Guida al fattore di rischio in ambito Aereonautico

Nel settore aeronautico, la protezione dei dati personali, delle informazioni tecniche sensibili e della proprietà intellettuale è fondamentale per garantire sicurezza, conformità normativa e competitività sul mercato.
Data la complessità delle infrastrutture informatiche, oltre che dei sistemi e la rilevanza delle attività svolte, è opportuno adottare un approccio chiaro e esemplificativo nella valutazione del rischio legato alla privacy e sicurezza aziendale. Questo elaborato è una proposta metodologica per calcolare il fattore di rischio al contesto operativo specifico, tenendo in considerazione le fasi operative, gli asset strategici e le normative di riferimento.

Normative e standard applicabili

- **Regolamento UE 2016/679 (GDPR)**: riferimento agli obblighi per la protezione dei dati personali dei dipendenti, dei clienti e dei fornitori.
- **EASA Cybersecurity Framework**: linee guida per la sicurezza informatica e protezione dei dati nel settore aeronautico.
- **LSMS & ISO/IEC 27001**: standard interno aziendale e internazionale per la gestione della sicurezza delle informazioni.
- **D.lgs. 81/2008** riferimento legislativo relativo alla sicurezza fisica e organizzativa dei lavoratori.
- **Standard interni di sicurezza e politiche aziendali** configurate seguendo le linee guida dell'Agenzia europea per la sicurezza aerea (EASA) e degli enti nazionali di certificazione.

Contesto operativo e rischi tipici in un’azienda aeronautica

In un’azienda operante nel settore, gli scenari di rischio sulla privacy e sulla sicurezza includono:

- Accesso non autorizzato a dati tecnici relativi a progetti aeronautici (disegni aereonautici e meccanici 3D e 2D su CAD e Katja e relative specifiche su componenti e fasi lavorative).
- Furto o perdita di dati riservati dei clienti, dati personali dei dipendenti, progetti e brevetti aereonautici.
- Attacchi informatici su sistemi di ricerca e sviluppo, ingegneria di produzione, cicli residenti, manutenzione, gestione magazzino o documenti relativi al controllo qualità.
- Interruzioni o rallentamenti operativi causati da malware o ransomware, in grado di bloccare processi critici produttivi, controllo qualità e la consulta di specifiche tecniche interne o del committente.
- Violazioni dei protocolli di sicurezza negli accessi a sistemi aventi dati sensibili.

Guida al calcolo del fattore di rischio

Formula generale:

R = P × I

- **R** = fattore di rischio
- **P** = probabilità che si verifichi una violazione o incidente di sicurezza/privacy
- **I** = impatto o gravità con annesse conseguenze aziendali

Valutazione della probabilità (P) in ambito aeronautico

La probabilità deve essere calcolata tenendo in considerazione:

- L'infrastruttura informatica aziendale composta da una rete LAN interna connessa ad una rete centrale gestita in un altro sito, tramite la quale le postazioni operative e tecniche comprese le macchine CNC , accedono in tempo reale a software, tool e part program indispensabili per le attività quotidiane.
- Il livello di protezione è garantito da soluzioni hardware e software, come antivirus e firewall industriali implementati da diramazioni di reti wireless e cablate con rack e antenne point to point, accedibili con autenticazione apposita tramite userid e password conformi ai criteri di complessità (lunghezza minima, uso di caratteri speciali, maiuscole/minuscole e cifre).
- Frequenza di aggiornamento e patch di sicurezza dei sistemi operativi, antivirus e software di disegni meccanici e specifiche aereonautiche nelle rispettive postazioni di lavoro.
- Sulla base storica di esperienze interne (Pomigliano D'Arco 2017 Leonardo AereostruttureS.P.A.) è possibile aumentare il livello di sicurezza e ridurre il rischio di data breach.

Valutazione delle probabilità (P):

Nella tabella è possibile determinare il numero dei livelli di probabilità legato alla temporalità del verificarsi dell'evento:

	Raro	Improbabile	Probabile	Quasi Certo
Livello	**1**	**2**	**3**	**4**
Periodicità	**10 Anni**	**5 Anni**	**1 Mese**	**1 Settimana**

Valutazione dell'Impatto (I) specifico

L'impatto viene valutato considerando le possibili conseguenze derivanti da:

- **Perdita o manipolazione dei dati tecnici**, con ripercussioni sulla qualità e sicurezza dei prodotti, oltre alla perdita di fiducia del cliente finale e compromissione dell'immagine etica aziendale.
- **Mancata conformità a GDPR**, con sanzioni elevate e danni etici a carattere internazionale.
- **Interruzione della produzione**, con ritardi sulle linee produttive e non conformità su certificazioni ENAC (Ente Nazionale per l'Aviazione Civile), EASA (European Union Aviation Safety Agency), FAA (Federal Aviation Administration) e ambito militare……. con annessi ritardi di consegne ai clienti.
- **Violazione delle misure di sicurezza hardware o software** con impatti sulla continuità operativa dei siti produttivi e ingegneristici, sull'integrità delle infrastrutture e sulla protezione dei dati sensibili.

