ALLIANZ
DIGITALE SICHERHEIT
SCHWEIZ

# Guida alla cybersicurezza per le PMI

Version 2.1 | 19. settembre 2022


Questa guida è stata sviluppata per aiutare le PMI a raggiungere un minimo di sicurezza informatica e quindi a proteggersi meglio dagli attacchi informatici più comuni.

Le PMI sono sempre più spesso bersaglio di attacchi informatici che possono avere gravi conseguenze. Anche poche misure importanti aiutano a raggiungere un livello minimo di protezione contro le minacce informatiche. Tali misure sono spiegate in questa guida. Il linguaggio della guida è chiaro, le azioni semplici e concrete - specificamente adattate alle esigenze delle PMI.

La guida è complementare al Cybersecurity Quick Test per le PMI e segue la struttura tematica ivi introdotta. Per un'autovalutazione del posizionamento della propria azienda in termini di cybersicurezza, consigliamo di completare il test rapido.

La guida cosi' come il test rapido per le PMI sono parte integrante della Strategia nazionale per la protezione della Svizzera contro i rischi informatici. Un gruppo di esperti ha sviluppato i contenuti e li ha adattati esplicitamente alle esigenze delle PMI.

I partner coinvolti nello sviluppo della guida lavorano insieme per garantire che il panorama delle PMI svizzere possa proteggersi dai rischi informatici nel miglior modo possibile.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

ICTSWITZERLAND · ISSS Information Security Society Switzerland · satw it's all about technology · SNV standards connect the world · SQS · ASA | SVV

## Panoramica

## Sicurezza nell'ambito dell'organizzazione e dei processi

### Perché è importante?

In caso di incidente informatico, la preparazione e la risposta giusta sono fondamentali e determinano se e quanto velocemente potrete continuare a gestire la vostra attività dopo un incidente.

Una risposta rapida e corretta può ridurre significativamente o addirittura prevenire i danni. A tal fine, è importante allineare la propria organizzazione a queste minacce e definire processi adeguati, come il backup regolare dei dati, l'assegnazione selettiva dei diritti di accesso e la creazione di un piano di emergenza.

### Cosa posso fare?

- ❑ Proteggete le vostre informazioni con un backup regolare.
- ❑ Garantire l'amministrazione appropriata degli utenti.
- ❑ Creare un piano di emergenza.

### Come posso procedere?

#### Informazioni di backup: Il backup come routine

- Creare regolarmente e, se possibile, automaticamente un backup su un supporto di sicurezza (disco rigido, online, ecc. - a seconda del modello aziendale e dei requisiti normativi della PMI).
- Archiviare il backup in un luogo esterno, protetto e separato dalla rete (backup offline).
- Verificare regolarmente se i dati possono essere ripristinati dal supporto di sicurezza.

#### Ridurre al minimo la superficie di attacco: Amministrazione appropriata degli utenti

Una corretta amministrazione degli utenti può rendere più difficile l'accesso alle informazioni particolarmente importanti da parte dei criminali.

- Creare account separati (login) per le attività di amministrazione (dati, informazioni e sistemi particolarmente sensibili) e per le attività "normali".
- Assegnate a ciascun utente solo i diritti di accesso più necessari. Ciò impedisce agli aggressori di ottenere un accesso illimitato a tutti i sistemi.
- Se possibile, utilizzate solo account personali (non utilizzate account utilizzati da più utenti con lo stesso nome utente/password).
- Determinare chi ha accesso a determinate applicazioni/informazioni informatiche. Assegnare i diritti di accesso in base ai ruoli (ad esempio, contabilità/amministratore del personale/segretario/amministratore del sistema/vendite).
- Bloccare gli account utente/i dati di accesso delle rispettive persone quando lasciano l'azienda.

## Prepararsi in caso di emergenza: piano di emergenza

Creare un piano di emergenza per sapere cosa fare in caso di necessità.

