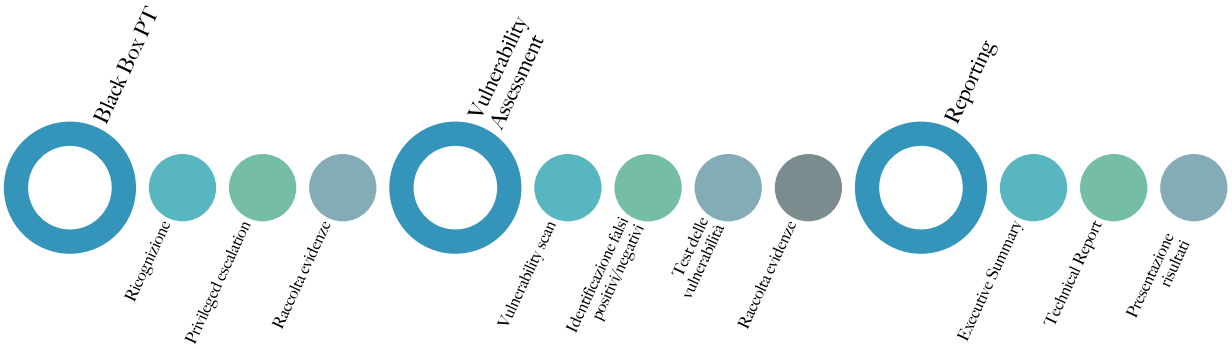
Oggetto: vulnerability assessment e penetration test

Con il seguente documento siamo a descrivervi sinteticamente le attività di esecuzione di penetration test e vulnerability assessment che possono essere svolte con cadenza trimestrale.

Descrizione dell'attività

L'attività prevede una prima fase di penetration testing con l'obiettivo di ottenere il controllo della rete.
A seguito dell'attività di PT si procederà con l'attività di vulnerability assessment al fine di rilevare di tutte le potenziali vulnerabilità presenti indipendentemente dal fatto che siano state sfruttate o meno nella fase di PT.
La fase di penetration test verrà eseguita in modalità manuale al fine di identificare le reali path di attacco mentre per la parte di vulnerability assessment i consulenti si avvarranno di strumenti di scansione automatica.
I risultati verranno in ogni caso valutati manualmente testando le vulnerabilità indentificate al fine di raccogliere evidenze relative alla reale possibilità di sfruttare le vulnerabilità identificate ed escludere la presenza di falsi negativi e/ o falsi positivi



Metodologia

Durante l'attività verranno utilizzati sia strumenti di scansione automatica per la ricerca delle vulnerabilità note, sia tecniche di attacco manuali al fine di verificare la reale possibilità di sfruttamento delle vulnerabilità rilevate.
I nostri specialisti si avvalgono della metodologia OSSTM per quanto riguarda i test infrastrutturali mentre per le attività relative al testing applicati vengono seguite le linee guide definite da OWASP.
Di seguito un elenco, non esaustivo delle attività che verranno svolte durante l'assessment:

- Enumerazione dei servizi esposti attraverso attività di port scanning che permettano di identificare tutte le porte TCP e UDP eventualmente esposte
- Esecuzione di scansione automatizzata con vulnerability scanner
- Identificazione dei servizi in uso e della loro versione (ove possibile)
- Analisi dell'output dei vulnerability scanner al fine di individuare falsi positivi
- **Tentativo di password brute-forcing (se previsto dalle regole di ingaggio)**
- Tentativi di privilege escalation (se previsto dalle regole di ingaggio)
- Tentativi di sfruttamento delle vulnerabilità rilevate (se previsto dalle regole di ingaggio)
- Raccolta di evidenze delle attività svolte e degli impatti critici sull'infrastruttura

Reportistica

Al termine dell'assessment verrà prodotto un report contente le vulnerabilità rilevate e le relative evidenze, in particolare nel report sarà presente:

- **Executive report:** un riassunto di alto livello, dedicato a personale non tecnico, di quanto rilevato atto a fornire una visione di insieme dell'attività e a definire una strategia di remediation
- **Technical report:** sunto delle attività svolte, delle metodologie impiegate e dei risultati ottenuti con il dettaglio degli aspetti tecnici e delle attività necessarie per mitigare le vulnerabilità.
  L'attività prevederà report separati per ogni modalità di test
- **Discussione del report**

Strumenti

Durante il penetration test ci potremo avvalere dei seguenti strumenti (elenco non esaustivo):

