ZAGLIO ORIZIO
E ASSOCIATI

CYBER-SECURITY AZIENDALE

RISCHI E RIMEDI

AVV. MATTEO PICCINALI

CONFAPI BRESCIA
15 MARZO 2023 – 14:30

ATTACCHI INFORMATICI IN AUMENTO

FATTORI RECENTI

- **Pandemia Globale**
- **Cyberspace è contesto vitale per lo svolgimento di qualsiasi attività umana (educazione, lavoro, socializzazione)**
- **Accelerazione del processo di transizione digitale**

BRESCIA E PRO

Qualità della vita | La sicurezza tra città e provincia

A Brescia tornano a crescere tutti i reati
Il boom dei crimini informatici: è +35%

F. Alberti, E. Montanari, 26 ottobre 2022, Giornale di Brescia

M. Casadei, M. Finizio, Delitti Web, incendi e rapine superano i livelli pre-Covid, 3 ottobre 2022, Il Sole 24 Ore.

Delitti informatici

LE PRIME		OGNI 100.000 ABITANTI	2021
1.	Mantova	174,81	707
2.	Brescia	143,98	1.806
3.	Savona	118,39	317
4.	La Spezia	97,73	210
5.	Cremona	94,51	332

PUNTI DI ATTENZIONE

1) Impatto economico-giuridico dell'attacco informatico in danno all'azienda

2) Quadro normativo in materia di cybersecurity

3) Rimedi che l'azienda ha a disposizione per contrastare il rischio da cybersecurity

1) IMPATTO ECONOMICO-GIURIDICO DELL'ATTACCO INFORMATICO

Dal punto di vista economico, l'impatto sulle aziende che subiscono un attacco informatico è significativo e variegato e può implicare:

- una perdita finanziaria (in via diretta, di somme di danaro, o indiretta, di produzione)

- una perdita di dati personali e di know how aziendale, ossia il patrimonio su cui l'azienda costruisce la propria "ricchezza"

- l'applicazione di sanzioni pecuniarie (ad esempio, violazione della normativa in materia di privacy, D.lgs. 231/01 delitti informatici = reati presupposto)

- un danno reputazionale, con perdita dell'accreditamento della propria azienda quale partner commerciale all'interno della propria filiera industriale

2) Quadro normativo in materia di cybersecurity (cenni)

I legislatori a livello europeo e italiano sono stati finora molto dinamici nell'emanare norme idonee a dotare i Paesi Membri di strumenti giuridici adeguati e aggiornati rispetto alle sofisticate minacce informatiche a livello globale.

Seppure gli strumenti legislativi risultino in prima battuta rivolti ai grandi operatori, questi devono assicurarsi che i loro fornitori siano a loro volta in grado di garantire un buon presidio del rischio da cybersecurity.

Per poter essere operatori accreditati lungo la filiera, è quindi necessario che anche le piccole e medie imprese si attrezzino rapidamente per garantire la sicurezza informatica nella propria operatività quotidiana, nel rispetto delle normative già introdotte e in corso di prossima attuazione.

2) Quadro normativo in materia di cybersecurity (cenni)

L’impostazione di buona parte della normativa sulla sicurezza informatica presenta molte similitudini con il modello imposto dalla normativa GDPR in materia di privacy:

→ Misure di Sicurezza tecniche e organizzative

→ Processo di adeguamento aziendale

→ Verifica e monitoraggio delle terze parti (fornitori, clienti, ecc.)

2) Quadro normativo in materia di cybersecurity (cenni)

 D.lgs. 65/2018 (Direttiva NIS n. 1148/2016 - Direttiva NIS2 n. 2555/2022): le società rientranti nel suo ambito di applicazione sono tenute ad adottare **misure tecniche ed organizzative adeguate e proporzionate** rispetto alla gestione dei rischi cyber.

- **fornitori di servizi digitali e operatori di Servizi Essenziali** (energia; trasporti; sanitario, alimentare, acque, rifiuti, servizi digitali e cloud computing)
- dal 17/10/2024: **sanzioni fino a € 10 Mln o fino al 2%** Fatturato Globale dell'impresa (da €150.000)

 Decreto-legge 82/2021, contenente disposizioni urgenti in materia di cybersicurezza, con cui viene tra le altre cose istituita **l'Agenzia per la cybersicurezza nazionale**

 D. lgs. 123/2022 (Regolamento Cybersicurezza 882/2019): disciplina la **certificazione di cybersicurezza** di prodotti e processi basati sulle nuove tecnologie dell'informazione.

 Regolamento Dora 2554 (27/12/2022): obiettivo di armonizzare a livello europeo i principali requisiti di cybersecurity per le società del **settore finanziario come banche e assicurazioni ma anche per i loro fornitori**, attraverso l'implementazione di misure di governance, gestione del rischio e segnalazione di incidenti.

3) Rimedi per contrastare il rischio da cybersecurity

a) Iniziative di mitigazione del danno (nel caso in cui l'attacco sia già stato subito)

Le iniziative da porre in essere, dal punto di vista legale comprendono in via esemplificativa

→ presentazione di una denuncia penale per truffa, frode informatica, accesso abusivo al sistema informatico,
→ svolgimento di una perizia informatica sui propri sistemi IT per verificare se e come si sia realizzato l'attacco informatico

Si tratta di iniziative volte altresì a dimostrare ai propri partner commerciali di aver operato con diligenza e di non avere alcuna responsabilità in relazione alla violazione posta in essere da terzi.

