# L’importanza della cybersecurity aziendale: come creare una cultura della sicurezza in azienda

La crescente digitalizzazione delle imprese ha portato numerosi vantaggi, ma ha anche aumentato i rischi legati alla cybersecurity aziendale. Le minacce cibernetiche sono sempre più sofisticate e i dati aziendali, così come quelli dei clienti, sono diventati obiettivi ambiti per i cybercriminali. In questo scenario, è fondamentale che le aziende adottino una cultura della sicurezza digitale che coinvolga ogni dipendente, dal più alto dirigente fino al personale operativo.

Solo con una cultura diffusa della sicurezza, le organizzazioni possono proteggere i propri dati e garantire la continuità operativa. In questo articolo, esploreremo come promuovere una cultura della cybersecurity in azienda, l’importanza della formazione continua e la consapevolezza dei rischi, l’integrazione della sicurezza nei processi aziendali quotidiani e il ruolo fondamentale del top management.

## Come promuovere una cultura della cybersecurity tra i dipendenti

La **security culture** è costituita da un insieme di principi e comportamenti che devono essere adottati e condivisi da tutti i membri di un’organizzazione, influenzando il modo in cui le persone percepiscono e affrontano le tematiche legate alla cybersecurity.

**Il fattore umano rappresenta l’anello debole della catena nell’ambito della cybersecurity aziendale** e costituisce uno dei rischi cyber più difficili da gestire.

La creazione di una cultura della cybersecurity non avviene però in modo spontaneo. La creazione di una cultura della cybersecurity richiede un approccio strutturato e consapevole. Per promuovere una mentalità di sicurezza tra i dipendenti, è necessario che ogni membro dell’organizzazione comprenda l’importanza della protezione dei dati e dei sistemi aziendali. La cultura della sicurezza deve essere vista come un valore condiviso che coinvolge ogni livello dell’azienda, non limitandosi a politiche e tecnologie ma influenzando anche i comportamenti quotidiani dei dipendenti.

Ogni dipendente, responsabile di reparto o membro del Consiglio di amministrazione deve essere consapevole del proprio ruolo nella sicurezza informatica, senza delegare interamente questo compito al reparto IT o al CISO.

Per ottenere questo, le aziende devono impegnarsi in attività educative e informative che sensibilizzino i dipendenti sui pericoli informatici, come il phishing, l’uso di password deboli e la navigazione su reti non sicure. Le comunicazioni devono essere chiare e facilmente comprensibili, così da rendere tutti consapevoli delle politiche di sicurezza aziendali. È importante, inoltre, che ogni dipendente percepisca la propria responsabilità nella protezione delle informazioni aziendali, facendo propria la cultura della sicurezza.

È certamente vero che la formazione in ambito di cyber security e la consapevolezza riguardo alle minacce informatiche, pur essendo fondamentali, non bastano da sole a garantire una difesa efficace contro attacchi sempre più avanzati, mirati e in costante evoluzione.

Questo significa che le misure di sicurezza devono essere

sviluppate in modo da ridurre al minimo l’impatto sull’esperienza dell’utente, senza però compromettere il livello di protezione necessario.

Ad esempio, un sistema con elevati standard di sicurezza potrebbe imporre procedure di autenticazione complesse o richiedere agli utenti di seguire rigidi protocolli, che potrebbero risultare poco pratici o scomodi. L’obiettivo è trovare un equilibrio ottimale tra sicurezza e usabilità.

Oltre a fornire risorse chiare, infatti le aziende dovrebbero coinvolgere i dipendenti in iniziative di sicurezza, come simulazioni di attacchi, corsi interattivi di cybersecurity e programmi di sensibilizzazione continua, che li preparino a riconoscere e a reagire correttamente ai pericoli. Inoltre, la sicurezza dovrebbe essere parte integrante del processo di Onboarding per ogni nuovo dipendente, così da stabilire fin dal primo giorno l’importanza della protezione dei dati aziendali.

## Formazione continua e consapevolezza dei rischi

La formazione continua è uno degli strumenti più efficaci per costruire una solida cultura della cybersecurity aziendale. Poiché le minacce e le tecnologie evolvono rapidamente, è fondamentale che i dipendenti vengano aggiornati regolarmente. I percorsi formativi dovrebbero includere sia sessioni teoriche che pratiche, come simulazioni di attacchi reali, che permettano ai dipendenti di riconoscere situazioni di minaccia e rispondere in modo adeguato.

