Guida sulla Sicurezza Informatica per PMI

timenet
connessi sicuri soddisfatti

Sicurezza Informatica per PMI

1. Valutazione dei Rischi della PMI

Ci sono tre aspetti fondamentali da prendere in considerazione.

Identificare tutte le risorse digitali:

Fate un inventario completo di tutti i dati e le informazioni digitali che la vostra azienda possiede o gestisce, anche per terzi. Questo include database Clienti, documenti finanziari, progetti in corso, e qualsiasi altra informazione che, se compromessa, potrebbe danneggiare la vostra attività sia a livello reputazionale che economico. Coinvolgete i responsabili di ogni reparto per assicurarvi di non tralasciare nulla. Se non avete competenze interne, considerate di consultare un esperto di sicurezza informatica. Un vero esperto saprà indirizzarvi in una completa valutazione dei rischi aziendali Online e non.

Analizzare ogni possibile minaccia:

Informatevi sui tipi di minacce più comuni per le PMI del vostro settore. I virus e il malware possono infettare i vostri sistemi attraverso email, siti web compromessi o dispositivi USB infetti. Gli attacchi di phishing, effettuati tramite mail, cercano di ingannare i dipendenti per ottenere accesso a informazioni sensibili. I furti di dati possono avvenire sia dall'interno che dall'esterno dell'azienda. Consultate le risorse online dell'Agenzia per la Cybersicurezza Nazionale (ACN) per informazioni aggiornate sulle minacce attuali.

Valutare il grado d'impatto sulla propria attività:

Per ogni minaccia identificata, stimate il potenziale impatto sulla vostra azienda. Le perdite finanziarie possono derivare da furti diretti, costi di ripristino o multe per violazioni della privacy. I danni alla reputazione possono portare alla perdita di Clienti e difficoltà nell'acquisirne di nuovi. L'interruzione delle operazioni può causare perdite di produttività e mancati guadagni. Considerate di consultare un analista di rischi aziendali per una valutazione più accurata.

2. Protezione dei dispositivi di Sicurezza Informatica e non

Tre aspetti fondamentali da prendere in considerazione.

Mantenere aggiornati tutti i sistemi:

Gli aggiornamenti spesso contengono correzioni di sicurezza cruciali. Fondamentale trovare una figura di fiducia che coordini questo processo aziendale realizzando un programma di aggiornamento mensile, in modo che le persone abbiano un punto di riferimento a cui chiedere per ogni necessità. Utile anche Impostare gli aggiornamenti automatici dove possibile. Per i sistemi operativi, visitate regolarmente i siti ufficiali di Microsoft, Apple o del vostro fornitore Linux. Per il software, controllate le impostazioni di aggiornamento automatico o visitate i siti web degli sviluppatori. Mantenete aggiornato l'antivirus e assicuratevi che esegua scansioni regolari. Se avete un reparto IT, affidategli questa responsabilità; altrimenti, considerate di assumere un consulente IT esterno per gestire questi aspetti.

Integrare un firewall aziendale:

I firewall agiscono come barriera tra la vostra rete e potenziali minacce esterne. Il firewall del sistema operativo è un buon punto di partenza: su Windows, cercate "Windows Defender Firewall" nelle

impostazioni; su Mac, andate su Preferenze di Sistema > Sicurezza e Privacy > Firewall. Per una protezione più robusta, considerate l'acquisto di un firewall hardware, specialmente se avete una rete aziendale di medie dimensioni. Consultate un fornitore di servizi IT locali per consigli su quale firewall hardware sia più adatto alle vostre esigenze, affidarsi a un esperto competente farà anche risparmiare tempo per l'implementazione del firewall.

