REPORT DI ANALISI DEL RISCHIO CYBER
Apex Footwear S.r.l.

Data: 12/0X/202X
Redatto da: Shonel Consulting
Ruolo: Cybersecurity Governance Consultant
Status: Strettamente Confidenziale

Oggetto: Risultati dell'analisi dei rischi informatici e piano di resilienza aziendale.

---

1. Introduzione

A seguito dell'analisi condotta sull'infrastruttura e sui processi della Apex Footwear S.r.l., è emersa una forte dipendenza del business dagli asset digitali (E-commerce e database clienti), a fronte di una postura di sicurezza che presenta alcune vulnerabilità critiche che potrebbero compromettere la continuità operativa e la conformità legale (GDPR).

*Figura 1 - **Identificazione e Classificazione degli Asset Critici***

ID Asset	Nome Asset	Proprietario (Owner)	Descrizione	C	I	A	Valore Criticità
A01	DB Clienti	Marketing	Dati sensibili Shopify	5	5	4	5
A02	Sito E-commerce	CEO	Piattaforma vendita	2	4	5	5
A03	Server NAS	Admin	File contabilità e design	4	5	4	5
A04	Laptop Dipendenti	IT	Dispositivi smart working	3	3	3	3

Il primo passo dell'analisi è consistito nella mappatura degli asset fondamentali per il business di Apex Footwear. Ogni bene (dato, software o hardware) è stato valutato in base alla triade CIA (Riservatezza, Integrità, Disponibilità) per determinarne il livello di criticità. Questo inventario costituisce il perimetro della nostra analisi e identifica i target principali da proteggere.

---

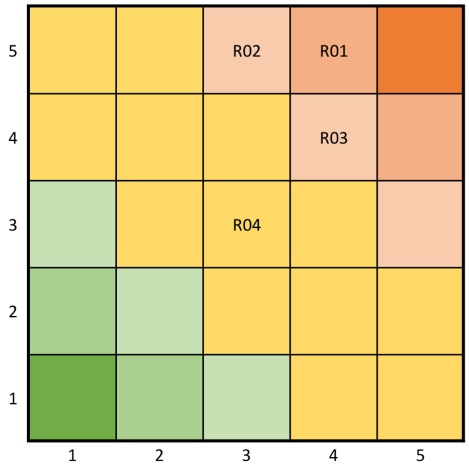
2. Principali Evidenze (Sintesi dei Rischi)

L'analisi ha identificato tre scenari di rischio con impatto "Critico":

- **Indisponibilità dei dati contabili:** Il server NAS in ufficio è vulnerabile ad attacchi Ransomware a causa di software non aggiornato e backup non isolati.
- **Data Breach e Sanzioni:** L'assenza di autenticazione forte (MFA) sugli account Shopify e Google espone l'azienda al furto dei dati di 15.000 clienti, con potenziali sanzioni pecuniarie e danni reputazionali irreparabili.
- **Interruzione delle vendite:** La gestione degli accessi e la scarsa consapevolezza del personale aumentano il rischio di fermo del sito e-commerce per errori umani o phishing.

La distribuzione visiva dei rischi sopra citati è rappresentata nella matrice di rischio qui di seguito.

Figura 2 - Matrice di Rischio (Heatmap)



La Heatmap permette di identificare immediatamente le priorità d'intervento. I codici R01, R02 e R03 situati nella zona rossa rappresentano minacce che richiedono l'applicazione immediata delle misure di mitigazione previste nel piano d'azione.

Figura 3 - Dettaglio Analitico della Valutazione (Risk Register)

ID Rischio	Scenario	Asset Rif.	Probabilità (P)	Impatto (I)	Livello Rischio (R)	Stato
R01	Ransomware su NAS	A03	4	5	20	Critico
R02	Data Breach Shopify	A01	3	5	15	Alto
R03	Phishing su CEO	A04	4	4	16	Alto
R04	Furto Laptop	A04	3	3	9	Medio

Il registro dei rischi fornisce una vista granulare degli scenari analizzati, incrociando le vulnerabilità rilevate sull'infrastruttura di Apex Footwear con le potenziali minacce. I valori di Probabilità e Impatto sono stati assegnati sulla base delle interviste tecniche e della criticità degli asset coinvolti (Triade CIA).

---

3. Piano d'Azione Strategico

Per ridurre l'esposizione al rischio da "Critica" a "Trascurabile", si raccomandano tre interventi prioritari da attuare nei prossimi 30 giorni:

1. **Protezione delle Identità:** Attivazione immediata dell'MFA su tutti gli account critici.
2. **Continuità Operativa:** Implementazione di un sistema di backup immutabile in cloud per garantire il ripristino dei dati in caso di attacco.
3. **Cultura della Sicurezza:** Avvio di un programma di formazione per i dipendenti per neutralizzare le minacce basate su ingegneria sociale.

Figura 4 - ***Strategie di Mitigazione e Rischio Residuo (Risk Treatment Plan)***

ID Rischio	Azione di Mitigazione	Costo Stimato	Priorità	Rischio Residuo (P x I)
R01	Backup Immutabile + Patching	1.200,00 €	Massima	4 (P:1, I:4)
R02	MFA + Training Awareness	500,00 €	Alta	5 (P:1, I:5)
R03	MFA + Email Filtering	300,00 €	Alta	4 (P:1, I:4)
R04	Crittografia Disco (BitLocker)	- €	Media	3 (P:1, I:3)

Il seguente piano d'azione (RTP) delinea le contromisure necessarie per riportare l'esposizione al rischio entro livelli accettabili. Per ogni voce viene indicata la priorità d'intervento e l'obiettivo di 'Rischio Residuo', ovvero il livello di pericolo rimanente una volta che la difesa sarà operativa.

---

4. Valutazione Costi-Benefici (ROI)

L'investimento stimato per la messa in sicurezza (circa **€2.000**) è ampiamente giustificato dalla prevenzione di una perdita potenziale calcolata in oltre **€20.000** (considerando 5 giorni di fermo vendite, costi di ripristino tecnico e sanzioni minime previste dal GDPR).

---

5. Conclusione

Apex Footwear ha l'opportunità di trasformare la cybersecurity da un costo a un vantaggio competitivo, garantendo ai partner logistici e ai clienti finali i più alti standard di protezione dei dati.