Gestione delle patch nelle PMI

Gli aggiornamenti sono un metodo efficace per gestire le falle nella sicurezza dei sistemi digitali complessi. Una buona gestione delle patch permette di installarli senza difficoltà anche nelle PMI.

Punti principali:

- Dedicate regolarmente alla manutenzione dei sistemi fasce orarie non coincidenti con la produzione.
- Ottenete gli aggiornamenti della sicurezza solo da fonti attendibili.
- Verificate l'efficacia e gli «effetti collaterali» degli aggiornamenti prima di installarli sui sistemi produttivi.
- Stabilite un piano per la distribuzione degli aggiornamenti sui vostri sistemi.
- Tenete pronto un backup aggiornato e un piano di fallback per l'eventualità che l'aggiornamento non funzioni a dovere.
- Documentate i lavori di manutenzione eseguiti sui sistemi.

Aggiornamenti della sicurezza

Lo sviluppo dei sistemi informatici è sempre più incalzante, con un aumento costante delle funzioni delle applicazioni e la tendenza ad abbreviare i cicli di vita di hardware e software. I produttori puntano a tenere il passo distribuendo le loro novità in tempi brevi mediante aggiornamenti (update).

Nel contesto delle PMI è possibile procedere in un certo senso con i piedi di piombo, non essendo sempre possibile applicare efficientemente al processo operativo ogni singola novità. Una grande eccezione in questo senso è costituita dagli **aggiornamenti della sicurezza**, che andrebbero installati il prima possibile.

Ogni sistema complesso presenta errori o punti deboli nascosti che nella maggior parte dei casi sfuggono innocuamente all'attenzione per lungo tempo. Una volta scoperti, tuttavia, diventano falle da valutare con attenzione (in informatica vengono chiamate **vulnerabilità**) e marcano l'inizio di una corsa contro il tempo.

Da un lato, infatti, gli hacker iniziano a cercare modi per sfruttarle queste falle per i loro scopi e sviluppare i cosiddetti **exploit**. Se ci riuscissero, potrebbero ad esempio accedere senza autorizzazione a sistemi e dati.

Allo stesso tempo, i produttori si danno da fare per risolvere i problemi nel minor tempo possibile mediante aggiornamenti della sicurezza o patch, inibendo così eventuali exploit nuovi o già diffusi.

La gestione delle patch

Come regola generale, gli aggiornamenti della sicurezza andrebbero quindi installati con la maggiore rapidità e capillarità possibile. In una postazione di lavoro privata e individuale l'operazione è semplice, ma in una PMI le difficoltà non sono poche. Ecco perché si rende necessaria una procedura ordinata inserita in un apposito processo.

Per l'installazione degli aggiornamenti della sicurezza è necessario seguire questi passaggi:

- identificazione dei sistemi interessati e dei relativi aggiornamenti;

- ottenimento degli aggiornamenti della sicurezza da una fonte attendibile, anche e in particolare per i sistemi privi di accesso diretto a Internet;
- verifica preliminare, su sistemi non critici, dell'efficacia e degli «effetti collaterali» degli aggiornamenti;
- distribuzione degli aggiornamenti in base al tipo di sistema e pianificazione dell'installazione al di fuori degli orari di produzione;
- per i sistemi critici: pianificazione di soluzioni di ripiego temporanee e scenari di fallback;
- documentazione delle modifiche apportate.

Trattandosi di un processo che avviene in forma continuativa, è consigliabile inserire in calendario la manutenzione dei sistemi con una periodicità regolare e fissa. Ciò consentirà di accumulare, testare e predisporre gli aggiornamenti della sicurezza per un certo periodo di tempo, posticipandone comunque l'installazione alla data prevista.

Le procedure di gestione delle patch consistono nell'ottenere, testare e installare gli aggiornamenti software al fine di risolvere le vulnerabilità di sistemi operativi e applicazioni.

Per saperne di più

L'**identificazione dei sistemi interessati e dei relativi aggiornamenti** dipende da numerosi fattori. In primo luogo l'hardware, per il quale occorre tenere aggiornati in particolare il firmware e i driver. A seguire il sistema operativo e i programmi installati, per i quali va costantemente verificata la disponibilità di aggiornamenti.

Per i sistemi dotati di accesso diretto a Internet esistono soluzioni di controllo automatizzate che stilano periodicamente un inventario dell'hardware e del software e cercano online gli aggiornamenti disponibili. Nelle PMI questi programmi dovrebbero svolgere al massimo una funzione di supporto: sono fortemente sconsigliate le installazioni di aggiornamenti non presidiate e controllate da un tecnico.

Anche l'**ottenimento degli aggiornamenti della sicurezza** può essere un'attività sensibile, perché non sempre gli aggiornamenti più facili da trovare in Internet sono «originali»: vi è infatti il rischio che il presunto aggiornamento della sicurezza installi invece nel sistema l'exploit. Ove possibile, bisognerebbe quindi affidarsi unicamente ai canali di distribuzione ufficiali dei produttori.

Prima di installare un aggiornamento su un sistema produttivo o addirittura critico, assicuratevi che sia compatibile con il sistema in questione e il contesto d'uso. L'ideale sarebbe **verificare l'efficacia e gli «effetti collaterali»** (cioè conseguenze potenzialmente indesiderate) degli aggiornamenti in un ambiente isolato e non produttivo, anche se nelle PMI spesso non è possibile.

Tuttavia, è consigliabile **distribuire gli aggiornamenti per categorie di sistema**, cominciando ad esempio con quelli meno critici. Solo dopo aver atteso un certo periodo di osservazione ed eseguito alcuni test si potrà procedere con gli altri sistemi.

All'installazione degli aggiornamenti, in particolare nei sistemi critici, andrebbero riservate fasce orarie sufficienti non coincidenti con la produzione. Non bisognerebbe dimenticare di prepararsi con backup (https://www.ebas.ch/it/backup-dei-dati-nelle-pmi/) e **soluzioni di ripiego in caso di fallback** all'eventualità che l'aggiornamento non si installi correttamente.

Le azioni eseguite nel processo di aggiornamento andrebbero annotate in modo comprensibile in apposita **documentazione** che offrirebbe indicazioni sulla causa di eventuali problemi riscontrati successivamente.