Investire nella cultura della sicurezza digitale è uno dei metodi principali per consentire ai dipendenti di correggere comportamenti errati, radicati nel tempo a causa di abitudini poco sicure e della scarsa attenzione precedentemente dedicata dall’organizzazione alla cybersecurity. È necessario

intervenire con strategie efficaci di sensibilizzazione e formazione.

Le aziende dovrebbero anche monitorare periodicamente i progressi dei dipendenti, attraverso test di verifica delle conoscenze acquisite, valutazioni delle competenze pratiche ed esercitazioni che simulano scenari di attacco reali

La formazione non deve essere un evento isolato, ma un processo continuo che tiene conto delle nuove minacce emergenti. In questo modo, l'azienda può garantire che i dipendenti siano sempre preparati a fronteggiare le minacce informatiche in tempo reale.

# Integrazione della sicurezza nei processi aziendali quotidiani

La sicurezza informatica non può essere trattata come un'attività isolata, separata dalle operazioni quotidiane. Deve essere integrata nei processi decisionali aziendali di routine, come la gestione dei dati, le comunicazioni aziendali e la protezione delle risorse digitali. È fondamentale implementare un approccio di security-by-design, incorporando misure protettive fin dalla fase iniziale di progettazione dei sistemi e dei processi.

## Normative e compliance avanzate nella sicurezza informatica

Questa integrazione della sicurezza nei processi aziendali è ulteriormente guidata e rafforzata dal quadro normativo in continua evoluzione. Infatti, un aspetto cruciale per garantire una protezione efficace è la conformità alle normative vigenti, che non rappresentano soltanto obblighi legali, ma anche linee guida preziose per strutturare un sistema di difesa completo.

**GDPR (General Data Protection Regulation)**: Oltre agli aspetti

generali di protezione dei dati personali, il GDPR impone requisiti specifici di cybersecurity come la pseudonimizzazione e la cifratura dei dati personali, l'implementazione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio, e il principio di Data Protection by Design and by Default. Quest'ultimo richiede che la protezione dei dati sia integrata fin dalla progettazione dei sistemi e dei processi, non come elemento aggiuntivo.

**NIS2 Directive**: L'evoluzione della direttiva sulla sicurezza delle reti e dei sistemi informativi amplia significativamente l'ambito di applicazione rispetto alla precedente NIS, estendendosi a settori critici come energia, trasporti, sanità, infrastrutture digitali e fornitori di servizi digitali. Impone requisiti di gestione dei rischi di cybersecurity più rigorosi, obblighi di notifica degli incidenti più severi e la necessità di implementare misure di sicurezza appropriate.

**DORA (Digital Operational Resilience Act)**: Specifico per il settore finanziario nell'UE, questo regolamento mira a garantire che le entità finanziarie possano resistere, rispondere e riprendersi da tutti i tipi di interruzioni e minacce legate all'ICT. Richiede test di resilienza operativa digitale, gestione dei rischi ICT e reporting degli incidenti gravi.

**SEC Cybersecurity Disclosure Requirements**: Per le aziende quotate, la Securities and Exchange Commission ha introdotto requisiti di divulgazione più rigorosi relativi ai rischi di cybersecurity e agli incidenti. Le organizzazioni devono divulgare informazioni materiali su incidenti di cybersecurity e sulle loro strategie di gestione del rischio.

L'integrazione di questi requisiti normativi nei processi aziendali non dovrebbe essere vista come un mero esercizio di conformità, ma come un'opportunità per elevare e

standardizzare le pratiche di sicurezza in tutta l'organizzazione. Un approccio efficace è quello di mappare i controlli di sicurezza esistenti rispetto ai requisiti normativi, identificando gap e sovrapposizioni, e sviluppando un framework di controllo unificato che soddisfi simultaneamente più normative.

Dando priorità all'integrazione delle misure di tutela in tutti gli aspetti delle operazioni, un'azienda può rafforzarsi contro potenziali minacce e vulnerabilità. Un approccio security-by-design è fondamentale per l'azienda e per le parti interessate. Integrare la sicurezza fin dalla progettazione è fondamentale per l'azienda e per le parti interessate. Se implementato correttamente, può aiutare a promuovere la fiducia tra dipendenti, clienti, fornitori e partner.

