GRUPPO 2G

NEWS

COMPLIANCE, TECHNICAL & ORGANISATIONAL CONSULTING

022/2021

SICUREZZA INFORMATICA IN AMBITO INDUSTRIALE

SICUREZZA INFORMATICA IN AMBITO INDUSTRIALE

Il Piano Industria 4.0 ha impresso negli ultimi anni un'accelerazione alla trasformazione digitale delle aziende, portando le macchine a essere sempre più interconnesse con sistemi informativi interni ed esterni.

La legge infatti concede la possibilità di godere di incentivi fiscali per determinate categorie di beni solo prevedendone l'interconnessione e l'integrazione logistica all'interno dell'azienda, la possibilità di integrazione con la rete di fornitura e l'obbligo di sistemi di tele-manutenzione o telediagnosi oppure di sistemi di controllo in remoto.

Ciò implica che attraverso la macchina interconnessa sia possibile accedere al know-how aziendale in termini di prodotto (ad esempio disegni) e di processo (ad esempio fasi di lavorazione, tempi ciclo, costi di trasformazione).

In altre parole, **con l'interconnessione l'azienda è stata "costretta" ad assumersi nuovi rischi, spesso in modo inconsapevole, senza valutarne adeguatamente l'impatto e le potenziali conseguenze e senza adottare appropriate contro-misure**.

Tali potenziali rischi possono riguardare il blocco degli impianti ***(ad esempio per sabotaggio o per richiesta di riscatto), azioni di danneggiamento o terroristiche, furto di informazioni e di know-how***.

È ad esempio sufficiente concedere l'accesso da remoto a un fornitore del quale non sia stata preventivamente verificata la sicurezza informatica per consentire ad un hacker di entrare nei sistemi attraverso la rete del fornitore stesso.

Il cosiddetto **DATA BREECH (violazione dei dati)** è una **breccia che si apre nel sistema di gestione dei dati aziendali e che implica diverse conseguenze: dalla distruzione di informazioni alla loro divulgazione non autorizzata fino all'accesso a dati personali**.

Secondo il recente report annuale di Ponemon Institute e IBM Securitysul tema dei *data breech*, **le imprese nel mondo pagano mediamente 4.24 milioni di dollari per ogni evento di violazione, circa +10% rispetto a un anno prima**. Si tratta di valori medi all'interno dei quali c'è molta varietà in funzione dei settori nei quali si opera: si va dai 9.23 milioni di US$ nell'assistenza sanitaria ai 5.72 milioni nella finanza e ai 5 milioni nell'industria farmaceutica.

COMPETENZA E ORGANIZZAZIONE

Il tema della sicurezza informatica non ha solo implicazioni tecnologiche: la questione è molto più ampia e riguarda competenze, comportamenti e strumenti organizzativi.

La mancanza di consapevolezza è il primo fattore di rischio. Molte aziende, infatti, non hanno ancora prestato attenzione a esaminare il nuovo contesto, la possibilità e l'impatto di eventi sfavorevoli. **La tecnologia può contrastare l'attacco effettuato dall'esterno verso la rete aziendale, ma può ben poco contro il furto di informazioni operato da chi – a vario titolo – può essere autorizzato ad accedere alle informazioni presenti sulle macchine e sugli impianti.**

Accanto alle tematiche relative alla protezione dei dati che afferiscono alla parte gestionale e commerciale (cui in media le aziende sembrano avere una crescente seppure non ancora sufficiente sensibilità), **la consapevolezza delle implicazioni di sicurezza connesse alla digitalizzazione della produzione e della logistica è nella maggior parte dei casi ancora molto scarsa**.

Si pensi ad esempio ai contratti di manutenzione siglati con aziende fornitrici: essi raramente prevedono che le **modalità di intervento da remoto prendano in esame e regolino le responsabilità dell'azienda incaricata per quanto concerne l'accesso e il trattamento dei dati attraverso la macchina o l'impianto.**

Spesso l'argomento non è nemmeno contemplato tra le clausole di servizio e quindi non è nemmeno regolata la proprietà dei dati di funzionamento.

