Suggerimenti per le PMI

Solitamente le reti aziendali sono più difficili da proteggere dagli attacchi della criminalità informatica rispetto a quelle private. Questo perché sono più complesse e l'impatto economico di eventuali avarie o malfunzionamenti è maggiore. Ciò rende indispensabile l'adozione di provvedimenti inattaccabili per ridurre i rischi.

Punti principali:

- Per valutare i rischi e adottare i giusti provvedimenti consultate **le linee guida e i promemoria** pubblicati da istituzioni affermate.
- Identificate quali **processi, sistemi e dati** sono i più preziosi per la vostra azienda e gestiteli per primi.
- Per aumentare la sicurezza dell'informazione nella rete aziendale valutate **misure** sia **tecniche** che **organizzative**
- Definite **responsabilità, competenze e interlocutori** per le questioni relative alla sicurezza.

Le reti aziendali sono solitamente strutture complesse, spesso evolutesi in un lungo periodo di tempo, con numerose interfacce e flussi di dati da e verso clienti e partner commerciali. Anche brevi interruzioni, se non complete avarie, dell'infrastruttura producono non di rado gravi conseguenze economiche per l'impresa. Ciò fa sì che le PMI siano in generale più esposte ai rischi che rappresenta la criminalità informatica rispetto ai privati.

Per aumentare la resistenza delle PMI a tali pericoli – la cosiddetta resilienza ITC – e ridurre al minimo i rischi connessi, occorre prevedere idonee misure di protezione. La complessità e la portata, tuttavia, ne determinano solitamente un elevato dispendio di denaro e risorse. Ne consegue che un'attenta ponderazione dei fattori in gioco riveste la massima importanza.

Avvalersi di linee guida e promemoria

Come deve affrontare questo importante compito una PMI? E come può avere la certezza di non trascurare nulla?

Non poche istituzioni di chiara fama si sono poste questi interrogativi e hanno studiato a fondo le modalità di attuazione di misure di protezione ICT con specifico riferimento alle PMI. Con il tempo si è così giunti alla pubblicazione di tutta una serie di linee guida e promemoria che presentano procedure tanto efficienti quanto efficaci. Non si potrà mai consigliare a sufficienza l'uso di tali strumenti.

Come introduzione all'argomento, si può citare il «Promemoria sulla sicurezza delle informazioni per le PMI» (https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html) dell'UFCS. Si tratta di un promemoria molto compatto che si rivolge esplicitamente alle PMI svizzere e si propone di aiutarle a incrementare la sicurezza dell'informazione nei loro sistemi e nelle loro reti aziendali.

Identificare processi, sistemi e dati

Dove e con cosa iniziare? Quali processi, sistemi o dati dovrebbe gestire per primi una PMI?

Alla base della risposta a questa domanda si trova un'analisi dei rischi (semplificata). Si tratta di identificare i processi, i sistemi e i dati di rilevanza specifica per la catena di creazione del valore dell'azienda e di valutarne la

suscettibilità ai pericoli ICT.

Adottare misure tecniche

Le misure tecniche di protezione rappresentano la prima linea di difesa contro i pericoli della criminalità informatica. L'elenco dei provvedimenti possibili è lungo. Ma quali sono le misure giuste?

La questione dipende in larga misura dalle minacce specifiche che incombono sulla singola PMI. Tuttavia, alcune misure tecniche si possono considerare generalmente valide e rientrano quindi nella protezione di base di ogni PMI. Tra queste vi sono indubbiamente:

- Esecuzione regolare di copie di sicurezza dei dati (backup) (https://www.ebas.ch/it/backup-dei-dati-nelle-pmi/)
- Installazione e gestione di un sistema antivirus (https://www.ebas.ch/it/protezione-antivirus-nelle-pmi/) aggiornato
- Installazione di aggiornamenti (https://www.ebas.ch/it/gestione-delle-patch-nelle-pmi/) periodici della protezione

Adottare misure organizzative

Le misure tecniche da sole non possono garantire una protezione completa. Vanno sempre integrate con misure organizzative.

Anche la lista delle misure organizzative è cospicua. In particolare, occorre sottolineare i punti seguenti:

- Sensibilizzazione e formazione regolare del personale
- Definizione di una politica rigorosa in materia di password (https://www.ebas.ch/it/politica-sulle-password-per-pmi/)
- Processi sicuri per le applicazioni critiche (p. es. principio del controllo incrociato, a più livelli, per le applicazioni dell'e-banking)

Definire responsabilità, competenze e interlocutori

Chi è responsabile del backup dei dati? Chi è competente per l'installazione degli aggiornamenti della protezione? A chi si devono rivolgere i dipendenti che sospettano un'infezione da malware, per esempio?

Per garantire il buon funzionamento delle procedure, è necessario non soltanto definire ma anche far conoscere al personale le responsabilità, le competenze e gli interlocutori in materia di sicurezza ICT.

Con una piattaforma informativa adeguata si può promuovere un accesso a bassa soglia agli uffici giusti. Ciò permette di ridurre i tempi di risposta agli incidenti e aumentare il tasso di segnalazione.

Le PMI svizzere sono sempre più spesso oggetto di attacchi da parte della criminalità informatica, in alcuni casi con gravi conseguenze per l'impresa colpita. Per questo è indispensabile adottare provvedimenti per ridurre i rischi.