# Gli AUDIT DI SICUREZZA - Considerazioni nel contesto dei sistemi informativi, informatici e tecnologici

## Gli AUDIT DI SICUREZZA - Considerazioni nel contesto dei sistemi informativi, informatici e tecnologici

### A cosa serve un auditing?

**L'Auditing** è una attività di **valutazione** ed **analisi** che, attraverso **obiettivi** e **procedure**, individua **criticità importanti** all'interno del contesto interessato.
Può essere fondamentalmente interno o esterno ed entrambi hanno il loro valore intrinseco. Relativo a piccole o grandi realtà ed in questo caso cambia per profondità e tempistiche di esecuzione.
Il primo passaggio che lo connatura è la raccolta di dati ed informazioni, attraverso verifiche dirette, acquisizioni di dati, interviste. Segue poi lo studio dei dati per una elaborazione scritta che rappresenta la base per attuare un miglioramento sui sistemi e sui processi analizzati.

### Che valore ha nel contesto aziendale? Anche in relazione ad attività come per esempio il Vulnerability Assessment ed il Penetration Testing?

L'Auditing ha la caratteristica di poter essere applicato **non solo nel contesto prettamente informatico**, ma anche nelle realtà aziendali attigue. Così, mentre un Vulnerability Assessment o un Penetration Testing possono essere applicati al solo

sistema informatico e in modo molto circoscritto, un audit **ha il vantaggio** di estendersi **a tutto il sistema informativo** che a sua volta **comprende** anche il **sistema informatico** e **tecnologico**.
Possiamo dire che un audit può restituire una fotografia ed una visione d'insieme, scalabile, complessa, più o meno approfondita (a seconda delle scelte) e per il tipo di analisi una valutazione relativamente più duratura nel tempo. Infatti, così come alcuni piccoli cambiamenti possono completamente capovolgere il risultato e i livelli di sicurezza di un VA o di un PT, nell'audit, essendo molto complesso, la valutazione sommaria può non discostarsi molto dall'analisi iniziale, questo perché un audit serve ad individuare criticità e definire linee guida, mentre un VA o un PT individuano generalmente solo i punti deboli da correggere.
Possiamo anche dire che un VA o un PT, possono rappresentare verifiche di sicurezza specifici all'interno di un contesto più ampio che investe tutto il processo di sicurezza del trattamento di dati ed informazioni e che possono rientrare nelle analisi di un audit.
Un audit quindi è e deve essere sempre il punto di partenza delle verifiche di sicurezza ed eseguito in modalità ciclica. Non sempre oltretutto è possibile utilizzare analisi molto invasive e rischiose come in un Penetration Testing.

## L'illusione degli standard

Molti auditor utilizzano schemi standard relativi a norme ISO o simili, ma se poniamo l'aspetto sul fatto che la sicurezza è un processo, ci rendiamo subito conto che spesso questi schemi possono rappresentare un aiuto alla valutazione che non di rado tralasciano però punti altrettanto importanti.
Il buonsenso e l'esperienza acquisita da un auditor nel tempo, rappresentano spesso valori salienti capaci di fare la differenza a livello pratico.
Un processo relativo alla sicurezza si deve adattare alla realtà specifica e deve tenere conto di più variabili possibili. Gli standard sono utilissimi ma rappresentano solo uno dei tanti punti di partenza. Chi crede di aver raggiunto un buon livello di sicurezza semplicemente perché ha conseguito una certificazione relativa ad un ISO 27001 piuttosto che un NIST, non ha capito molto dei problemi di sicurezza intrinseci…
Un Hacker per esempio non ragiona in modalità standard, è abituato a raggirare i problemi e ad utilizzare molto anche l'aspetto creativo. Guardare quindi le analisi da un'ottica Hacker incluso l'aspetto del Social Engineering aggiunge una ricchezza di analisi importantissima.

## La sicurezza non è mai al 100%

Sì, è vero, però c'è una grande differenza tra chi certifica l'impossibile è ha poi una sicurezza apparente, da chi magari non certifica quasi nulla ma all'atto pratico ha saputo attuare le giuste scelte.

