White Paper

L’importanza di patch e aggiornamenti

L'IT AL CENTRO DELLE AZIENDE

Negli ultimi anni il modo di lavorare delle aziende è cambiato radicalmente, ne siamo tutti testimoni.

Sotto la spinta dell'innovazione tecnologica sono mutati strumenti, processi e abitudini di ogni tipo di azienda: produzione, servizi, retail… nessuna fa eccezione.

Come conseguenza di tutto **ciò la tecnologia si è pian piano presa un ruolo di sempre maggior rilievo all'interno delle organizzazioni**, tanto che si è arrivati al punto in cui **se gli strumenti informatici non funzionano è impossibile generare fatturato per le imprese**.

Possiamo quasi affermare che per tante imprese un PC è più importante di un ufficio: pensa a quante aziende sono state in grado (e lo sono tuttora) di continuare a essere operative anche quando i loro uffici erano inaccessibili a casa dei lockdown da Covid-19.

E **cosa accadrebbe alla tua azienda se domani PC, server e connettività fossero fuori uso?** Con ogni probabilità **ti ritroveresti a pagare il personale e i costi infrastrutturali e allo stesso tempo non riusciresti a produrre, vendere o fatturare nulla**.

Ma cosa può portarti a una situazione del genere?

Sicuramente alluvioni, incendi, terremoti o altri **disastri naturali** sono tra le cause più evidenti e "rumorose".

E non esiste un incantesimo in grado di rimettere in funzione l'infrastruttura IT in uno schiocco di dita, qui l'arcano non c'entra nulla: **ci vuole un piano di disaster recovery** ben studiato e supportato dalla tecnologia adeguata. Questo tipo di tecnologia è in grado di rimetterti in condizioni di lavorare in tempi ragionevoli.

Di che tempi sto parlando? Dipende dalla soluzione tecnologica in uso e dall'efficacia del piano di ripartenza, oltre che da quanto sei disposto a investire per la protezione dei tuoi sistemi.

Ma non voglio soffermarmi troppo su questo tema: **ti invito a contattare il tuo fornitore IT per verificare quale possa essere la soluzione più adatta alle tue esigenze** e per preparare un piano di ripartenza su misura per te.

OLTRE I DISASTRI NATURALI: IL CYBER CRIME

Oltre ai disastri citati in precedenza **esiste un altro tipo di disastro**, ben più subdolo e silenzioso e che non ha nulla a che vedere con le bizze di madre natura.

Ci sono, infatti, **organizzazioni di cyber criminali che mirano a colpire aziende come la tua per ottenere dei profitti**. Si tratta di un business, se così vogliamo definirlo, che globalmente muove miliardi di euro ogni anno ed è in costante crescita.

I cyber criminali spesso **puntano a far girare nei sistemi delle aziende dei virus chiamati "ransomware"** o "cryptovirus" **che sono in grado di rendere illeggibili e inutilizzabili tutti i file e i dati** salvati su PC e server. Questo, di fatto, rende impossibile l'utilizzo di qualsiasi strumento informatico e l'accesso a database, CRM, software e file utilizzati per lavorare.

Dopo aver cifrato tutti i dati dell'azienda vittima, **i cyber criminali richiedono un compenso in denaro per sbloccare i sistemi IT** e renderli nuovamente utilizzabili.

L'azienda vittima può scegliere se pagare questa cospicua somma di denaro, tuttavia non ha nessuna garanzia che i dati verranno resi leggibili in seguito al pagamento: dopo tutto stiamo parlando di cyber criminali, non di boy scout.

Ti stai chiedendo **perché questi cyber criminali vogliono colpire proprio la tua azienda?**

Non devi immaginare un'organizzazione segreta di hacker russi che studia un colpo per mesi per attaccare il centro estetico del tuo paese.

I cyber criminali, infatti, prendono di mira chiunque: a volte studiano il bersaglio prima di attaccarlo, spesso pescano "a strascico" facendo partire delle **vere e proprie campagne email malevole** su un gran numero di contatti simultaneamente.

I piccoli hacker possono anche facilmente trovare in rete, nel dark web, dei virus "pronti all'uso" da poter veicolare secondo le modalità più disparate.

Molte volte questi attacchi **si nascondono dietro file apparentemente innocui**, come una (finta) fattura o un documento di un sedicente corriere.

I malviventi, all'interno di queste campagne email, generalmente fanno leva su sconti, pubblicità o altri argomenti a cui siamo tutti sensibili, con lo scopo di "farti cliccare". **Oppure si fingono un tuo fornitore o uno dei grossi brand da cui tutti comprano qualche prodotto o servizio**, come Amazon, Google, Facebook, Microsoft e così via.

Potrebbe quindi bastare un click su una di queste email per installare un ransomware su tutti i tuoi sistemi.

Per funzionare, molto spesso, questi file malevoli **sfruttano quelle che vengono definite falle di sicurezza**.

Ma **come si creano i "buchi di sicurezza"?**

Per prima cosa è molto importante affidare la sicurezza della tua infrastruttura IT a un professionista competente. Questi, attraverso l'uso di strumenti di sicurezza e protezione, farà in modo che la tua rete possa difendersi da alcune minacce informatiche.

Ma purtroppo **questo non è sufficiente a mettere al sicuro i tuoi sistemi IT da tutti pericoli**.

VULNERABILITÀ E PATCH

Gli strumenti che usiamo tutti i giorni per lavorare **sono dei programmi creati da esseri umani**. Si tratta di prodotti, quindi, **non esenti da difetti e problemi**: sono queste le falle che spesso sfruttano i cyber criminali.

