Botium Toys: Ambito, obiettivi e rapporto di valutazione del rischio

Ambito e obiettivi dell'audit

Ambito:
L'ambito di questo audit è definito come l'intero programma di sicurezza di **Botium Toys**.
Ciò include i loro **asset** (risorse) come le apparecchiature e i dispositivi dei dipendenti, la **rete interna** e i **sistemi** aziendali.
Sarà necessario esaminare le risorse possedute da Botium Toys e i **controlli** e le **pratiche di conformità** attualmente in uso.

Obiettivi:
Valutare le risorse esistenti e completare la **checklist dei controlli e della conformità**, per determinare quali controlli e buone pratiche di conformità devono essere implementati per migliorare la **postura di sicurezza** di Botium Toys.

Risorse attuali

Le risorse gestite dal **Dipartimento IT** includono:

- Attrezzature **on-premises** per le esigenze operative in ufficio.
- **Apparecchiature dei dipendenti:** dispositivi per l'utente finale (desktop/laptop, smartphone), postazioni di lavoro remote, cuffie, cavi, tastiere, mouse, docking station, telecamere di sorveglianza, ecc.
- **Prodotti del punto vendita** disponibili per la vendita al dettaglio in sede e online, conservati nel magazzino adiacente all'azienda.
- **Gestione di sistemi, software e servizi:** contabilità, telecomunicazioni, database, sicurezza, e-commerce e gestione dell'inventario.
- **Accesso a Internet.**
- **Rete interna.**
- **Conservazione e archiviazione dei dati.**

- **Manutenzione dei sistemi legacy:** sistemi a fine ciclo di vita che richiedono monitoraggio umano.

Valutazione del rischio

Descrizione del rischio:
Attualmente, la gestione delle risorse è **inadeguata**. Inoltre, Botium Toys **non dispone di tutti i controlli appropriati** e potrebbe **non essere pienamente conforme** alle normative e agli standard statunitensi e internazionali.

Buone pratiche di controllo

La prima delle cinque funzioni del **NIST Cybersecurity Framework (CSF)** è **Identify (Identificare)**.
Botium Toys dovrà dedicare risorse per **identificare le proprie risorse** al fine di gestirle adeguatamente.
Dovranno inoltre **classificare le risorse esistenti** e **determinare l'impatto** della loro eventuale perdita (incluse le perdite di sistemi) sulla **continuità operativa**.

Punteggio di rischio

Su una scala da 1 a 10, il **punteggio di rischio è 8**, considerato **piuttosto elevato**.
Ciò è dovuto alla **mancanza di controlli** e alla **non piena aderenza alle migliori pratiche di conformità**.

Commenti aggiuntivi

L'impatto potenziale derivante dalla perdita di una risorsa è valutato come **medio**, poiché il Dipartimento IT **non conosce con precisione** quali risorse sarebbero a rischio.
Il **rischio di perdita di risorse o di sanzioni** da parte degli enti regolatori è **elevato**, perché Botium Toys **non dispone di tutti i controlli necessari** e **non rispetta pienamente** le migliori pratiche di conformità volte a mantenere **dati critici riservati e sicuri**.

Dettagli specifici:

- Attualmente, **tutti i dipendenti di Botium Toys** hanno accesso ai dati archiviati internamente e **potrebbero accedere ai dati delle carte di pagamento e alle PII/SPII (informazioni personali e sensibili) dei clienti.**

- **Non viene utilizzata la crittografia** per garantire la riservatezza delle informazioni sulle carte di credito dei clienti accettate, elaborate, trasmesse e archiviate localmente nel database interno dell'azienda.

- **Non sono stati implementati controlli di accesso** basati sul principio del **minimo privilegio** o sulla **separazione dei compiti**.

- Il **Dipartimento IT** ha garantito la **disponibilità** dei sistemi e ha integrato controlli per assicurare l'**integrità dei dati**.

- È installato un **firewall** che blocca il traffico in base a un set di regole di sicurezza adeguatamente definite.

- È installato e regolarmente monitorato un **software antivirus** dal Dipartimento IT.

- Il Dipartimento IT **non ha installato un sistema di rilevamento delle intrusioni (IDS)**.

- **Non esistono piani di disaster recovery** e l'azienda **non dispone di backup** dei dati critici.

- Il Dipartimento IT ha stabilito un piano per **notificare i clienti dell'UE entro 72 ore** in caso di violazione della sicurezza. Inoltre, **politiche e procedure sulla privacy** sono state sviluppate e applicate tra i membri del Dipartimento IT e gli altri dipendenti per documentare e mantenere correttamente i dati.

- Sebbene esista una **policy sulle password**, i requisiti sono **minimali** e **non conformi** agli standard attuali di complessità minima (ad esempio: almeno otto caratteri, combinazione di lettere e almeno un numero o caratteri speciali).

- **Non esiste un sistema centralizzato di gestione delle password** che imponga tali requisiti minimi, il che a volte riduce la produttività quando dipendenti o fornitori inviano ticket al Dipartimento IT per il recupero o il reset delle password.

- Sebbene i **sistemi legacy** vengano monitorati e mantenuti, **non esiste un programma regolare** per queste attività e **i metodi di intervento non sono chiari**.

- La **sede fisica** dell'azienda, che comprende gli **uffici principali, il negozio e il magazzino**, dispone di **serrature adeguate**, un sistema **CCTV (telecamere a circuito**

chiuso) aggiornato, nonché di **sistemi antincendio e di rilevamento fumo funzionanti**.