I principali stakeholder, come il **Chief Information Officer** (CIO), il **Chief Information Security Officer** (CISO) e il **Chief Financial Officer** (CFO), lavorano insieme in modo sinergico, supportati da strumenti specifici come il Cybersecurity Risk Register e l'Enterprise Risk Register.

Questa struttura sottolinea l'importanza di una visione globale e integrata delle minacce, evitando che la sicurezza digitale sia confinata in un ambito specialistico limitato alle sole tecnologie.

Tale integrazione è fondamentale per allineare le strategie di sicurezza con gli obiettivi aziendali generali, assicurando che le decisioni in ambito cyber security siano in linea con il livello di rischio accettato dall'organizzazione e contribuiscano al raggiungimento della missione e degli obiettivi strategici complessivi.

## Metriche e KPI avanzati per la gestione della sicurezza

Per gestire efficacemente la sicurezza informatica e misurarne il valore all'interno dell'organizzazione, è essenziale

adottare metriche e KPI avanzati che vadano oltre i semplici indicatori operativi. Un framework di metriche sofisticato dovrebbe includere:

### Metriche di maturità della sicurezza

Basate su modelli come il Capability Maturity Model Integration (CMMI) o il NIST Cybersecurity Framework, queste metriche valutano il livello di maturità dei controlli di sicurezza dell'organizzazione su una scala progressiva. Tali misurazioni consentono di tracciare l'evoluzione delle capacità di sicurezza nel tempo e di confrontarle con standard di settore o best practice. Un approccio particolarmente efficace è la valutazione della maturità mediante heat map che evidenziano aree di forza e di debolezza, facilitando l'allocazione strategica delle risorse.

### Metriche basate sul tempo

Questi indicatori misurano la velocità ed efficienza dei processi di sicurezza:

- Mean Time to Detect (MTTD): Misura il tempo medio tra l'inizio di un incidente di sicurezza e la sua rilevazione. Un MTTD ridotto indica capacità di detection più efficaci.
- Mean Time to Respond (MTTR): Quantifica il tempo necessario per rispondere a un incidente dopo la sua rilevazione. Riflette l'efficienza dei processi di incident response.
- Mean Time to Contain (MTTC): Misura quanto tempo occorre per isolare o contenere una minaccia dopo la sua identificazione, limitando l'impatto potenziale.
- Mean Time to Recover (MTTR): Indica il tempo necessario per ripristinare completamente le operazioni normali dopo un incidente.

### DORA metrics per la resilienza operativa

Originariamente sviluppate nel contesto DevOps, le metriche

DORA (DevOps Research and Assessment) sono particolarmente rilevanti per la cybersecurity moderna poiché misurano la capacità dell'organizzazione di implementare cambiamenti in modo rapido e sicuro:

- Frequenza di deployment: Nel contesto della sicurezza informatica, misura la velocità con cui vengono rilasciati aggiornamenti di sicurezza critici, patch e nuove configurazioni dei controlli difensivi. Un'alta frequenza indica maggiore agilità nel rispondere a nuove minacce o vulnerabilità.
- Lead Time for Changes: Quantifica il tempo che intercorre tra l'identificazione di una vulnerabilità o di un requisito di sicurezza e la sua effettiva implementazione nell'ambiente di produzione. Un lead time ridotto è cruciale per minimizzare la finestra di esposizione alle minacce note.
- Change Failure Rate: Rappresenta la percentuale di modifiche ai sistemi di sicurezza che introducono nuovi problemi, come falsi positivi nei sistemi di rilevamento, interruzioni di servizio o nuove vulnerabilità. Un basso tasso di fallimento indica processi di test e validazione maturi.
- Time to Restore Service: Misura la rapidità con cui l'organizzazione può ripristinare la normale operatività dopo un incidente di sicurezza, riflettendo direttamente la resilienza operativa dell'infrastruttura e l'efficacia dei piani di disaster recovery.

L'implementazione di queste metriche consente alle organizzazioni di valutare oggettivamente la propria capacità di evolvere i sistemi di difesa al ritmo richiesto dal panorama delle minacce in continua evoluzione.

## Risk-based metrics

Indicatori che collegano direttamente le attività di sicurezza al rischio aziendale:

- Esposizione quantificata al rischio (QRE): Stima del rischio residuo in termini monetari.
- Return on Security Investment (ROSI): Misura il rendimento degli investimenti in sicurezza, confrontando il costo di implementazione con la riduzione del rischio atteso.
- Risk reduction per dollar spent: Quantifica l'efficienza degli investimenti in sicurezza in termini di riduzione del rischio.