La vulnerabilità del sistema è spesso legata anche a questioni di obsolescenza. Tipicamente la vita utile di una macchina operatrice è di gran lunga superiore a quella dei sistemi informativi che ne regolano il funzionamento e ai sistemi gestionali in continua evoluzione. A ciò si aggiunge il tema della sicurezza della sensoristica **IoT (*Internet of Things*)** installata per l'acquisizione dei dati di processo: molte volte, al fine di minimizzare i costi d'investimento delle aziende, sono stati proposti sensori di dubbia qualità, facili da "bucare" dall'esterno anche da hacker poco esperti.

Anche il boom dello *smart working* ha contribuito alla crescita dei casi di *data breech*, con costi e tempi medi di individuazione e contenimento della "falla" superiori alla media mondiale rispettivamente di 1 milione di US$ e di 58 giorni. Si comprende allora come un'attenta regolamentazione dello *smart working* sia di fondamentale importanza alla *business continuity* aziendale.

Ulteriore necessità, infine, è quella di riprogettare i sistemi di archiviazione e conservazione dei dati. Bisogna valutare se le informazioni raccolte dagli strumenti digitali siano adeguatamente conservate e amministrate, oltre che salvaguardate dall'obsolescenza dei sistemi di lettura e archiviazione e protette contro errori umani e attacchi esterni.

NUOVO REGOLAMENTO MACCHINE

È proprio per tenere in considerazione dei forti cambiamenti degli ultimi anni delle macchine e degli impianti interconnessi e delle relative implicazioni in termini di sicurezza che la Commissione Europea ha programmato di rivedere e aggiornare la Direttiva Macchine 2006/42/EC.

Nel **febbraio 2020** la Commissione ha pubblicato il **report sulle implicazioni di sicurezza e di affidabilità dell'intelligenza artificiale, dell'IoT e della robotica**, evidenziando numerosi gap normativi ad esempio in termini di:

- ***Nuovi rischi originati dalle nuove tecnologie;***
- ***Incertezza normativa e probabili lacune di sicurezza nelle tecnologie tradizionali;***
- ***Lacune normative per macchinari ad alto rischio;***
- ***Contraddizioni con la normativa di sicurezza dell'Unione.***

Tenendo conto di tali *gap*, il **21 aprile 2021** la Commissione ha pubblicato la **proposta di revisione della Direttiva Macchine in un nuovo Regolamento**, immediatamente applicabile in tutti gli Stati membri una volta terminato l'iter di approvazione senza necessità di recepimento da parte dei singoli Stati.

Tra le novità più importanti c'è l'introduzione delle **figure dell'IMPORTATORE *(che avrà responsabilità di assicurarsi che il fabbricante abbia effettuato l'appropriata verifica della conformità del prodotto***) e del **DISTRIBUTORE *(cui spetta la responsabilità di verificare che il prodotto sia correttamente identificato e accompagnato dalla documentazione necessaria).***

Il nuovo Regolamento allarga la definizione di **componente di sicurezza anche ai componenti digitali, compresi i software che svolgono funzioni di sicurezza: in altre parole, esso si applicherà anche a beni immateriali.**

Il Regolamento inoltre affronta il **tema dell'intelligenza artificiale delle macchine,** preoccupandosi che l'integrazione con i sistemi sia progettata in modo sicuro. Nella fase di apprendimento dell'intelligenza artificiale, ad esempio, il comportamento della macchina deve avere delle limitazioni, mediante adeguati circuiti di sicurezza. Esso stabilisce infine anche i requisiti di sicurezza da seguire nell'interconnessione Industria 4.0 delle macchine alle reti di dati.