Tool	Descrizione
Nessus/Nexpose	Vulnerability scanner che permette di individuare eventuali vulnerabilità note, configurazioni standard non sicure e mancate configurazioni
Nmap	Strumento open source per analisi di rete, permette attraverso varie tecniche e modalità di identificare gli host attivi in rete e le relative porte aperte (comprese la versione del servizio e del sistema operativo)
Hydra	Tool open source dedicato all'identificazione di password mediante attacchi brute force e dizionario
Kali Linux	Kali Linux è una distribuzione sviluppata per l'informatica forense e la sicurezza informatica, in particolare per effettuare penetration test. Kali offre una larga collezione di tools per la sicurezza dal port scanning ai password cracker.
Impacket	Tool specificatamente sviluppato per il testing dell'infrastruttura di Dominio Microsoft

Scope

Internal PT

- Asset: Tutti i dispositivi presenti nelle reti locali del cliente
- Modalità: Black Box

Requisiti

- Accesso Fisico alla sede
- Possibilità di accesso alla rete LAN
- Visibilità delle subnet da testare
- Subnet e/o indirizzi IP da testare ed eventuali esclusioni
- Identificazione degli asset critici
- Firma del documento di Manleva

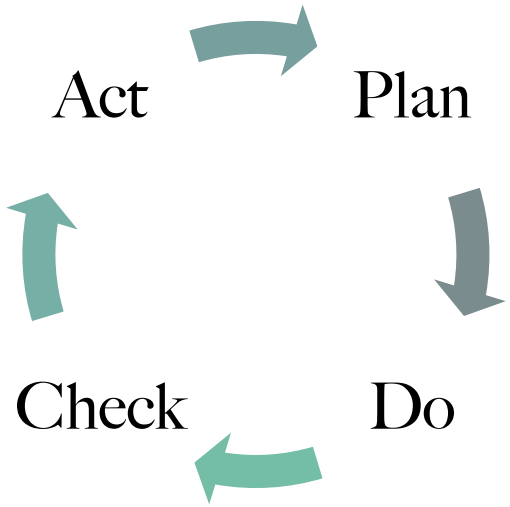
Vincoli di Riservatezza

Le informazioni contenute nella presente offerta, relative ai e servizi di Invisiblefarn S.r.l e Fragma Security S.r.l., sono da considerarsi strettamente riservate e sono di esclusiva proprietà di Invisiblefarn S.r.l e Fragma Security S.r.l.; tali informazioni devono pertanto essere utilizzate unicamente dal personale dell'azienda cliente autorizzato a valutare la presente offerta.

Ringraziandovi per l'attenzione, vi salutiamo cordialmente.

Oggetto: IT Information Security Audit

Con il seguente documento siamo a descrivervi sinteticamente in merito alle attività di:



- Valutazione del livello di maturità in termini di sicurezza delle informazioni dell'organizzazione
- Identificazione delle misure da applicare in via priorità
- Definizione di un piano di azione indicante tempistiche e soluzioni da applicare

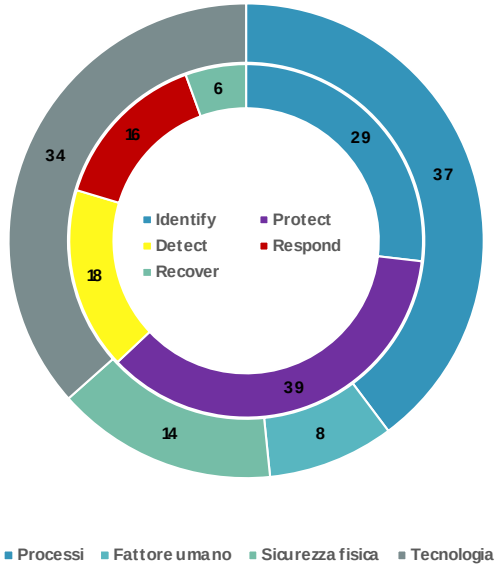
Come tutti i processi aziendali la sicurezza aziendale dovrebbe considerare un approccio ciclico orientato al miglioramento continuo di conseguenza alcune delle attività di seguito descritte dovrebbero essere ripetute periodica (ad esempio l'attività di security audit).

Tutte le 'attività previste si baseranno sulle linee guida descritte dallo standard ISO 27001:2022 (ISMS), che definisce come implementare un sistema di gestione per la sicurezza delle informazioni, e il relativo Annex A che identifica i controlli di sicurezza ritenuti necessari per garantire un'adeguata protezione delle informazioni trattate dall'organizzazione.