Quando uno di questi difetti viene scoperto, **il fornitore** del software **si preoccupa di rilasciare un aggiornamento correttivo** quanto prima attraverso quelle che vengono definite "**patch**".

Nessuno fa eccezione: anche le più grandi e famose software house rilasciano in continuazione delle patch a causa di bug ed errori presenti nei propri prodotti.

E i cyber criminali non se ne stanno con le mani in mano: cercano furbescamente di sfruttare questi errori a proprio vantaggio per fare breccia nei sistemi IT, creare virus ad hoc e compiere le malefatte elencate in precedenza.

Qui abbiamo **due possibili scenari**:

- **gli hacker si accorgono di una vulnerabilità e iniziano a sfruttarla**: questo porta alcune aziende a cadere vittima dei loro attacchi prima che la vulnerabilità venga sistemata tramite una patch;
- **i produttori di software si accorgono dell'errore** e rilasciano prontamente una patch.

A questo punto potresti pensare che solo il primo scenario preveda delle vittime e che queste siano in numero limitato, visto che i produttori di software rilasciano quanto prima degli aggiornamenti correttivi.

Sbagliato! Nei casi di gravi vulnerabilità **entrambi i casi prevedono un gran numero di vittime**.

Vediamo insieme come mai.

L'IMPORTANZA DEGLI AGGIORNAMENTI

Perché non basta che il vendor di turno rilasci una patch per essere al sicuro?

Le patch vengono rilasciate dal produttore, ma poi **devono essere installate perché risolvano il problema sui sistemi impattati**. E indovina un po'? **La maggior parte delle aziende non installa le patch tempestivamente**.

Quindi, **quando un produttore di software che rilascia una patch sta**, di fatto, **annunciando al mondo che il suo software presenta un problema**.

Di conseguenza, anche se la vulnerabilità era fino ad allora ignota ai **cyber criminali**, questi **possono prontamente mettersi all'opera per sfruttarla** e colpire quante più aziende possibile.

Per tutto il lasso di tempo che intercorre tra la pubblicazione della patch correttiva e l'installazione di tale patch, quindi, la tua azienda corre dei rischi. Più passa il tempo, più i rischi aumentano!

Considera che, secondo un report del Ponemon Institute, **il 60 % delle violazioni di dati**, o data breach, **avviene sfruttando vulnerabilità per le quali sono disponibili delle patch**, ma queste non sono state installate.

Un'altra brutta abitudine delle aziende è quella di **utilizzare versioni** di applicazioni e sistemi operativi che **non sono più supportate del vendor** che le ha prodotte. Se il vendor smette di supportarle significa che non rilascia più patch correttive né aggiornamenti di nessun tipo: è come giocare alla roulette russa informatica!

Per cui è estremamente pericoloso se un utente, ignaro degli aspetti relativi alla sicurezza, pensa che il suo PC con Windows 7 vada bene solo perché riesce lavorare su un foglio di calcolo o a utilizzare le applicazioni che gli servono per lavorare.

In questo caso **occorre acquistare una versione del software più recente**, e dunque supportata dal produttore, se non si vuole rischiare di ritrovarsi nei guai.

Ma le patch non servono solo a risolvere problematiche di sicurezza. Infatti vengono rilasciati aggiornamenti anche per:

- **risolvere blocchi o errori** che si presentano durante l'utilizzo dei software;
- **migliorare le performance** del prodotto;
- **aggiungere nuove funzionalità**.

Quindi, installando gli aggiornamenti, ci si ritrova a usare un tool più performante, meno propenso a bloccarsi e "crashare", con funzionalità aggiuntive e, non dimentichiamolo, più sicuro.

LA SOLUZIONE PER MITIGARE I RISCHI

Come avrai avuto modo di capire **l'unica soluzione veramente efficace** per mitigare i rischi dovuti alle vulnerabilità **è installare le patch**. Ma non devi preoccupartene da solo, non è il tuo lavoro!

Il mio consiglio è quello di **chiedere aiuto al tuo fornitore di servizi IT**. Quest'ultimo **potrà effettuare un'analisi completa** dei tuoi sistemi per capire qual è la situazione attuale e in quali aree intervenire con degli aggiornamenti.

Ma non solo: potrà **elaborare un piano di installazione delle patch che capisca quali macchine sono più critiche rispetto ad altre in quale modo debbano essere installati gli aggiornamenti**. Tutte queste operazioni potranno essere tenute sotto controllo tramite appositi sistemi di monitoraggio.

Le operazioni di aggiornamento periodico potranno poi essere effettuate da remoto, **in modo "invisibile"**, così che tu e i tuoi colleghi non dobbiate interrompere il vostro lavoro per permettere a un tecnico di intervenire fisicamente su PC e server.

Per concludere, una volta riconosciuta l'importanza delle patch, è importante affidarsi a un fornitore che conosca la tua infrastruttura IT e sappia quando è il momento più opportuno per installare un aggiornamento e con quali modalità.

Glossario

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

Patch – File di aggiornamento che ha lo scopo di correggere uno o più errori che causano un non corretto funzionamento di un'applicazione o di un sistema operativo.

Ransomware – Un particolare tipo di malware che crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete) che diventano così inaccessibili a meno di non pagare un riscatto per ottenere la chiave di decifrazione necessaria. Non sono rari i casi in cui anche la disponibilità di questa chiave non consenta il ripristino corretto dei sistemi, con gravi conseguenze per le aziende.

Data breach – una violazione della sicurezza informatica che porta alla copia, diffusione o furto di dati da parte di individui non autorizzati.