L'implementazione di queste metriche avanzate consente non solo di monitorare lo stato della sicurezza, ma anche di comunicare efficacemente il valore della cybersecurity ai vertici aziendali attraverso un linguaggio orientato al business. È fondamentale che tali metriche siano contestualizzate rispetto agli obiettivi aziendali e presentate mediante dashboard interattivi che consentano analisi approfondite e decision-making basato sui dati.

# Sfide nell'integrazione della sicurezza nei processi aziendali

Possono essere identificate diverse sfide da affrontare per garantire una corretta integrazione strategica, tattica e operativa tra le funzioni tecniche e quelle di governance aziendale. Ecco alcune delle principali problematiche:

1. **Differente percezione del rischio tra le funzioni aziendali**: Nel contesto del Cybersecurity Risk Management (CSRM), l'analisi delle minacce tende ad essere focalizzata su valutazioni specifiche e su sistemi singoli, portando a una visione frammentata. In molti casi, ad esempio, il perimetro di valutazione degli asset si limita solo a quelli IT/cyber, senza considerare gli asset gestiti dalla funzione di Risk Management. Questo può generare sovrapposizioni nelle responsabilità, come nel caso dei datacenter, che

includono sia asset IT che non-IT, come infrastrutture fisiche e hardware di rete. La funzione di governance cyber deve essere consapevole della natura interconnessa e critica di tali asset per garantirne una protezione adeguata. L'asimmetria informativa tra le funzioni può ostacolare la condivisione delle informazioni, impedendo una gestione efficace del rischio e influenzando negativamente la prontezza nelle risposte a eventuali crisi.

2. **Differenze nelle tassonomie e nelle competenze**: Le funzioni tecniche, orientate sugli aspetti IT, tendono a produrre report dettagliati sui sistemi, includendo analisi delle vulnerabilità, incidenti di sicurezza e indicatori di compromissione. Sebbene utili per la gestione delle operazioni IT, questi rapporti potrebbero essere troppo dettagliati per le funzioni di governance, che necessitano di una visione più strategica e aggregata. La mancanza di KPI (Key Performance Indicators) comuni rende difficile per la governance integrare e utilizzare le informazioni provenienti dal CSRM, complicando ulteriormente l'analisi delle minacce a livello aziendale.
3. **Cybersecurity nelle nuove iniziative aziendali**: In occasione di operazioni come fusioni e acquisizioni (M&A) o il lancio di nuovi prodotti, le valutazioni di cybersecurity sono essenziali per prevenire perdite di dati durante l'integrazione di sistemi IT o per affrontare vulnerabilità nelle tecnologie da integrare. La capacità di comunicare efficacemente eventuali vulnerabilità e risolvere le problematiche relative ai tempi di rilascio è cruciale nel contesto dell'Enterprise Risk Management (ERM). La diversità di linguaggio e di priorità tra le funzioni tecniche e la governance può generare disallineamenti, portando a una visione frammentata dei pericoli associati a queste iniziative strategiche.

Le sfide nell’integrare le informazioni provenienti dalle funzioni cyber nell’ERM condividono principi comuni legati alla natura specialistica della cyber security, che è stata storicamente trattata come un ambito separato, con risorse e competenze dedicate. Inoltre, l’assenza di classificazione e di un linguaggio comune per rappresentare i rischi cyber nel contesto strategico aziendale contribuisce a queste difficoltà.

## Misure di sicurezza quotidiane

Ogni dipendente però, deve essere consapevole delle pratiche di sicurezza pertinenti al proprio ruolo, affinché ogni attività aziendale si svolga nel rispetto delle politiche di protezione dei dati.

La gestione sicura delle credenziali, l’adozione di password robuste e l’utilizzo dell’autenticazione a più fattori (MFA) devono essere politiche standard applicate a tutti i livelli aziendali. Allo stesso modo, l’uso di software di sicurezza aggiornati, come antivirus e firewall, deve essere parte integrante dei processi operativi quotidiani. In questo modo, le aziende possono ridurre al minimo i pericoli legati a vulnerabilità non controllate.

Anche le comunicazioni aziendali devono essere protette. Per garantire la sicurezza delle informazioni, è essenziale che tutte le comunicazioni interne ed esterne avvengano tramite canali sicuri e che i dati sensibili vengano criptati per evitare violazioni della privacy. Attraverso la gestione sicura dei dispositivi mobili e del lavoro remoto, la sicurezza informatica diventa una componente naturale delle attività aziendali, riducendo il rischio di errori umani e attacchi informatici.

