TISAX: la sicurezza delle informazioni nell’automotive

La normativa IATF 16949 prevede alcuni requisiti che riguardano la sicurezza delle informazioni dell’organizzazione automotive ed infatti le *Sanctioned Interpretation* riguardano anche la sicurezza delle informazioni gestite. Ricordiamo che una **Sanctioned Interpretation** modifica l’interpretazione di una regola o di un requisito della IATF 16949 e diventa essa stessa la base di una non conformità.

In particolare, alcune di esse riguardano ai punti seguenti:

6.1.2.3 PIANI DI EMERGENZA

L’organizzazione deve:

a) – b) (…)

c) preparare piani di emergenza per la continuità della fornitura in caso si verifichino: guasti di apparecchiature chiave (vedere anche sezione 8.5.6.1.1), interruzione dei prodotti, processi e servizi di fornitura esterna, disastri naturali, incendi, interruzione di servizi, attacco informatico ai sistemi informativi, mancanza di manodopera o problemi alle infrastrutture.

> S.I.: “Le organizzazioni devono affrontare la possibilità di un attacco informatico che potrebbe interrompere le proprie attività produttive e logistiche, inclusi i ransomware. Le organizzazioni devono assicurarsi di essere preparate in caso di attacco informatico.”

7.1.3.1 PIANIFICAZIONE DELLO STABILIMENTO, DEI MEZZI E DELLE APPARECCHIATURE

…l’organizzazione deve… implementare la protezione informatica delle apparecchiature e dei sistemi di supporto della produzione

> S.I.: “La sicurezza informatica non si limita alle funzioni di supporto e alle aree degli uffici che utilizzano i computer. Anche la produzione utilizza controlli e attrezzature computerizzati potenzialmente a rischio in caso di attacchi informatici. L’aggiunta di questo requisito guida verso l’implementazione delle protezioni necessarie per garantire il continuo funzionamento e l’ininterrotta produzione, al fine di soddisfare le esigenze dei clienti”

Le suddette prescrizioni restano generiche e non entrano molto nel merito di una disciplina molto articolata e complessa come quella della sicurezza delle informazioni in generale e della sicurezza informatica in particolare.

Per questa ragione è uscito lo standard **TISAX®** (*Trusted Information Security Assessment eXchange*), che rappresenta uno schema a fronte del quale le aziende automotive più importanti (OEM, Tier 1) richiedono l’*assessment* ai loro fornitori in quanto essi trattano informazioni critiche dal punto di vista della **Riservatezza**, dell’**Integrità** e della **Disponibilità** delle stesse.

È facile immaginare che alcune informazioni scambiate nella catena di fornitura automotive, richiedono una certa protezione. Si tratta di: **dati di prodotti e di componenti** (specifiche tecniche, documenti progettuali e disegni dimensionali, dati di validazione file PPAP/APQP, dati di collaudo e omologazione), **dati aziendali fondamentali per il business** (schede processi, programmi di produzione, software di produzione e manutenzione, informazioni personali, strategie aziendali, dati di marketing e di vendita), **dati collegati ai rapporti tra fornitori e clienti del settore** (offerte, contratti, ordini di componenti, fatture, piani di consegne, dati e informazioni su clienti e fornitori), **dati su veicoli** (anomalie, guasti, richieste di assistenza, …).

TISAX è un meccanismo di valutazione e di scambio dei risultati di un assessment fra le organizzazioni della catena di fornitura automotive, nato per iniziativa del **VDA** tedesco – attualmente responsabile dello schema – e che si sta affermando come una declinazione degli standard di sicurezza delle informazioni (ISO 27001 su tutti, ma anche SPICE ISO 15504 per il software automotive) nel settore automotive.

Il sistema TISAX si basa su:

1. Una registrazione dell’azienda al TISAX®
2. La scelta di un organismo (*audit provider*) che effettua audit secondo questo schema
3. L’esecuzione dell’assessment da parte dell’organismo indipendente
4. La condivisione dei risultati dell’assessment con i partecipanti al TISAX e l’accesso ai dati degli altri partecipanti.

I partecipanti registrati al TISAX possono anche essere OEM che si ritengono partecipanti “passivi” in quanto non effettuano un assessment, ma invitano i loro

fornitori a farlo per poi accedere ai risultati dell'assessment stesso.

L'intero meccanismo è monitorato dall'**ENX**, associazione no profit che svolge un ruolo simile ad un Ente di Accreditamento.

L'audit o assessment TISAX porta ad ottenere una "**Label**" mediante un processo che è del tutto simile a quello delle certificazioni dei sistemi di gestione.

