UNIONE INDUSTRIALE BIELLESE

News - 24/02/2025

Perché investire nella Cybersecurity non è una spesa in più, ma un investimento per il futuro?

In collaborazione con Digital Innovation Hub Piemonte e Valle D'Aosta

Grazie alla collaborazione con il **Digital Innovation Hub Piemonte e Valle D'Aosta** vi proponiamo una selezione di notizie e articoli sui temi della digitalizzazione delle imprese, con l'obiettivo di offrirvi contenuti sempre aggiornati e di alta qualità su queste tematiche strategiche.

Perché investire nella Cybersecurity non è una spesa in più, ma un investimento per il futuro?

Immagina di avere una cassaforte piena di tesori. La metti nel bel mezzo della piazza principale senza serratura? Certo che no! La cybersecurity per la tua impresa è esattamente questo: proteggere il tuo tesoro, cioè i tuoi dati, i tuoi clienti, e il tuo business. Ma attenzione, la chiave di questa cassaforte non è una spesa improvvisata: serve un **budget annuale pianificato** e, soprattutto, una strategia. L'informatizzazione della realtà (IOT, Industrial Security, ecc) e la materializzazione dell'informazione (social networking, influencers, e commerce, ecc) riducono la distanza tra Information Security, Cybersecurity ed Industrial Security.

La complessità che ci circonda rende oggi pressoché impossibile proteggere senza prevenire.
I criminali sono sempre alla ricerca di nuovi modi per entrare nei sistemi. C'è un flusso costante di patch di sicurezza da applicare, nuovi dati da proteggere, nuovi dipendenti che necessitano dell'accesso al sistema ed ex dipendenti a cui è necessario revocare l'accesso. I**nvestire nell'upskilling** dei dipendenti in ottica di sicurezza si traduce anche in un vantaggio competitivo. Personale adeguatamente formato è infatti in grado di gestire i rischi cyber in modo più efficiente, riducendo l'esposizione a potenziali violazioni, interruzioni di servizio e conseguenti danni reputazionali ed economici.
Pianifica, Forma, Implementa: definire un budget annuale per la cybersecurity non è solo una questione di tecnologia, ma di persone, processi e cultura aziendale.

Conviene investire nella cybersecurity?

Allocare risorse dedicate per la cybersecurity significa avere una base solida per:

- **Aggiornare costantemente le strategie aziendali** per stare al passo con normative, tecnologie e nuovi scenari di rischio. Una strategia di valutazione dei rischi efficace deve essere continua e adattativa
- **Valutare rischi e impatti** con una metodologia strutturata, che vada oltre il "tappare le falle". In poche parole: prevenire è meglio che rattoppare. Definire un **Risk Management Plan** che tenga conto delle vulnerabilità, del potenziale impatto, delle azioni di mitigazione rispetto alla tipologia degli apparati. Il Risk Manager a seguito di valutazioni costi/benefici, stima che il rischio rappresentato sia entro le soglie di accettabilità, non ravvede la necessità di proporre ulteriori interventi.

- **Eseguire un Cyber Maturity Assessment** per capire il livello di vulnerabilità dell'azienda ed avere un quadro chiaro di dove si è e dove si vuole andare. Per proteggere al meglio la tua attività e i dati ad essa connessi, devi sapere dove la tua infrastruttura informatica è più vulnerabile Comprendere dove e come un hacker potrebbe infiltrarsi nel tuo sistema informativo, ti consente di essere proattivo nell'identificare eventuali falle del sistema di sicurezza. Ed è qui che entra in gioco il **Vulnerability Assessment un test da effettuare periodicamente.** Dopo aver effettuato opportuni aggiornamenti dei software in uso, è opportuno **effettuare dei pentest** per verificare che le vulnerabilità individuate siano state soppresse e che le misure di prevenzione e protezione della sicurezza digitale siano corrette e in grado di reagire ai possibili attacchi, verificando con tentativi di penetrazione di prova e non distruttivi.

Valutare rischi e impatti sono analisi che valgono non solo per i progetti ICT! Qualsiasi nuovo progetto aziendale, dal lancio di un prodotto ad un'espansione logistica, dovrebbe passare attraverso un'attenta valutazione dei rischi cyber.