# Ruolo del top management nel promuovere la cybersecurity aziendale

Il top management svolge un ruolo cruciale nella promozione della cultura della sicurezza digitale. È compito del top management assicurarsi che l'organizzazione adempia a tutte le normative e disposizioni vigenti in materia di sicurezza delle informazioni. Ciò implica un approccio proattivo, volto a monitorare costantemente il contesto normativo e a incorporare i requisiti di conformità all'interno dei processi aziendali.

I dirigenti devono essere i primi a dare l'esempio, adottando buone pratiche di sicurezza e mostrando il loro impegno per la protezione dei dati aziendali. La leadership deve supportare e promuovere la cultura della cybersecurity, facendo capire a tutta l'organizzazione che la sicurezza è una priorità strategica.

In questo contesto, è fondamentale che il management fornisca le risorse necessarie per implementare politiche di sicurezza efficaci. Ciò include investimenti in tecnologie avanzate, formazione continua per i dipendenti e l'assunzione di esperti di cybersecurity per garantire che l'azienda sia sempre protetta da minacce esterne e interne.

Inoltre, i dirigenti devono stabilire una visione strategica per la sicurezza, integrandola nella pianificazione aziendale complessiva e assicurandosi che tutte le politiche e i processi aziendali siano allineati con gli obiettivi di protezione dei dati.

## I dirigenti come bersaglio privilegiato

Un aspetto importante da sottolineare è che, i **bersagli privilegiati** di questi attacchi, fanno notare gli esperti, sono proprio i **dirigenti**. I manager C-level sono le vittime

ideali per i cyber criminali.

Proprio i top manager sono sempre più spesso il bersaglio principale dei cyber criminali. Il motivo è chiaro: per un hacker, violare i sistemi di un dirigente significa ottenere accesso a dati sensibili e operare all'interno della rete aziendale con privilegi elevati, aumentando così l'impatto dell'attacco e il possibile guadagno illecito.

I manager C-level rappresentano le vittime ideali per i cyber criminali per diversi motivi:

1. L'accesso a un account di un dirigente consente di ottenere privilegi elevati all'interno dei sistemi aziendali
2. I dirigenti hanno accesso a informazioni commerciali e strategiche di alto valore
3. Possono autorizzare transazioni finanziarie significative, facilitando le frodi

I dirigenti sono sempre più vulnerabili agli attacchi informatici, poiché le loro vite digitali e professionali sono sempre più intrecciate. Dispositivi domestici, sistemi di sicurezza, dispositivi utilizzati dai familiari e persino l'attività sui social media possono costituire punti deboli, aumentando il rischio di violazioni che potrebbero avere ripercussioni anche sull'ambiente lavorativo.

Di conseguenza, la sfera privata è diventata un nuovo fronte di attacco per i cyber criminali. È fondamentale che dirigenti e membri del CdA siano consapevoli di queste minacce e adottino adeguate pratiche di sicurezza per proteggere sia se stessi che l'azienda.

La gestione delle minacce esterne rappresenta una sfida complessa per le organizzazioni, poiché questi fattori non possono essere facilmente controllati. La vita digitale dei dirigenti, infatti, può esporre l'azienda a pericoli significativi, dato che una parte di loro potrebbe già avere

informazioni personali compromesse.

Per questo motivo, è essenziale che le aziende adottino misure di protezione specifiche per tutelare i propri dirigenti e prevenire eventuali vulnerabilità derivanti dalla loro vita privata e digitale, come:

- Formazione specifica sui rischi di social engineering mirati;
- Protezione avanzata dei dispositivi personali;
- Monitoraggio della presenza online e delle possibili esposizioni di dati;
- Procedure di sicurezza rafforzate per gli accessi privilegiati.

Un altro aspetto fondamentale è la responsabilizzazione dei dipendenti. Il top management deve lavorare per far capire che la sicurezza è una responsabilità condivisa, non solo una funzione del dipartimento IT. In questo modo, i dipendenti si sentiranno coinvolti attivamente nel processo di protezione dei dati aziendali e saranno più motivati a seguire le linee guida di sicurezza.

