Dieci consigli per sventare cyberattacchi

Una cyberaggressione può colpire qualunque impresa. Alcune misure cautelari Le consentono tuttavia di proteggersene.

Salvi i Suoi dati
Definisca una procedura che regoli periodicamente la salvaguardia dei dati. Calcoli quante giornate di perdita dati la Sua impresa potrebbe eventualmente sopportare e delocalizzi una copia supplementare del Suo backup separatamente (offline) e fuori sede (offsite). Si accerti di conservare una versione precedente del backup per un periodo di alcuni mesi.

Regoli la gestione delle informazioni aziendali
Valuti attentamente quali informazioni siano da pubblicare ad esempio sul proprio sito web o sui media sociali. Nessuna informazione riservata andrebbe trasmessa in linea di massima attraverso canali anonimi come il telefono o la posta elettronica.

Sensibilizzi i Suoi collaboratori attorno alla gestione delle e-mail
Diffidi di link o allegati in e-mail di mittenti sconosciuti. Non rifugga da richieste di ulteriori spiegazioni se qualcosa nell'e-mail Le sembra insolito o sospetto e raccomandi ai Suoi collaboratori una equivalente e adeguata cautela.

Utilizzi password sicure
La lunghezza minima di una password dovrebbe essere di almeno dodici caratteri e comprendere sia lettere sia numeri e caratteri speciali. Punti sempre quando possibile sull'autentificazione a due fattori. Eviti in ogni caso l'utilizzo ripetuto della stessa password! Si avvalga invece di un password manager e generi una propria password per ogni applicazione.

Regoli la protezione di accesso ai dati
I collaboratori non dovrebbero generalmente disporre di diritti da amministratori.

Usi un computer separato per i pagamenti
Per i pagamenti Le converrebbe utilizzare un computer separato con cui non navigare su internet e non ricevere e-mail. Regoli le procedure che riguardano le operazioni di pagamento (per esempio il principio del doppio controllo e la firma collettiva) e discuta possibili misure di sicurezza con la Sua banca.

Esegua gli aggiornamenti di sicurezza
Si assicuri che qualunque computer e server della Sua rete riceva automaticamente tutti gli aggiornamenti di sicurezza.

Protegga la Sua rete
Su ogni computer dovrebbe essere installato un firewall personale. Protegga inoltre la Sua rete aziendale da internet per mezzo di un firewall.

Divida la Sua rete in singole sezioni come ad esempio produzione, personale e contabilità. Non esiste alcun motivo per cui i collaboratori del reparto del personale debbano poter accedere alla sezione degli impianti di produzione.

Protegga l'accesso remoto alla Sua rete aziendale con un'autentificazione a due fattori, oppure impieghi un collegamento sicuro attraverso una rete virtuale privata (VPN).

Installi una protezione antivirus
Si accerti che una protezione antivirus sia installata su ogni computer e vi sia attivato il funzionamento a tempo reale.

Impiego prudente di servizi cloud
Dati sensibili e segreti aziendali non dovrebbero mai essere salvati in chiaro nel cloud.

Particolari sulle misure illustrate li trova nel nostro opuscolo «Impedire la cibercriminalità. Manuale per piccole e medie imprese» oppure su www.melani.admin.ch

In collaborazione con la Polizia cantonale di Berna e MELANI