economiesuisse

Pericoli per le PMI: aumento dell'efficienza digitale nel cyberspazio

Per molte delle nostre aziende, l'uso di strumenti digitali è fondamentale per lo sviluppo dei loro modelli commerciali. La sicurezza informatica non deve tuttavia essere dimenticata. La negligenza in questo settore può avere gravi conseguenze per l'azienda e per i suoi partner commerciali.

Chiunque associ il termine "digitalizzazione dell'economia" solo a grandi imprese basate sulla tecnologia o a start-up dinamiche della Crypto Valley dimentica che oggi praticamente ogni impresa trae profitto dal progresso digitale. Numerose facilitazioni offerte dalle nuove tecnologie sono diventate indispensabili, soprattutto nella vita quotidiana delle PMI locali, che si tratti di falegnamerie, fiduciarie o negozi di biciclette.

Questo non vale solo per i PC per la contabilità o l'elaborazione di testi. I progetti di costruzione vengono creati e inviati elettronicamente, l'addetto alle vendite inoltra l'ordine direttamente sul tablet, le materie prime vengono acquistate tramite una piattaforma e il dispositivo di analisi del laboratorio scarica gli aggiornamenti direttamente da Internet. Altri imprenditori sono pienamente impegnati negli strumenti digitali. Le parole chiave sono qui “nomade digitale” e “produzione additiva”.

Osservando alcuni dei sondaggi più recenti, si ha l'impressione che molte aziende del nostro paese suppongano di non avere nulla a che fare con la digitalizzazione. Quando si affronta questo argomento, esse rispondono che lo sviluppo tecnologico non le riguarda direttamente. Come si spiega questa apparente contraddizione?

Molti usi delle moderne tecnologie si sono lentamente insinuati nella vita quotidiana delle nostre PMI anche se non rientravano in una strategia di digitalizzazione mirata.

Pertanto, non tutti gli sviluppi sono stati di gran lunga il risultato di una decisione consapevole e spesso sono stati indotti da altre misure, come ad esempio il passaggio a un nuovo telefono, la gestione dei documenti digitali o l'uso regolare di Internet. Gli strumenti elettronici connessi sono così comuni, soprattutto nelle nostre PMI di oggi, che spesso non sono più percepiti come tali. Ed è proprio qui che risiede il pericolo maggiore dal punto di vista della sicurezza informatica.

Nuove opzioni tecnologiche, nuove forme di criminalità

La digitalizzazione e l'interconnessione dei sistemi (numerosi strumenti, telecamere di sorveglianza o elettrodomestici da cucina sono già collegati a Internet) ci rendono vulnerabili a un livello completamente nuovo. Perché, soprattutto nello spazio digitale, le persone o le organizzazioni con macchinazioni criminali si stanno muovendo. Gli attacchi possono essere effettuati in modo anonimo e con poco sforzo direttamente alle nostre aziende da qualsiasi parte del mondo. I cybercriminali non si curano dei confini nazionali.

Essi colpiscono dove il bottino è facile, cioè dove si può guadagnare molto con relativamente poco sforzo. Ad esempio, anche le PMI svizzere sono vittime di criminali specializzati. L'attenzione è particolarmente rivolta a coloro che non si occupano di questioni di sicurezza e non adottano misure difensive adeguate.

La digitalizzazione ha quindi un rovescio della medaglia: nuove forme di criminalità. I dati possono essere rubati o modificati via Internet, i sistemi danneggiati e le aziende ricattate. Ciò apre nuovi pericoli che non esistevano ancora nel mondo analogico. Tuttavia, è possibile prevenire un gran numero di attacchi criminali. Come nel mondo fisico, un'azienda deve pensare a come proteggersi da questi criminali. Se si trascura la sicurezza, le semplificazioni tecniche diventano rapidamente un pericolo esistenziale per una PMI. Molti utenti, aziende e privati ignorano i pericoli che possono derivare dall'uso delle nuove tecnologie.