Governance della cybersecurity: ruoli e responsabilità

La **cybersecurity** non è solo una questione tecnica, ma un **pilastro fondamentale della sostenibilità aziendale.**
Non fare l'errore comune di delegare tutto e solo al reparto IT o al fornitore esterno di servizi ICT.
Il vertice deve saper scegliere fornitori competenti e affidabili, e saperli supervisionare nella loro gestione della sicurezza digitale; essa non rappresenta solo un problema tecnico, ma soprattutto di business, dato che ormai è determinante per la continuità operativa dell'intera impresa. Le policy conosciute e comprese da parte dei fornitori (es. sottoscrizione delle policy cybersecurity da parte del fornitore in fase di apertura rapporto).
La cybersecurity è una questione di **governance aziendale**, dove:

- I **ruoli e le responsabilità** sono chiari, definiti e condivisi: assegnati con nomine, mansionari, organigrammi o procedure e che siano ben compresi.
- **Le policy e le procedure** non sono lasciate al caso, ma formalizzate e comprensibili a tutti. Le responsabilità specifiche di ciascun ruolo definite all'interno di un modello organizzativo/operativo che descriva in modo completo i processi comunicativi e di escalation per la gestione degli adempimenti di sicurezza di tutta l'organizzazione. Sono inoltre essenziali per dimostrare l'accountability, così come richiesto dal GDPR e dalle altre normative dell'Unione Europea nell'ambito della sicurezza digitale, quali NIS2, DORA.
- L'intera azienda è consapevole che la sicurezza digitale è **un lavoro di squadra.**

Insomma, serve un approccio **olistico e integrato,** che coinvolga ogni funzione, dal marketing alle risorse umane.

Quali sono i rischi se non si investe in cybersecurity?

Pensare che "non succederà a noi" è il primo passo verso il disastro. **Attacchi ransomware, furti di dati, interruzioni di servizio**… non sono scenari da film, ma realtà quotidiana. Sottovalutare questi aspetti può significare:

- Perdere la fiducia dei clienti.
- Subire danni economici significativi.
- Compromettere la reputazione aziendale.

Perchè investire in cybersecurity aumenta la consapevolezza?

Essere critici e consapevoli oggi significa preservare il tuo business per il domani. **Pianificare un budget dedicato alla cybersecurity**, aggiornare le strategie, e fare analisi strutturate come il Cyber Maturity Assessment non sono lussi, ma necessità.
La vera sfida? Capire che la sicurezza non è un prodotto, ma un processo continuo.
Anche in un momento di incertezza come quello attuale, con cali dei volumi e mercati instabili, esistono strumenti concreti per guardare avanti e fare scelte trasformative. I bandi del PNRR, dell'Europa e delle Regioni rappresentano un'opportunità unica per le imprese di investire in innovazione, rafforzare la propria resilienza e collocarsi in un sistema più ampio.
Questo è il momento giusto per agire: **costruire nuove relazioni, esplorare collaborazioni strategiche e prepararsi a un futuro in cui la sostenibilità, la sicurezza e la digitalizzazione siano al centro.**

Guardare avanti significa non solo proteggere, ma anche trasformare il proprio business per affrontare con successo le sfide di domani.
Sei prontə a cogliere questa occasione?

Il DIHP e la partecipazione di Unione Industriale Biellese

Il **Digital Innovation Hub Piemonte e Valle D'Aosta (DIHP)** è un "centro di trasferimento tecnologico" creato per supportare la trasformazione digitale delle imprese delle due regioni, in particolare le PMI, e la Pubblica Amministrazione. L'obiettivo è aumentare la consapevolezza e la comprensione delle sfide digitali, guidando le aziende nell'elaborazione dei loro piani di digitalizzazione e fornendo servizi di mentoring e supporto. Collaborano con università, centri di ricerca e aziende leader per promuovere l'innovazione tecnologica. L' **Unione Industriale Biellese** partecipa al DIHP offrendo supporto alle aziende locali per avviare strategie di digitalizzazione, accedere a finanziamenti e migliorare la loro maturità digitale attraverso valutazioni e consulenze specializzate.

Scopri di più: DIHP
