza informatica per mitigare le minacce.
Gli analisti del NOC conoscono ogni lato dell'infrastruttura fisica della rete, sono fondamentali per la buona riuscita del risk assessment.

**Help Desk:**
Assistenza agli utenti per problemi di accesso e autenticazione,
Registrazione e gestione dei ticket relativi ai controlli di accesso e
Rilevamento di anomalie o segnalazioni di utenti riguardanti l'accesso non autorizzato.
L'help desk si occupa di gestione dei ticket relativi ai controlli di accesso, quindi anche le informazioni reperibili da questo organo sono molto importanti.

# DOCUMENTAZIONE DA SEGUIRE

Una delle tabelle più utilizzate del National Institute of Standards and Technology (NIST) nel contesto del risk management è la tabella 800-53, parte della serie di documenti NIST Special Publication 800-53 intitolata "Security and Privacy Controls for Federal Information Systems and Organizations".
All'interno della NIST SP 800-53, la tabella 800-53 fornisce un insieme completo di controlli di sicurezza che possono essere utilizzati per gestire e mitigare i rischi di sicurezza delle informazioni.
Ecco un esempio di famiglie di controlli presenti nella tabella **NIST SP 800-53**:

1. **Access Control (AC)**: Questa famiglia di controlli riguarda la gestione dell'accesso alle risorse di sistema e delle informazioni. Include controlli come l'identificazione e l'autenticazione degli utenti, la gestione dei privilegi di accesso e il controllo dell'accesso fisico e logico.
2. **Audit and Accountability (AU)**: Questa famiglia di controlli si concentra sulla registrazione e sull'analisi delle attività di sistema per garantire la responsabilità e la tracciabilità delle azioni degli utenti. Include controlli come la registrazione delle attività, la protezione dei log e l'analisi degli eventi di sicurezza.
3. **Risk Management (RM)**: Questa famiglia di controlli è specificamente dedicata al risk management. Include controlli che supportano l'identificazione, l'analisi, la valutazione e la mitigazione dei rischi di sicurezza delle informazioni. Alcuni esempi di controlli in questa famiglia includono l'identificazione dei rischi, l'analisi delle vulnerabilità, la valutazione degli impatti e la pianificazione della continuità operativa.

La tabella NIST SP 800-53 fornisce dettagli su ciascun controllo, inclusi scopo, implementazione e riferimenti pertinenti ad altre linee guida e standard. È una risorsa estremamente utile per le organizzazioni che cercano di sviluppare e implementare un programma di sicurezza delle informazioni completo e conforme alle migliori pratiche.

# APPENDIX K DEL NIST:

In particolare nel contesto del **Risk Assessment** è bene seguire l'Appendice K del documento NIST-SP 800-30.
Complessivamente, questa appendice fornisce una guida dettagliata per le organizzazioni che desiderano valutare e gestire i rischi di sicurezza informatica associati alle terze parti con cui fanno affari, aiutando a proteggere l'organizzazione da potenziali minacce e vulnerabilità derivanti da queste relazioni, alcuni punti salienti di questa appendice sono:

1. **Introduzione al rischio della terza parte**: L'appendice inizia spiegando il concetto di rischio della terza parte e perché è importante per le organizzazioni comprendere e mitigare questi rischi.
2. **Definizioni e concetti chiave**: Viene fornita una serie di definizioni e concetti chiave relativi alla gestione del rischio della terza parte, che aiutano a stabilire una base comune per la discussione.
3. **Processo di gestione del rischio della terza parte**: L'appendice descrive un processo strutturato per valutare e gestire i rischi di sicurezza informatica legati alle terze parti. Questo processo può includere l'identificazione delle terze parti coinvolte, l'analisi dei rischi associati a ciascuna terza parte, la valutazione dei controlli di sicurezza implementati da esse e la mitigazione dei rischi identificati.
4. **Documentazione e comunicazione**: Viene discusso l'importanza della documentazione e della comunicazione efficace riguardo ai rischi della terza parte, compresa la necessità di contratti o accordi di servizio che definiscano le responsabilità e le aspettative in materia di sicurezza informatica.

# COBEL

Per quanto riguarda il framework Cobel, abbiamo deciso di selezionare l'**EG07-"Quality of management information"**, e si concentra sull'assicurare che l'informazione utilizzata per la gestione aziendale sia di alta qualità, tempestiva, rilevante e sicura, fornendo così una base affidabile per prendere decisioni informate e guidare le attività dell'organizzazione.
L'Alignment Goal selezionato è invece L'**AG07-"Security of information, processing infrastructure and applications, and privacy"** e mira a garantire che l'IT e le iniziative IT siano allineate agli obiettivi strategici dell'organizzazione, consentendo così un utilizzo efficace delle risorse e un contributo significativo al successo complessivo dell'azienda.
Infine per quanto riguarda Governance e Gestione Obiettivi e Finalità, abbiamo scelto due punti per noi importantissimi, **l'EDM03 e l'APO12**. Il COBEL è un framework indispensabile per la conduzione di un ottimo risk assessment, è bene sempre consultarlo!