Tabella riassuntiva dell'Impatto specifico:

Indice	Impatto	Descrizione
1	Basso	Dati non critici e danni limitati
2	Medio	Dati tecnici parzialmente compromessi con leggeri ritardi operativi
3	Alto	Dati essenziali alterati o distrutti con ritardi produttivi e di consegna significativi e sanzioni da parte del Garante per la protezione dei dati
4	Critico	Perdita di dati sensibili con annesse conseguenze legali e danni etici e reputazionali gravi

Esempio di calcolo del rischio in azienda aeronautica (Ipotizzato)

Con l'intersezione delle tabelle sopra indicate è possibile ottenere la matrice del rischio e ipotizzare il calcolo attraverso la relativa formula:

Matrice Calcolo Rischio				
Probabilità / Impatto	RARO 1	IMPROBABILE 2	PROBABILE 3	QUASI CERTO 4
ALTO 4	4	8	12	16

MEDIO ALTO 3	3	6	9	12
MEDIO BASSO 2	2	4	6	8
BASSO 1	1	2	3	4

Possibile scenario: rischio di accesso non autorizzato a documenti tecnici protetti.

- Probabilità stimata: Media (P = 2, Ipotizzato con un livello medio di sicurezza e uno storico di casi isolati)
- Impatto stimato: Alto (I = 4, Conseguente perdita o diffusione di dati sensibili che potrebbero compromettere la sicurezza e la segretezza del prodotto)

Calcolo:

R = 2 × 4 = 8 (R = P x I)

Anche se Leonardo adotta standard personalizzati con l'utilizzo di LSMS (Leonardi Security Management System) si è ritenuto opportuno calcolare in maniera empirica e ipotetica il rischio significativo, che richiede interventi di rafforzamento sull'accesso ad aree riservate con autenticazione biometrica, che andrebbero sostituiti ai metodi tradizionali con inserimento di username e password considerati robusti.
Si richiedono, inoltre, audit sul controllo attuale delle forme di sicurezza adottate con annessa formazione e sensibilizzazione del personale a nuovi strumenti da impiegare o migliorie da adottare.

Best practice consigliate in azienda aeronautica

- Miglioramento continuo del LSMS (Leonardo Security Management System) per garantire efficacia e conformità agli standard di sicurezza aeronautica, per affrontare nuove minacce e vulnerabilità per rispondere adeguatamente ai requisiti normativi e ai possibili attacchi di Cyber Security.

- Formazione continua e specializzata, con corsi incentrati sulle procedure e le politiche di LSMS, per offrire maggiore consapevolezza in ambito di sicurezza informatica e regolamentazione privacy nel settore aereonautico all'intera popolazione aziendale.

- Controllo rigoroso degli accessi fisici ai sistemi, con autenticazione biometrica e limitazione dei privilegi utente ispezionato da un monitoraggio continuo, con adozione di audit interni.
- Definizione di Recovery Plant e Incident Response da adottare nel settore aereonautico, aerospaziale e della difesa, per garantire continuità operativa e sicurezza dei dati trattati ed elaborati, e delle informazioni. Audit regolari e valutazioni di rischio aggiornate, in linea con i riferimenti normativi e tecnologici nel settore aeronautico.
- Collaborazione con enti regolatori e certificatori (EASA, ENAC, FAA)[1]e partecipazione a incontri di settore per aggiornamenti costanti sulle minacce emergenti.

Nel delicato contesto di aziende aeronautiche come Leonardo Aerostrutture SPA, il documento con il calcolo ipotetico del fattore di rischio in materia di privacy e sicurezza aziendale, mette in focus le vulnerabilità specifiche del settore e dei siti facenti parte della One Company, proponendo l'adozione di misure preventive volte a garantire la protezione dai dati grezzi, all'elaborazione di informazioni terminando ai processi critici di lavorazioni e di ingegnerizzazione protetti anche da brevetti industriali. L' approccio è basato su normative e legislazioni con focus su best practice del settore, rappresentando una soluzione efficace al fine di ottenere elevati standard di sicurezza rispettando le specifiche tecniche imposte anche dagli enti certificatori.

1

[1] EASA: European Union Aviation Safety Agency (Agenzia per l'Unione Europea per la sicurezza aerea)
ENAC: Ente Nazionale per l'Aviazione Civile
FAA: Federal Aviation Administration (Amministrazione Federale dell'Aviazione Statunitense)