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**

Distribuire e configurare la crittografia BitLocker in 7 step

La crittografia del disco Microsoft BitLocker fornisce una protezione e una sicurezza indispensabili per i dati aziendali sensibili. Questa check-list in 7 step spiega come introdurla e configurarla in modo preciso per soddisfare le vostre esigenze.

Controllare l'hardware e definire le linee guida

Verificate se i dispositivi finali soddisfano i requisiti di BitLocker, tra cui il supporto TPM e BIOS o UEFI, i formati dei drive e le versioni di Windows. Definite linee guida di utilizzo chiare e quali dispositivi devono essere crittografati, ad esempio i notebook.

Introduzione passo-passo ed esecuzione di test

Pianificate un rollout graduale con test su singoli dispositivi. Installate BitLocker su tutti i dispositivi interessati solo dopo aver verificato che gli utenti possano accedere in modo affidabile ai loro dispositivi e che non vi siano incompatibilità.

Attivazione centrale durante l'installazione del sistema operativo

Il modo migliore per implementare BitLocker è attivarlo durante l'installazione del sistema operativo da una console di amministrazione centralizzata. In questo modo si risparmia tempo e si facilita il rollout.

Sospendere BitLocker durante la distribuzione del software

Assicuratevi di mettere in pausa o sospendere BitLocker quando installate o aggiornate determinati software, applicazioni di terze parti e firmware, altrimenti le installazioni automatiche si bloccheranno in attesa di un PIN BitLocker. Ricordatevi di riattivare BitLocker al termine dell'installazione.

Implementare lo sblocco della rete

Attivate la funzione di sblocco della rete in modo che i sistemi collegati alla rete protetta dell'azienda possano avviarsi automaticamente senza il PIN BitLocker. In questo modo si mantiene la protezione e si migliora la soddisfazione dell'utente.

Salvare le chiavi di ripristino a livello centrale

Conservate le chiavi di ripristino BitLocker in una location centrale e sicura, facilmente accessibile ai membri autorizzati del team IT, in modo che i collaboratori possano riottenere rapidamente l'accesso in caso di password dimenticata o di modifiche all'hardware.

Formazione degli utenti finali e supporto

Informate tutti gli utenti finali su BitLocker e sui suoi vantaggi. Potrebbe anche essere necessario informarli sulle procedure di accesso modificate. Preparate il team di supporto a risolvere i problemi o a rispondere alle domande relative a BitLocker.

In sintesi: L'introduzione e l'attivazione di BitLocker migliorano notevolmente la sicurezza dei dati aziendali. Questa check-list e il modulo baramundi Defense Control vi aiuteranno a completare il rollout in modo efficiente ed efficace.