Uno studio condotto dalla Scuola universitaria professionale di Lucerna in collaborazione con l'Associazione delle PMI, la Segreteria di Stato dell'economia (SECO), l'Associazione svizzera dei quadri (ASQ) ed economiesuisse lo conferma: le imprese locali non sono sufficientemente preparate alle minacce nel cyberspazio. Il 40% delle aziende intervistate ha dichiarato di essere stato recentemente colpito da attacchi sotto forma di virus come malware o phishing-mail. Nonostante il pericolo concreto, le imprese non sono in grado di reagire adeguatamente agli attacchi. Uno dei motivi è che molte PMI non sanno come affrontare il tema della sicurezza delle informazioni.

La consapevolezza dei pericoli cresce, ma ...

Lo studio conclude che la sensibilità alla sicurezza informatica è generalmente aumentata. "Digitalizzazione, robotica e automazione" sono divenute, per i team di dirigenti, il secondo tema più importante, subito dopo l'aumento dell'efficienza. Circa il 78% delle PMI intervistate ha inoltre dichiarato che la sicurezza

informatica è diventata più importante negli ultimi tre anni. Anche se le PMI stanno ora ampiamente discutendo di questioni di sicurezza informatica, è necessario intervenire. Lo studio rileva inoltre che meno della metà delle aziende intervistate rivede regolarmente le proprie misure di sicurezza. Anche le guide su come affrontare le minacce nel cyberspazio sono utilizzate raramente. Lo stesso vale per la formazione continua. Sono pertanto necessarie strategie per reagire ai crescenti pericoli derivanti da Internet.

Spesso ci vuole poco per migliorare in modo significativo la sicurezza in un'azienda. L'attenzione rivolta alla sicurezza informatica nelle aziende interessate, ma anche tra i partner commerciali, i fornitori e i clienti, ha consentito di limitare massicciamente i casi di abuso. Un rischio per la sicurezza può diventare un vero e proprio inibitore del business e persino mettere in pericolo l'azienda nel suo complesso, insieme ai suoi partner commerciali. Pertanto, la sicurezza e i relativi costi devono essere presi in considerazione nel Business Case fin dall'inizio. L'obiettivo deve essere che ogni impresa, grande o piccola che sia, possa sviluppare un concetto di sicurezza adeguato che offra sufficienti garanzie e al tempo stesso mantenga una buona capacità operativa.

La responsabilità inizia dall'individuo

Così come siamo responsabili della sicurezza della nostra casa contro i furti con scasso, è in primo luogo responsabilità di ogni azienda proteggersi dalle minacce nel cyberspazio. La risposta a queste minacce non può essere prescritta dallo Stato, al contrario. I sistemi decentralizzati ed eterogenei sono più resistenti nel settore della sicurezza informatica rispetto ai sistemi progettati a livello centrale. Soprattutto quando si tratta di affrontare sfide e crisi inaspettate. Nel caso in cui occorrano delle soluzioni settoriali, l'economia stessa deve affrontarle di petto. Può prevedere norme minime, nel senso di raccomandazioni, rafforzando notevolmente la cybersicurezza.

Delle guide chiare e comprensibili possono fungere da aiuti. Tali standard minimi consentirebbero inoltre alle PMI di beneficiare del know-how delle grandi imprese e di evitare asimmetrie settoriali in ambito informatico. Lo Stato fornisce il suo contributo anche promuovendo tali norme di sicurezza e vegliando ad un'applicazione equilibrata nei confronti della legislazione internazionale. In caso di crisi, vale a dire in caso di attacco su larga scala, è indispensabile una chiara ripartizione dei compiti tra il settore privato e lo Stato.

Mediante mezzi di incitamento adeguati, lo Stato dovrebbe pertanto vegliare affinché gli incidenti informatici siano segnalati. Ciò aumenta la trasparenza, abbassa il livello di pericolo e contribuisce a ridurre l'impatto di tali attacchi su terzi. La popolazione, l'economia, l'amministrazione e la politica devono essere sensibilizzate in modo adeguato per migliorare la comprensione dei rischi informatici. La sicurezza nel cyberspazio è un classico compito collaborativo. Tutto è collegato in rete e i sistemi si influenzano a vicenda. Ciò significa anche che ognuno deve fare la propria parte per aumentare la sicurezza. Richiedere un intervento dello Stato, come pure il fatto di ignorare la propria vulnerabilità tecnologica, non serve a nulla.

Articolo apparso in tedesco nella rivista IT business.