LA PROPOSTA DI GRUPPO 2G

Gruppo 2G ha un **team di ingegneri** in grado di supportare l'azienda cliente nell'analisi della situazione attuale del proprio sistema di gestione delle informazioni e del *know-how* e nella individuazione dei rischi connessi.
Di seguito alcuni esempi di attività di cui Gruppo 2G si occupa in questo ambito:

- **Analisi e gestione dei rischi e della sicurezza** dei sistemi informativi e informatici dell'azienda secondo standard e *best practice* riconosciute a livello internazionale;

- **Analisi dell'infrastruttura informatica in termini di vetustà tecnologica e rischio di sicurezza** e predisposizione di un piano di ammodernamento attraverso i partner tecnologici;
- **Realizzazione di *Vulnerability Assesment***, condotto periodicamente e principalmente in modo automatico al fine di identificare le eventuali vulnerabilità di sistema e definire le azioni di miglioramento;

- **Realizzazione di *Penetration Test***, processo nel quale in manuale si prova ad identificare le vulnerabilità esistenti nel sistema;
- **Intrusion Detection** ed **Ethical Hacking**, al fine di avere un quadro completo del livello di sicurezza informatica;
- **Studio dell'identità digitale** dell'azienda cliente per comprenderne il grado di esposizione e di rischio**;**
- **Valutazione dei rischi in ottica BYOD (*Bring Your Own Device*),** cioè in riferimento ad attività di trasmissione dei dati verso l'azienda svolte da dipendenti / consulenti tramite dispositivi elettronici in concessione d'uso o di proprietà o mediante piattaforme social o di messaggistica;
- **Progetto della soluzione di Disaster Recovery** al fine di ottimizzare le misure tecnologiche e i processi organizzativi volti a ripristinare sistemi, dati e infrastrutture nel caso di gravi emergenze;
- **Realizzazione di un SOC (*Security Operations Center*)** che possa garantire il controllo *on-line* e in modo continuativo dello stato dell'arte e di eventuali tentativi di attacco, allertando immediatamente il personale coinvolto e mettendo in atto le azioni di contenimento o correttive**;**
- **Supporto alla creazione e al mantenimento di un sistema di gestione delle informazioni conforme alle norme ISO 27001** (gestione della sicurezza delle informazioni), **ISO 27018** (privacy dei dati in cloud), **ISO 31000** (tecniche di analisi dei rischi) e **ISO 22301** (continuità operativa);
- **Consulenza nella predisposizione di un progetto di trasformazione digitale dell'azienda in ottica Industria 4.0**, con analisi preliminare della **Mappa del Valore** e individuazione delle tecnologie digitali più adeguate al miglioramento dei processi;
- **Supporto alla creazione e al mantenimento di un sistema di gestione dell'infrastruttura informatica che sia conforme allo standard IEC 62443-3-3;**
- **Formazione del personale** alle tecniche digitali e di sicurezza informatica. Tra i corsi proposti si citano:

- *La trasformazione digitale nel settore manifatturiero*
- *Industrial Internet of Things*
- *Cloud Computing*
- *Big Data & Analitics*
- *Blockchain & Smart Contracts*
- *Sicurezza Informatica*
- *Il sistema di gestione delle informazioni (in ottica ISO 27001)*

Ing. Giuseppe PANACCIONE
- **Componente del C.d.A. di Gruppo 2G con delega per le NUOVE INIZIATIVE.**
- Esperto di **lean manufacturing** e **riorganizzazione dei flussi produttivi**.
- Esperto di **turnaround e di rilancio di aziende** in crisi e nell'ottimizzazione delle giacenze e dei sistemi automatici di programmazione della produzione

Sig.ra Cristina GAGLIARDO
Per avere maggiori informazioni
sui nostri servizi potete contattare
Il ns. Ufficio Sales & Back Office
che fisserà un appuntamento
con uno dei ns. Esperti
Tel. 011/5620022
c.gagliardo@gruppo2g.com
gruppo2g@gruppo2g.com