# 1) INDIVIDUAZIONE DELLE VULNERABILITÀ:

## Configurazioni di Accesso Non Sicure:

Usiamo strumenti come **Nessus o OpenVAS** per scovare configurazioni deboli sui nostri sistemi di accesso.

## Mancanza di Aggiornamenti dei Software:

Dai un'occhiata a **Qualys o Rapid7** per vedere se abbiamo bisogno di qualche aggiornamento di sicurezza.

## Debolezze nei Protocolli di Rete:

Con **Wireshark o Nmap**, controlliamo se ci sono debolezze nei protocolli di rete che usiamo per l'autenticazione.

## Password Deboli o Condivise:

Con strumenti come **Hydra o John the Ripper**, cerchiamo password deboli o condivise nei nostri sistemi.

# 2) VALUTAZIONE DELLE VULNERABILITÀ:

Per ogni problema, valutiamo:

La **probabilità** che possa essere sfruttato (alta, media, bassa).
L'**impatto** sulla sicurezza e le operazioni aziendali (alto, medio, basso).
La **criticità** del problema (alta, media, bassa).

| Rischio | Probabilità | Impatto | Criticità |
|---|---|---|---|
| Violazione della Privacy dei Dati | Alta | Alto | Alta |
| Perdita di Dati Sensibili | Media | Alto | Media |
| Violazione della Conformità Normativa | Alta | Alto | Alta |
| Interferenze con le Operazioni Aziendali | Media | Medio | Medio |

# 3) Trattamento delle Vulnerabilità:

Per ogni problema, vediamo cosa possiamo fare:

**Patch e Aggiornamenti**: Utilizziamo WSUS o yum/apt per aggiornare e correggere le vulnerabilità.
**Miglioramento delle Politiche di Accesso**: Configuriamo le politiche di password con Active Directory Group Policy.
**Ripristino delle Configurazioni di Sicurezza**: Automatizziamo il ripristino con Ansible o Puppet.

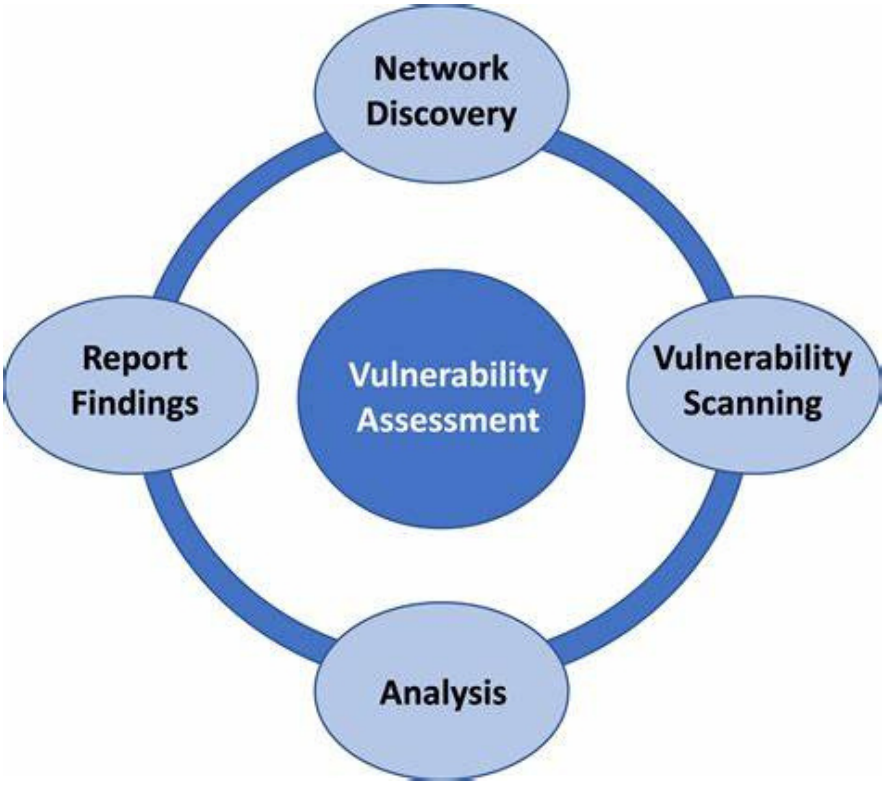
# 4) Implementazione delle Misure Correttive:

Attuiamo le soluzioni identificate:

Distribuiamo patch e aggiornamenti con i nostri tool di gestione dei patch.
Configuriamo le politiche di accesso e le regole di sicurezza usando gli strumenti giusti.
Monitoriamo costantemente il sistema con Nagios o Zabbix per individuare e mitigare nuove vulnerabilità.

# 5) Monitoraggio e Aggiornamento:

Continuiamo a monitorare e ad aggiornare il sistema per affrontare nuove minacce ed è essenziale formare costantemente i dipendenti riguardo la cybersecurity.



PHANTOM SRL

**Presented By :**
Iannone Luca
Pignatello Giuseppe
D'Ottavio Alessio

# GRAZIE

**www.phantomatici.com**