# Modelli avanzati di simulazione e stress test

Per un'efficace valutazione della resilienza dell'organizzazione alle minacce cyber, il top management dovrebbe promuovere l'implementazione di modelli avanzati di simulazione e stress test che vanno oltre i tradizionali penetration test. Questi approcci sofisticati consentono di valutare non solo la resistenza tecnica dei sistemi, ma anche l'efficacia dei processi decisionali e la preparazione del personale:

## Breach and Attack Simulation (BAS):

A differenza dei test di penetrazione tradizionali, che

rappresentano valutazioni puntuali, le piattaforme BAS consentono simulazioni continue e automatizzate di tecniche di attacco reali. Questi strumenti emulano il comportamento degli avversari mappando le loro tattiche e tecniche secondo framework come MITRE ATT&CK, e testano continuamente i controlli di sicurezza esistenti per identificare gap di protezione. I vantaggi principali includono:

- Valutazione continua dell'efficacia dei controlli di sicurezza in produzione;
- Validazione automatizzata delle configurazioni di sicurezza dopo modifiche all'infrastruttura;
- Prioritizzazione degli investimenti in sicurezza basata su evidenze empiriche di vulnerabilità sfruttabili;
- Generazione di metriche oggettive per la misurazione dell'efficacia della sicurezza.

## Tabletop Exercises specifici per C-level:

Esercitazioni strutturate che simulano scenari di crisi cyber, specificamente progettate per testare la preparazione del top management e del Consiglio di Amministrazione. Questi esercizi sono facilitati da esperti che guidano i dirigenti attraverso scenari realistici come attacchi ransomware, violazioni di dati o compromissione della supply chain, richiedendo decisioni in tempo reale. Gli scenari sono accuratamente adattati al contesto specifico dell'organizzazione, al suo settore e al suo profilo di rischio, e includono considerazioni su:

- Gestione della comunicazione interna ed esterna durante una crisi;
- Implicazioni legali e normative degli incidenti;
- Valutazione dell'impatto finanziario e reputazionale;
- Trade-off tra continuità operativa e contenimento della minaccia;
- Interazione con le autorità competenti e gli stakeholder esterni.

## Cyber Range Training:

Ambienti virtualizzati che replicano l'infrastruttura aziendale reale in cui team di sicurezza, sviluppatori e personale operativo possono esercitarsi a rispondere a scenari di attacco sofisticati. I Cyber Range offrono:

- Simulazioni immersive di scenari di attacco avanzati in un ambiente controllato;
- Addestramento hands-on per il personale tecnico con feedback immediato;
- Possibilità di testare tecniche di difesa innovative senza rischi per l'ambiente di produzione;
- Valutazione delle capacità di risposta agli incidenti in condizioni di stress realistico;
- Perfezionamento della collaborazione cross-funzionale durante gli incidenti.

L'implementazione sistematica di questi modelli di simulazione avanzati consente all'organizzazione di identificare proattivamente vulnerabilità e gap nei processi, migliorare le capacità di risposta, rafforzare il coordinamento tra i vari team e, in ultima analisi, aumentare significativamente la resilienza complessiva agli attacchi cyber. È fondamentale che i risultati di queste simulazioni si traducano in piani d'azione concreti con chiare responsabilità e tempistiche, e che le lessons learned siano incorporate nei processi di sicurezza e nei programmi di formazione.

## Conclusioni

In un mondo in cui le minacce informatiche sono sempre più pervasive e sofisticate, la cultura della sicurezza informatica è essenziale per proteggere i dati aziendali e garantire la continuità operativa. La promozione di una cultura della cybersecurity aziendale richiede un impegno costante da parte di tutte le aree aziendali: la sensibilizzazione dei dipendenti, la formazione continua, l'integrazione della sicurezza nei processi quotidiani e il

coinvolgimento attivo del top management. Solo quando la sicurezza diventa una priorità condivisa, ogni membro dell’organizzazione può contribuire a difendere l’azienda dalle minacce informatiche, riducendo il pericolo di attacchi e garantendo una protezione efficace contro le violazioni della privacy.

Attraverso un approccio integrato e consapevole, le aziende possono affrontare le sfide della cybersecurity e costruire un ambiente sicuro per i propri dati, le proprie risorse e i propri clienti. Con il continuo avanzamento delle tecnologie e un adeguato supporto normativo, la cultura della sicurezza informatica può diventare una forza fondamentale nel successo a lungo termine di un’azienda.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/cybersecurity-aziendale-2/