Autotest di cybersecurity

CyberScore: 

Data di generazione del report: **08/11/2026 20:16**

> Questo report è una semplice autovalutazione del Suo livello di sicurezza informatica, basata esclusivamente sulle risposte al questionario ideato dagli esperti di Oxydian. Non costituisce in alcun modo un audit tecnico approfondito. Pur offrendoLe una prima panoramica dei Suoi punti di forza e delle Sue vulnerabilità in materia di cybersecurity, non sostituisce un'analisi rigorosa delle Sue infrastrutture e dei Suoi sistemi. Per andare oltre e beneficiare di un audit tecnico completo, non esiti a contattarci:
>
> contact@oxydian.fr

Sintesi:

Il Suo livello di sicurezza presenta debolezze significative che richiedono un'attenzione immediata. Il rischio di sfruttamento di alcune vulnerabilità è elevato e potrebbe compromettere la sicurezza complessiva della Sua organizzazione. Raccomandiamo vivamente l'adozione di misure correttive e un supporto specialistico per realizzare un audit approfondito.

Dettaglio dei punteggi per categoria (40.0%)

Password

Sicurezza dei dati



Monitoraggio e rilevamento



Sicurezza interna



Sicurezza esterna



Gestione della sicurezza



Identificazione dei rischi



Sicurezza fisica



Piano d'azione personalizzato:

Questo piano d'azione si basa sui risultati della Sua valutazione. Le consigliamo di seguire queste indicazioni per migliorare la Sua sicurezza informatica.

Conservazione sicura delle password
Si assicuri che tutte le password siano conservate in un password manager sicuro anziché su supporti non protetti.

Utilizzare un antivirus
Si assicuri che tutti i server e i computer siano dotati di un antivirus aggiornato per rilevare e bloccare le minacce.

Sostituzione dei computer obsoleti
Sostituisca o migri i computer obsoleti (Windows XP, Vista, 7, 8 o Windows Server 2003 / 2008 / 2012) per ridurre i rischi legati a vulnerabilità non corrette.

Separare i diritti utente e amministratore
Questa pratica consiste nell'assegnare account distinti per le attività quotidiane e per quelle amministrative. Riduce notevolmente il rischio di compromissione, limitando l'accesso ai privilegi elevati alle sole operazioni che richiedono effettivamente una gestione amministrativa.

Adozione di una policy per le password
Adotti una policy per le password rigorosa, affinché le password siano sicure, complesse e rinnovate regolarmente.

Protezione della posta elettronica con la 2FA
Attivi l'autenticazione a due fattori (2FA) su tutti gli account di posta elettronica aziendali (Microsoft 365, Google Workspace...). La compromissione della posta è il vettore di attacco più frequente contro le PMI e la 2FA blocca la grande maggioranza di questi attacchi.

Analisi regolare delle password
Faccia analizzare regolarmente le password da un professionista o dal Suo reparto IT per individuare password deboli e riutilizzate e rafforzare la sicurezza.

Attivazione della cifratura del disco
Si raccomanda vivamente di attivare la cifratura del disco su tutti i PC e server, utilizzando soluzioni come BitLocker per Windows o LUKS per Linux, per proteggere i dati sensibili da accessi non autorizzati.

Test di ripristino dei backup
Pianifichi test di ripristino regolari (almeno una volta a trimestre) per verificare che i backup siano realmente utilizzabili e misurare il tempo necessario alla ripresa dell'attività.

Realizzazione di una mappatura degli asset esterni
Aggiorni e completi regolarmente la mappatura dei Suoi asset esposti su internet per migliorare la gestione della sicurezza.

Adozione della 2FA per la VPN
Attivi l'autenticazione a due fattori (2FA) per tutti gli accessi VPN, così da rafforzare la sicurezza delle connessioni da remoto.

Procedura di risposta agli incidenti
Formalizzi una procedura di risposta agli incidenti: prime azioni da compiere, elenco dei contatti di emergenza (fornitore specializzato, assicuratore, Garante per la protezione dei dati personali in caso di violazione dei dati) e ruoli interni. La verifichi almeno una volta all'anno con un'esercitazione a tavolino (tabletop).

Adozione dell'autenticazione a due fattori
Attivi l'autenticazione a due fattori (2FA) su tutti gli account e i servizi critici per aggiungere un ulteriore livello di sicurezza.

Ridondanza dei backup
Si raccomanda vivamente di conservare i backup in più luoghi distinti per ridurre il rischio di perdita dei dati in caso di incidente.

Passaggio a un EDR
Sostituisca o integri il Suo antivirus tradizionale con una soluzione EDR (Endpoint Detection and Response), in grado di rilevare i comportamenti malevoli e di isolare i computer compromessi di fronte ad attacchi moderni come i ransomware.

Centralizzazione dei log
Centralizzi i log dei server e degli apparati critici su uno spazio di archiviazione dedicato e li conservi per diversi mesi (da 6 a 12 mesi consigliati). In questo modo potrà rilevare gli incidenti e analizzarli anche se l'attaccante cancella le tracce locali.

Realizzazione di una mappatura degli asset interni
Aggiorni e completi regolarmente la mappatura dei Suoi asset interni per migliorare la gestione della sicurezza.

Segmentazione della rete Wi-Fi
Implementi più reti Wi-Fi per separare gli accessi pubblici da quelli interni, così da rafforzare la sicurezza pur offrendo una rete Wi-Fi pubblica per il solo accesso a internet.

Adozione di una policy di aggiornamento esterna
Adotti una policy di aggiornamento rigorosa per tutti i Suoi asset esterni, così da ridurre al minimo i rischi legati alle vulnerabilità.

Adozione di un regolamento informatico aziendale
Si assicuri che tutti i dipendenti sottoscrivano un regolamento informatico che definisca regole e buone pratiche di sicurezza, con particolare attenzione alla protezione dei dati personali per rispettare i requisiti del GDPR.

Simulazioni di phishing regolari
Organizzi campagne di phishing simulato almeno una volta all'anno per misurare i riflessi dei Suoi collaboratori in condizioni reali e concentrare la sensibilizzazione sui punti deboli individuati.

Regolamentazione degli accessi dei fornitori
Regolamenti gli accessi dei Suoi fornitori: account nominativi dedicati, diritti limitati allo stretto necessario, disattivazione sistematica a fine intervento o contratto e tracciabilità delle connessioni.

Controllo degli accessi alla sala server
Implementi un controllo rigoroso degli accessi alla sala server per evitare manomissioni non autorizzate.

Adozione di una procedura di ingresso e uscita
Si assicuri di definire una procedura chiara per l'ingresso e l'uscita dei collaboratori, che preveda l'eliminazione degli account e degli accessi per proteggere l'azienda dai rischi per la sicurezza.

Legenda:

INFORMAZIONE

Rischio complessivo nullo, si tratta semplicemente di osservazioni emerse durante l'audit.

MINORE

Rischio complessivo basso che non richiede interventi rilevanti.

MODERATO

Rischio complessivo moderato che richiede interventi a medio termine.

MAGGIORE

Rischio complessivo elevato che richiede interventi a breve termine.

CRITICO

Rischio complessivo critico che richiede interventi immediati.