Un audit non è solo un'occasione di verifica ma anche di apprendimento sull'attuazione delle valutazioni e dei metodi da seguire in relazione alla propria realtà.
Se la sicurezza è un processo, la ricerca della sicurezza è parte del processo ed è un esercizio costante da ripetere nel tempo, che mira a mitigare nel miglior modo possibile tutto ciò che potenzialmente può accadere, con la coscienza che l'errore o l'imprevisto sono sempre dietro l'angolo e che ci sono sempre aspetti nuovi da scandagliare. Ma, con la coscienza che per contrastare i pericoli ci vuole altrettanta energia espressa ben spesa e perdurata nel tempo.

## Il nostro metodo

La coscienza del fatto che la perfezione non esiste e che gli schemi possono essere a volte una trappola, ci spinge a ricercare ogni giorno il miglior equilibrio. Le nostre valutazioni tengono conto sì degli standard del settore, ma valutano in continuazione tutti quegli aspetti tangenziali che spesso vengono persi di vista. Per noi la differenza è sempre nel particolare.
Un nostro modulo di auditing non compilato consta in non meno di 200 pagine di analisi da porre su tutto il contesto del sistema informativo, informatico e tecnologico. A fine analisi il modulo può raggiungere anche migliaia di pagine, a seconda della grandezza di quanto analizzato, degli allegati e della profondità di analisi richiesta.
Utilizziamo audit proprietari, protetti da diritti, che vengono revisionati costantemente (quasi ogni settimana) e che sono frutto di esperienza e ricerca continua.
Se la sicurezza non è reale non serve a nulla, ecco che le best practice unite agli errori, comuni o particolari che rileviamo continuamente sul campo, diventano ogni volta spunti da inglobare nelle revisioni documentali dell'auditing.
In questo modo, le nostre stesse analisi, diventano un processo continuo di sicurezza.
Non solo teniamo conto di questi fattori ma partendo dal fatto che come per esempio l'Hacking è prima di tutto un atto creativo, a prescindere da come lo si utilizzi, non possiamo esimerci dal ricercare la sicurezza nei processi mettendoci sempre prima nei panni di chi attacca per simulare quello stesso pensiero creativo ed utilizzarlo nell'atteggiamento di difesa.
Ciò non ci rende perfetti, ma ci restituisce uno schema simulato di pensiero, dinamico, originale, atto a prevenire con più realismo le problematiche all'interno delle realtà che analizziamo.
All'interno delle nostre analisi sono comprese le problematiche tradizionali come quelle relative a problematiche più particolari, come per esempio la difesa da tecnologie TEMPEST e dalle tecniche di spionaggio in genere.
Un'attenzione particolare è posta su tutti quegli aspetti che non riguardano le architetture di difesa, in quanto l'anello più debole è sempre il fattore umano, insieme alle scelte ed azioni che produce.

Policy, procedure, processi e soluzioni adottate su tutto il sistema informativo sono scandagliate in modo minuzioso, per evidenziare tutto ciò che spesso sfugge e che può esporre a punti deboli importanti non valutabili con altre attività.

## Per concludere

La nostra attività di auditing non vi garantirà mai una sicurezza al 100%, che di fatto non esiste, ma vi garantirà un approccio valido che giustifica una spesa economica ed un corretto approccio per rendere il concetto di sicurezza una realtà e non un qualcosa di teorico.
Rivolgetevi a noi solo se volete qualcosa di vero e se volete spendere correttamente i vostri soldi…
Ricordiamo inoltre che in parallelo ai servizi si audit di sicurezza, offriamo tutta una serie di servizi come per esempio le bonifiche ambientali da microspie.

Sul nostro sito **www.tttesla.it** potrete visualizzare tutti i servizi utili offerti e reperire maggiori informazioni e documentazione.

**TTTesla**
**Mob +39 3280542204**
**info@tttesla.it - www.tttesla.it**
Siamo presenti anche su **Linkedin** e **Facebook**

Sede legale: Via G. B. Viotti, 6 - 10098 Rivoli (TO)
P IVA 12513990015 - CF GZZNDR74M12H355V