Protezione antivirus nelle PMI

La protezione antivirus fa parte della dotazione di base di ogni azienda, dato che il software dannoso rappresenta una minaccia in rapida crescita nel mondo digitale – anche per le PMI. La soluzione migliore consiste nel combinare sistemi tecnologici e una condotta consapevole.

Punti principali:

- Definite e implementate nella vostra PMI un **processo di protezione antivirus**.
- Create uno schema generale dei **percorsi di ingresso e diffusione** del malware nella vostra impresa.
- In uno **schema di protezione antivirus**, definite in quali punti della rete il controllo risulta più efficiente.
- **Sensibilizzate** il vostro personale verso i pericoli posti dal software dannoso.

Il processo di protezione antivirus

Al giorno d'oggi sono molti i produttori che offrono eccellenti sistemi antivirus adattabili alle più svariate esigenze e configurazioni di rete delle PMI. Il primo passo, tuttavia, consiste nell'eseguire un'analisi preliminare per valutare la soluzione ottimale che in seguito si attuerà a regola d'arte.

Ma non finisce qui: proprio come la criminalità informatica e il malware sono in continua evoluzione, così anche le misure di difesa richiedono una cura e un aggiornamento continui. Per esempio, la protezione antivirus va sempre aggiornata con le definizioni di virus più recenti.

Ecco perché va stabilito un processo di protezione antivirus che garantisca sia il corretto monitoraggio dei flussi di dati e la rilevazione/rimozione del malware (https://www.ebas.ch/it/infezione-da-malware/) , sia la manutenzione dei sistemi. Altrettanto importante è che il processo preveda una periodica sensibilizzazione del personale verso questo tipo di minacce.

I canali di diffusione

Le reti delle PMI sono caratterizzate da un continuo aumento della complessità. Quasi ogni giorno si implementano nuove soluzioni software, si creano nuove connessioni dati o si migliora l'infrastruttura. I criminali informatici sfruttano questa complessità per trovare e sfruttare nuovi percorsi di ingresso e diffusione per il loro malware.

Alla base dello schema di protezione antivirus (#concept) deve perciò esserci l'identificazione, con il maggior dettaglio possibile, di tali canali. È utile in questo senso studiare alcuni scenari:

1. «Come e dove un hacker potrebbe introdurre del malware nella rete?»
2. «Come potrebbe poi diffondersi il malware sulla rete?»

In particolare, per introdurre software dannoso spesso si usano questi canali:

- connessioni Internet, WLAN e VPN
- allegati di mezzi di comunicazione, come la posta elettronica

- dispositivi mobili di collaboratori e ospiti
- applicazioni di desktop remoto (RDP) e terminal server
- scambio di supporti di dati fisici
- ambienti IoT non sufficientemente protetti

Una volta raggiunta la rete interna, il malware può diffondersi sfruttando le falle di sicurezza, e attivarsi e scatenare il suo effetto nocivo, per esempio, con un gesto poco accorto di un collaboratore. In tali casi, è importante contenere i danni e prevenire una diffusione su larga scala.

Lo schema di protezione antivirus

Sulla base dei percorsi di ingresso e diffusione identificati si possono determinare i nodi della rete in cui le misure di protezione mostrano la massima efficienza.

Considerando la loro esposizione, un occhio di riguardo dovrebbe andare alle connessioni a Internet in entrata e in uscita, da controllare per rilevare la presenza di malware. Questa operazione può avvenire nel firewall o sui server proxy e di comunicazione. È opportuno notare che i contenuti devono essere controllati prima di essere crittografati o dopo che sono stati decrittografati.

A questo proposito anche i dispositivi mobili di collaboratori e ospiti pongono un grande pericolo, perché spesso vengono utilizzati anche in ambienti non protetti. Pertanto, non dovrebbero mai avere accesso alla rete interna prima di un'adeguata verifica. Lo stesso ragionamento vale anche per le connessioni VPN dall'esterno, p. es. per il personale in home office (https://www.ebas.ch/it/5-buone-regole-per-lavorare-in-sicurezza-da-casa/) . In questo caso è utile che i dispositivi vengano controllati da un software antivirus gestito centralmente.

Infine, anche i dispositivi fissi a cui però si collegano supporti dati esterni devono essere dotati di un'adeguata protezione antivirus.

L'intero sistema antivirus e la sua configurazione vanno stabiliti nello schema di protezione.

Suite antivirus per le aziende

Numerosi produttori offrono soluzioni antivirus adatte anche alle reti più complesse. Le operazioni di roll-out, configurazione e manutenzione della protezione si possono così gestire centralmente per tutte le piattaforme e le sedi. In questo modo, si può garantire che la politica di sicurezza della PMI possa essere rispettata non appena un dispositivo si connette alla rete.

Le statistiche sulla criminalità informatica parlano chiaro: negli ultimi anni gli attacchi di malware con conseguenze dannose sono aumentati in modo significativo. Il ransomware, in particolare, rappresenta una grave minaccia per le PMI.