→ sarà necessario altresì avviare trattative negoziali volte a ripristinare le relazioni con la controparte contrattuale, per salvaguardare il rapporto commerciale e stabilire se e in quale misura ripartire le perdite economiche causate dall'attacco informatico
→ in caso di data breach va inoltre ricordato che l'imprenditore dovrà notificare al Garante per la Privacy la violazione subita entro le 72 ore successive e dimostrare la corretta adozione delle misure di sicurezza organizzative e tecniche onde evitare (o limitare) l'applicazione delle sanzioni.

3) Rimedi per contrastare il rischio da cybersecurity

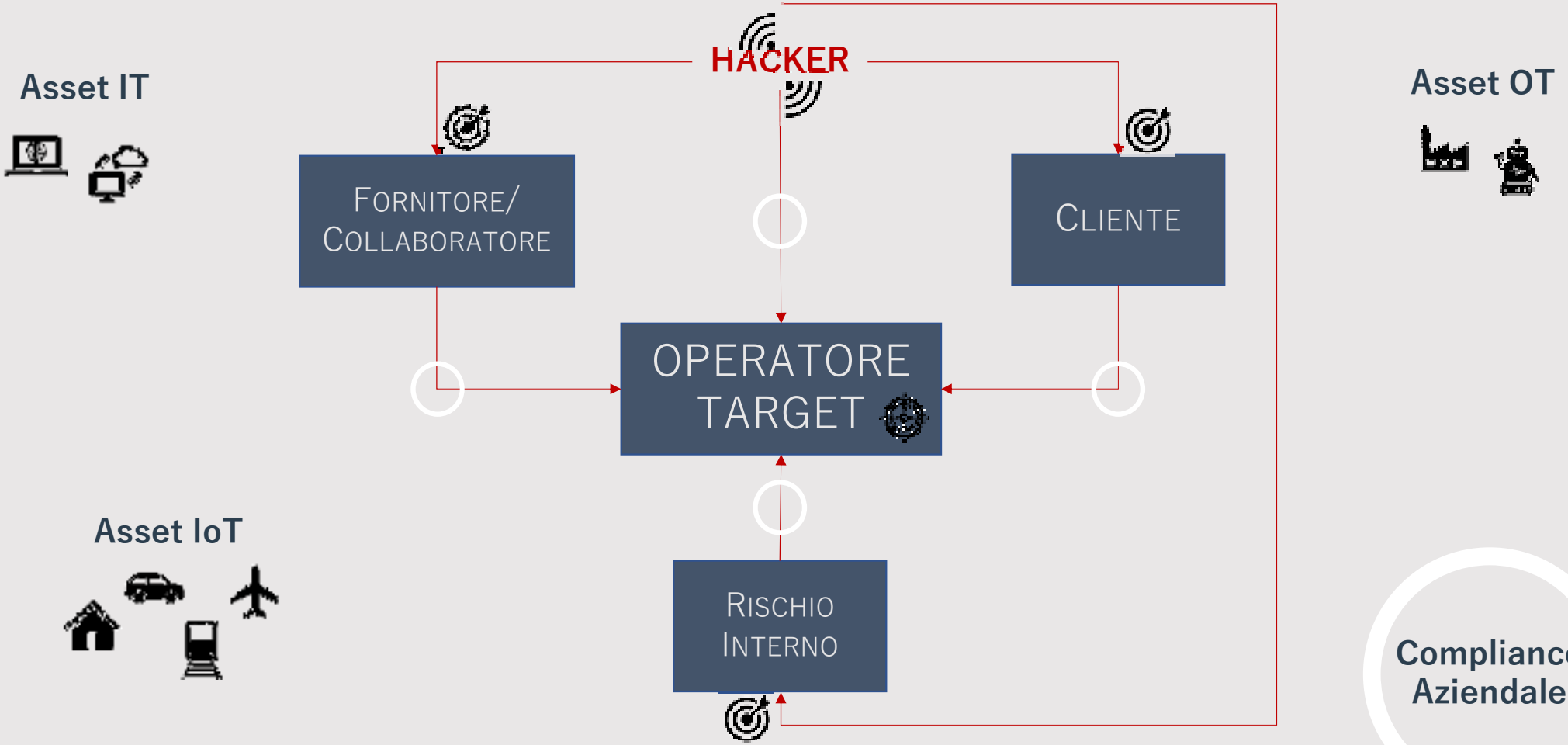
b) misure di sicurezza organizzative, documentali e contrattuali (prevenzione del danno o mitigazione del rischio)

Queste iniziative sono volte a:
→ scongiurare per quanto possibile il rischio di subire un attacco,
→ rendere l'azienda più affidabile per i propri partner commerciali,
→ aumentare la possibilità per l'impresa di negoziare un'adeguata copertura assicurativa del rischio correlato.

Misure Documentali:
 Contratti idonei a disciplinare i rapporti con terzi (fornitori, dipendenti, collaboratori), mediante la stipula ad esempio di accordi di riservatezza e di condizioni generali di contratto verso fornitori e clienti

Misure Organizzative:
 adozione di procedure aziendali che regolamentino il recupero operativo dei propri sistemi informatici,
 adozione di procedure di gestione dei data breach e degli incidenti informatici,
 esecuzione di procedure di audit dei propri fornitori,
 adozione di programmi di formazione e aggiornamento del personale

Dinamiche del Rischio



ZAGLIO ORIZIO
E ASSOCIATI

BRESCIA
Piazza della Loggia, 5
25121

Avv. Matteo Piccinali – m.piccinali@zaglio-orizio.it
Tel. +39.030.2408170 I www.zaglio-orizio.it