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**

Sempre aggiornati – 5 trucchi per una gestione efficiente degli aggiornamenti

Oltre al phishing, le vulnerabilità non aggiornate sono il metodo più comune tramite il quale vengono compromessi i sistemi IT. Anche se il numero di vulnerabilità aumenta di giorno in giorno, è possibile risolvere facilmente questo problema con gli strumenti giusti e seguendo 5 semplici trucchi.

Identificare l'hardware e il software critici

Valuta costantemente i rischi attuali, a partire dai sistemi mission-critical e dalle applicazioni software essenziali per mantenere la produttività dei diversi reparti. Assegna la priorità alla distribuzione di patch e aggiornamenti.

Test pre-deployment

Gli aggiornamenti e le patch possono contenere bug o introdurre incompatibilità impreviste. Testa innanzitutto le patch e gli aggiornamenti su dispositivi e configurazioni rappresentativi per individuare e correggere i problemi prima di una distribuzione più ampia. In questo modo si ridurranno al minimo gli arresti anomali e i rallentamenti degli endpoint.

Implementare anelli di distribuzione

Crea anelli di endpoint o gruppi logici di dispositivi che riceveranno gli aggiornamenti applicabili contemporaneamente in una sequenza graduale di anelli sempre più grandi. Gli anelli con gli endpoint più importanti riceveranno per primi le patch o gli aggiornamenti.

Automatizzare!

L'aggiornamento manuale richiede molto tempo e lavoro ed è soggetto a errori. La chiave è l'automazione. I rollout di patch e aggiornamenti possono essere configurati nel dettaglio e distribuiti. Le soluzioni UEM avanzate forniscono inoltre ampie librerie di pacchetti di patch pre-testate pronte per essere distribuite.

Gestire e isolare i rischi

Non tutti gli aggiornamenti e le patch possono o devono essere distribuiti immediatamente. Oltre agli aggiornamenti difettosi o incompatibili, esistono sistemi legacy che non possono essere modificati facilmente, soprattutto quelli utilizzati in ambienti di produzione in tempo reale. Potrebbe essere necessario isolarli, disconnetterli o metterli in sicurezza con altre misure.

In sintesi: Una gestione efficiente degli aggiornamenti è fondamentale per evitare vulnerabilità non aggiornate. L'identificazione dei sistemi critici, la verifica degli aggiornamenti, il concetto di anello, l'automazione della sicurezza e la gestione equilibrata del rischio sono strategie centrali che possono essere implementate in modo affidabile dalla baramundi Management Suite.