La scelta di utilizzare come riferimento la norma ISO27001:2022 è dovuta ai seguenti motivi:

- **Possibilità di dividere i controlli in 4 aree** (Processi, Tecnologia, Fattore Umano, Sicurezza Fisica) facilitando la gestione della conformità interna e la suddivisione dei compiti all'interno dell'organizzazione
- **Possibilità di utilizzare l'audit come base per l'avvio di un processo di** conformità alla norma in ottica di una certificazione
- **Migliore riconoscimento da parte della supply chain**: soprattutto per quanto riguarda il mondo europeo ISO27001 è la base delle principali norme cogenti (GDPR, NIS/NIS2, PNSC, ecc.) e standard di settore. Di conseguenza qualora all'organizzazione venga richiesta da una terza la dimostrazione dell'applicazione di controlli di sicurezza, un audit basato su ISO27001 agevolerebbe la conformità

Al fine di semplificare l'applicazione dei controlli e delle misure di sicurezza consigliate nonostante **l'analisi venga condotta seguendo la norma ISO27001 nella reportistica, per ciascun controllo, verranno inoltre indicati i riferimenti anche ai controlli del NIST Cyber Security Framework (CSF) e alle linee guida dello standard NIST-SP800.**
Il NIST, infatti, ha definito un framework di controlli di sicurezza equivalente a quanto definito da ISO27001 nella reportistica forniremo l'equivalente contro del CSF
NIST SP-800 è invece uno standard che definisce linee guide sull'implementazione dei vari controlli, per ogni controllo analizzato nel report verrà fornito il riferimento al relativo documento di NIST SP-800 che ne descrive le modalità di implementazione.



Il progetto di seguito descritto oltre ad avere lo scopo di valutare il livello di maturità dell'organizzazione e standardizzare la gestione delle informazioni dal punto di vista della sicurezza delle informazioni può anche essere visto come un primo passo verso il raggiungimento della conformità allo standard ISO27001:2022
Nel proseguo del documento verranno descritte le fasi previste dal progetto, i driver che hanno portato alla quantificazione economica, le tempistiche indicative per il completamento delle attività e gli aspetti economici.
Maggiori dettagli sulle attività previste dal progetto possono essere trovati nel documento con protocollo 230010 già in vostro possesso

Per facilitare l'attività di miglioramento

Fasi dell'attività

La fase iniziale dell'attività consisterà in un "information security audit" che permetterà di:

- Individuare il livello di soddisfazione dei controlli
- Individuazione delle aree di miglioramento
- Definire quali attività intraprendere per levare il livello di sicurezza e le relative priorità
- Definire KPI per monitorare i miglioramenti

L'attività, che sarà svolta parzialmente on-site e parzialmente da remoto, prevede:

- Analisi del contesto
- Identificazione degli stakeholder
- Mappatura dei servizi erogati e dei processi aziendali coinvolti
- Verifica di quali controlli dell'ANNEX A di ISO27001:2022 e del NIST CSF sono soddisfatti dall'organizzazione
- Valutazione delle misure adottate per soddisfare i controlli applicati
- Definizione di un livello di maturità dell'organizzazione e identificazione delle priorità
- Definizione di un piano di miglioramento
- Valutazione, se presenti, dei KPI adottati dall'organizzazione per valutare aspetti ISMS
- Stesura di reportistica executive riportante "as-is", "non conformità", livello di maturità e piano di azione con le attività prioritarie
- Report "technical" riportate per ogni controllo tutte le osservazioni rilevate durante l'audit

Parametri utilizzati per la costruzione dell'offerta

L'offerta sarà costruita basandosi sui parametri discussi nei precedenti incontri, il progetto prevede l'intervista e il coinvolgimento delle seguenti figure

- Risorse umane/HR Manager
- IT Officer
- Information Security Officer
- Responsabili di area con funzioni decisionali in merito alla catena d fornitura
- Procurement/Ufficio acquisti

Vincoli di Riservatezza

Le informazioni contenute nella presente offerta, relative ai e servizi di Invisiblefarm S.r.l e Fragma Security S.r.l., sono da considerarsi strettamente riservate e sono di esclusiva proprietà di Invisiblefarm S.r.l e Fragma Security S.r.l.; tali informazioni devono pertanto essere utilizzate unicamente dal personale dell'azienda cliente autorizzato a valutare la presente offerta.

Ringraziandovi per l'attenzione, vi salutiamo cordialmente.