baramundi

Le **CHECK-LIST BARAMUNDI** forniscono consigli concisi, passo dopo passo, per gestire in modo semplice le sfide informatiche più comuni. Altre check-list sono disponibili su **www.baramundi.com/check-list**

Audit IT: ottimizzare la sicurezza informatica con questi 7 passaggi

Alla minima occasione, gli hacker si annideranno negli angoli bui della vostra rete alla ricerca di vulnerabilità aperte e tecnologie obsolete da sfruttare, per rubare dati o danneggiare la vostra azienda e arricchirsi con ransomware e altri attacchi. Un audit IT sistematico e approfondito può portare alla luce questi potenziali rischi e carenze, in modo da poter adottare le misure necessarie per proteggere gli utenti e i sistemi della vostra organizzazione, garantire la conformità e sostenere la produttività aziendale.

Pianificazione

Dall'hardware alla gestione dei dati, identificate le aree e i sistemi da verificare. Definite obiettivi specifici, come garantire la conformità, documentare le pratiche di sicurezza esistenti o promuovere la sensibilizzazione della cybersicurezza tra gli utenti.

Documentazione

Mantenete un inventario aggiornato e completo di tutti gli hardware, i software, i componenti di rete e le configurazioni di sistema. Questo vi aiuterà a fornire una chiara valutazione dello stato attuale e dei progressi successivi.

Verifica dell'efficacia della sicurezza

Rivolgetevi a risorse fidati per effettuare pentesting e analisi delle vulnerabilità delle misure di cybersicurezza IT esistenti, come firewall e programmi antivirus. Assicuratevi di esaminare la configurazione dei server e dei componenti di rete.

Controllo della conformità

Assicuratevi che la vostra infrastruttura IT sia conforme a tutte le normative vigenti, agli standard di settore o ai vostri requisiti interni in materia di sicurezza, protezione dei dati e continuità operativa. Prestate particolare attenzione a proteggere adeguatamente i dati critici per l'azienda, in modo che le normali operazioni possano riprendere rapidamente dopo un'emergenza, un incidente o un disastro.

Ottimizzazione della performance

Analizzate se le performance del sistema e l'infrastruttura di rete soddisfano le esigenze aziendali attuali e sono sufficientemente scalabili per supportare periodi di forte domanda, anche durante il ripristino.

Creazione di un piano d'azione

Definite le azioni e le risorse necessarie in base alla priorità o all'urgenza, designate responsabilità e scadenze chiare e affrontate le debolezze e le carenze identificate.

Reporting

La fase finale è il report di audit, che registra i risultati, le raccomandazioni e le priorità di miglioramento. È la base per tutte le misure successive. Mettete il report a disposizione delle parti interessate.

In sintesi: tramite gli audit IT regolari, si identificano i rischi per la cybersicurezza. Che si tratti di inventario, di scanner delle vulnerabilità o di gestione degli aggiornamenti, potete contare sulla baramundi Management Suite per garantire che il vostro audit abbia successo in ogni sottoarea.

TUTTI GLI ENDPOINT SOTTO CONTROLLO

La baramundi Management Suite offre ai team IT gli strumenti e la flessibilità necessari per gestire gli attuali ambienti di informatica ibrida da qualsiasi luogo. Per saperne di più sull'Unified Endpoint Management di baramundi, visitate il sito **www.baramundi.com.**