L'assessment TISAX ha uno scopo, un ambito di applicazione per il quale viene valutato dall'audit provider (esiste lo scopo di tipo *Standard*, *Narrow* ed *Extended*). L'ambito di applicazione di una valutazione TISAX, però, non può essere determinato dall'organizzazione, ma deve necessariamente comprendere tutti i processi e le risorse coinvolte nel trattamento di informazioni afferenti all'industria automobilistica.

Dallo scopo derivano gli obiettivi dell'assessment che permettono di ottenere una "Label" di un determinato tipo (Livello di Maturità da 0 = *Incomplete* a 5 = *Optimizing*).

La documentazione (tutta in lingiua inglese o tedesca) resa disponibile per questo schema è ampia e comprende un **TISAX Handbook** dettagliato, un TISAX *Simplified Group Assessment* e soprattutto una check-list per l'autovalutazione. Tutti i documenti aggiornati sono reperibile al link https://portal.enx.com/en-US/TISAX/downloads/.

Anche l'audit non è di un unico tipo: esiste l'audit di livello 1 (AL 1) che essenzialmente è una autovalutazione dell'organizzazione, quello di livello 2 (AL 2) che consiste in una verifica di quanto indicato dall'azienda nel questionario di valutazione, condotta prevalentemente da remoto, infine l'audit di livello 3 (AL 3) è più completo ed approfondito, dunque più severo per l'organizzazione.

Probabilmente molte organizzazioni a cui è stato richiesto dai loro clienti un assessment TISAX non sanno rispondere alle domande della check-list di autovalutazione, oppure risponderebbero in modo errato senza una consulenza competente in grado di guidarli verso l'audit/assessment TISAX senza rischiare di fare un buco nell'acqua.

Photo by Pixabay on Pexels.com

La check-list per l'assessment TISAX propone, per ciascun punto di controllo, uno o più obiettivi di controllo ai quali sono associati requisiti obbligatori (*must*), requisiti auspicabili (*should*), requisiti aggiuntivi necessari laddove è richiesto un elevato livello di protezione delle informazioni e, tra le altre informazioni, il riferimento al requisito ISO 27001 dell'appendice A (equivalente al controllo ISO 27002) corrispondente.

I controlli sono suddivisi in tre aree: *Information security*, *Prototype protection* e *Data protection*.

I risultati degli obiettivi di controllo sono poi riepilogati nella scheda dei risultati (*Result*) che produrrà la valutazione complessiva e genererà un grafico Radar complessivo per evidenziare i livelli di maturità per i diversi punti di controllo, oltre a grafici radar per singola area.

Sono infine riportati alcuni esempi, anche di KPI significativi per monitorare l'adeguatezza della gestione della sicurezza delle informazioni in ambito automotive.

La copertura dei controlli ISO 27001 Appendice A – ISO 27002 è solo parziale, ma l'obiettivo è far raggiungere anche ad aziende medio-piccole che operano nel settore automotive un livello di maturità accettabile sulla sicurezza delle informazioni, senza pretendere di ottenere l'ardua ed onerosa certificazione ISO 27001.

Tuttavia, un'azienda del settore manifatturiero che opera in questo settore spesso non ha risorse IT interne adeguate per gestire un progetto di adeguamento al TISAX e l'infrastruttura tecnologica implementata potrebbe non fornire adeguate garanzie dal punto di vista della sicurezza.

Occorre dunque effettuare una sorta di *gap analysis* per capire qual è lo stato attuale dell'organizzazione rispetto alla sicurezza delle informazioni, per capire quali azioni occorre mettere in campo per poter raggiungere il livello di maturità richiesto e la conseguente Label TISAX. Credo che alcune organizzazioni, però, si attiveranno subito con l'iscrizione al TISAX per avviare il processo, senza sapere cosa li aspetta.

I costi per l'ottenimento di una determinata Label TISAX variano in funzione del numero dei siti e degli scopi, ma sono comunque ripartiti nei seguenti:

- Costo di registrazione al TISAX (a partire da € 405)
- Costi per l'audit da parte di un Audit Provider (dipendono dal livello di audit e sono ricorrenti per rinnovare la Label ogni 3 anni, ma non sono previsti audit di sorveglianza)
- Costi per l'eventuale consulenza finalizzata al raggiungimento del livello di maturità richiesto
- Costi del personale interno per seguire il progetto (personale IT, qualità,

direzione, risorse umane, …)

- Speseper adeguamento di hardware e software
- Costi per eventuale assistenza sistemistica esterna.