Crittografare dati sensibili:

La crittografia rende i dati illeggibili a chi non possiede la chiave di decrittazione. Per i file importanti, potete usare software come VeraCrypt (gratuito) o Symantec Endpoint Encryption (a pagamento). Sui dispositivi mobili, attivate la crittografia integrata: su iPhone, è attiva di default se avete un codice di accesso; su Android, andate su Impostazioni > Sicurezza > Crittografia. Se non siete sicuri di come procedere, chiedete assistenza al vostro fornitore di servizi IT o a un consulente di sicurezza informatica.

3. Gestione delle chiavi di accesso

Tre punti salienti da analizzare.

Creazione di Password difficili da scoprire:

Una password forte dovrebbe avere almeno 12 caratteri, includendo maiuscole, minuscole, numeri e simboli. Evitate di rendere facile il lavoro ai cybercriminali quindi niente: nomi, date di nascita o altre informazioni personali. Un metodo efficace è creare una frase "passphrase", come "IlMioCaneMangia71BiscottiAlGiorno!". Incoraggiate i dipendenti a seguire queste linee guida e considerate di implementare una politica aziendale sulle password. Se avete difficoltà a gestire password complesse, il prossimo punto vi sarà d'aiuto.

Integrare l'autenticazione a due fattori:

La 2FA o autenticazione a due fattori aggiunge un livello di sicurezza in più, richiedendo una seconda forma di verifica oltre alla password. Potrebbe essere un codice inviato via SMS, generato da un'app come Google Authenticator, o fornito da un dispositivo fisico come YubiKey. Attivate la 2FA su tutti gli account critici, come email aziendali, sistemi di gestione Clienti e conti bancari. Molti servizi offrono guide passo-passo per attivare la 2FA; se avete dubbi noi come sempre consigliamo di chiedere assistenza al vostro reparto IT o a un consulente di sicurezza.

Abilitare un gestore delle password:

Un gestore di password è un software che memorizza in modo sicuro tutte le vostre password, permettendovi di usare password uniche e complesse per ogni account senza doverle ricordare. Opzioni popolari includono LastPass, 1Password e Dashlane. Questi strumenti possono anche generare direttamentepassword forti per voi. Scegliete un gestore di password con una buona reputazione e recensioni positive. La formazione del personale sull'uso del gestore di password scelto è essenziale per garantire che venga utilizzato correttamente da tutti.

4. Formazione delle risorse aziendali

Tre elementi essenziali da considerare attentamente.

Formazione programmata:

La formazione dovrebbe essere un processo continuo, l'evoluzione degli attacchi informatici è sempre troppo rapida. Organizzate sessioni trimestrali o semestrali che coprano vari aspetti della

sicurezza informatica. Per il phishing, mostrate esempi reali di email di phishing e insegnate ai dipendenti a verificare l'autenticità dei mittenti e dei link. Spiegate come i dati aziendali possono essere compromessi e non risparmiatevi su illustrare quali sono le conseguenze. Considerate di invitare esperti esterni o utilizzare piattaforme di formazione online specializzate in cybersecurity per PMI.

La cultura della sicurezza:

Stabilite un sistema semplice per la segnalazione di attività sospette, come un indirizzo email dedicato o un modulo online. Assicuratevi che i dipendenti sappiano che non saranno penalizzati per segnalazioni errate fatte in buona fede. Considerate di implementare un programma di riconoscimento per chi dimostra di utilizzare pratiche di sicurezza esemplari. Fondamentale mantenere alta l'attenzione sulla sicurezza, ogni reparto a rischio deve essere incluso in questo progetto.

Stabilire una politica chiara:

Fondamentale che ogni dipendente sia fornito di dispositivi per il lavoro in cui sia già integrato ogni possibile forma di sicurezza. Questo dovrebbe includere requisiti di sicurezza come l'uso di password forti e l'installazione di software antivirus approvato dall'azienda. Per la gestione dei dati, create linee guida che specifichino come classificare, archiviare e condividere le informazioni aziendali. Assicuratevi che queste politiche siano facilmente accessibili, ad esempio sulla intranet aziendale, e che siano riviste e aggiornate almeno annualmente.

5. Proteggere la rete aziendale

Tre aspetti imprescindibili da valutare.

Segmentazione della rete:

La segmentazione della rete limita i danni in caso di violazione. Create una rete separata per gli ospiti, che non abbia accesso alle risorse aziendali interne. Per i sistemi che contengono dati sensibili, come i server finanziari o i database dei Clienti, create una sottorete isolata con accesso limitato. Questo può essere realizzato utilizzando VLAN (Virtual Local Area Network) su switch di rete gestiti. Se non avete competenze interne, consultate un esperto di networking per implementare queste configurazioni.

Mettere in sicurezza la rete wireless:

WPA3 è lo standard più recente per la sicurezza Wi-Fi. Verificate che i vostri router lo supportino e attivatelo dalle impostazioni del router. Se i vostri dispositivi non supportano WPA3, usate almeno WPA2. Cambiate la password del Wi-Fi ogni trimestre e assicuratevi che sia complessa. Non condividete mai la password della rete aziendale con i visitatori; usate invece la rete ospiti separata. Se avete difficoltà a configurare il Wi-Fi, chiedete assistenza al vostro fornitore di servizi Internet o a un tecnico IT.

Tenere monitorata la rete:

Un sistema di rilevamento delle intrusioni (IDS) monitora la rete per attività sospette. Opzioni popolari includono Snort (open source) o soluzioni commerciali come Cisco Secure IDS. Per le PMI più piccole, anche un firewall di nuova generazione può offrire funzionalità di IDS. Stabilite una routine per controllare i log di sistema almeno settimanalmente, cercando accessi non autorizzati o altre attività anomale. Se non avete le competenze interne, considerate di esternalizzare questa attività a un Managed Security Service Provider (MSSP).

6. Il Sistema di Backup

Tre criteri importanti da prendere in esame.

Implementare una strategia organizzata:

I backup sono la vostra ultima linea di difesa contro la perdita di dati. Utilizzate software di backup automatico per eseguire backup giornalieri dei dati critici. La regola 3-2-1 significa: mantenete tre copie dei vostri dati (una principale e due backup), su almeno due tipi diversi di supporto (ad esempio, hard disk e cloud), con una copia conservata offsite (come un servizio di backup cloud). Servizi come Acronis, Veeam o Carbonite offrono soluzioni complete di backup per PMI. Assicuratevi che almeno una persona nell'azienda sia responsabile di verificare quotidianamente che i backup siano stati eseguiti correttamente.

Testare la sicurezza delle copie:

Non basta fare i backup, dovete essere sicuri di poterli ripristinare quando serve. Almeno una volta al mese, provate a recuperare alcuni file dai vostri backup per assicurarvi che funzionino. Ogni trimestre, simulate uno scenario di recupero completo, come se aveste perso tutti i dati a causa di un ransomware. Questo vi aiuterà a identificare eventuali problemi nel vostro processo di backup e recupero. Se non avete le competenze interne, considerate di coinvolgere un consulente IT specializzato in disaster recovery per guidarvi in questi test.

Pianificare la Business Continuity:

Un piano di continuità aziendale descrive come la vostra azienda continuerà a operare durante e dopo un incidente significativo. Questo piano dovrebbe includere procedure per vari scenari (ad esempio, attacco ransomware, violazione dei dati, disastro naturale), elencare i contatti chiave (interni ed esterni), e definire chiaramente chi è responsabile e di quali azioni. Coinvolgete i responsabili di ogni reparto nella creazione di questo piano e assicuratevi che sia facilmente accessibile in caso di emergenza. Considerate di collaborare con un consulente specializzato in continuità aziendale per sviluppare un piano completo e realistico.

Guida realizzata da
Timenet SpA

Guida distribuita gratuitamente da
Timenet SpA

www.timenet.com

timenet
connessi sicuri soddisfatti