- Identificare i sistemi critici per le emergenze, ad esempio il database degli indirizzi, il sistema di posta elettronica, il calendario degli appuntamenti e così via, nonché i dati personali e i dati dei clienti.
- Definire i livelli di fallback (fornire PC sostitutivi; dotare tutte le postazioni di lavoro di almeno due browser; concordare con i fornitori i tempi di risposta e le scadenze di consegna).
- Registrare chi lavora con quale sistema (nomi e numeri di telefono) per poter fornire informazioni mirate in caso di emergenza.
- Definire la prima reazione in caso di incidente: scollegare le connessioni di rete (cavo e WLAN) dei sistemi interessati.
- Definire le misure per il ripristino rapido dei vostri sistemi e valutare come continuare a lavorare in caso di guasto dei sistemi critici (ad esempio, stampando i dati dei contatti più importanti, ecc.)
- Definire le responsabilità e i ruoli, ossia chi deve essere informato e come in caso di incidente (ad es. ransomware o guasto di un sistema critico di emergenza):
    - Persona/azienda che deve risolvere l'incidente informatico.
    - Persona/azienda per l'adozione di misure legali immediate. Se, ad esempio, si tratta di dati personali, è consigliabile rivolgersi a un consulente legale o a un esperto in materia.
    - Persona/azienda per le misure di comunicazione immediata.
    - Persona incaricata di segnalare l'incidente: questa persona informa la stazione di polizia più vicina e il Centro nazionale di sicurezza informatica della Confederazione (NCSC) utilizzando il modulo di segnalazione corrispondente. In caso di frode informatica che comporti un danno economico, si raccomanda vivamente di contattare immediatamente la banca, la polizia e/o una società specializzata per poter bloccare i pagamenti.
    - Esercitate l'emergenza nella vostra azienda.

## Sicurezza grazie al "fattore umano

### Perché è importante?

Nonostante tutti gli ausili tecnici, in ultima analisi sono i dipendenti a essere decisivi per la sicurezza della vostra azienda. È quindi importante che voi e tutti i vostri dipendenti siate consapevoli dei pericoli attuali, sappiate come maneggiare l'attrezzatura tecnica e osserviate le regole più importanti.

### Cosa posso fare?

- ❑ Consolidare la sensibilizzazione dei dipendenti nella routine quotidiana dell'azienda.
- ❑ Garantire la migliore protezione possibile alle vostre applicazioni con password sicure.
- ❑ Definire le linee guida per l'uso sicuro di Internet e della posta elettronica.

## Come posso procedere?

### Tema in ambito di sicurezza

- Fare della sicurezza e in particolare di un comportamento sicuro su Internet un argomento ricorrente in azienda.
- Organizzate una formazione di base per i vostri dipendenti con i seguenti contenuti:
  - Quali sono i vantaggi della sicurezza informatica?
  - Cosa sono le password forti? (vedi sotto)
  - Cosa si intende per uso sicuro di Internet e della posta elettronica? (vedi sotto)

### La migliore protezione possibile per le vostre applicazioni: Password forti

- Scegliere password forti, ossia utilizzare password il più possibile lunghe con almeno 12 caratteri, composte da lettere minuscole e maiuscole, numeri e caratteri speciali.
- Utilizzate un gestore di password e password generate automaticamente.
- In alternativa, utilizzate la passphrase: scegliete una frase personale che nessuno possa facilmente indovinare. Da questa frase, prendete la prima o le prime due lettere di ogni parola per formare una password. Fate attenzione a non usare frasi comunemente conosciute come titoli di libri, modi di dire, ecc.
- Non usate le password più di una volta, cioè usate una password diversa per ogni servizio come l'account di posta elettronica, l'online banking, il software di contabilità, le applicazioni CRM, ecc.
- Se possibile, utilizzate l'autenticazione a due fattori per proteggere l'accesso ai vostri servizi Internet (ad esempio, una password unica, un token SMS, ecc.).
- Non inserire la password in una pagina Internet a cui si è acceduto tramite un link, ma inserire manualmente l'indirizzo (URL) della pagina corrispondente nella riga dell'indirizzo del browser.
- Cambiare le password impersonali sul posto di lavoro quando i dipendenti lasciano l'azienda.

### Per un uso sicuro di Internet e della posta elettronica: Linee guida per gli utenti

Definire le linee guida per l'uso sicuro di Internet e della posta elettronica. Questi possono includere i seguenti punti:

- Non divulgare i dati di accesso (nome utente e password) a terzi in nessun momento e in nessuna circostanza.
- Inviate i numeri di carta di credito solo a siti web affidabili, ad esempio assicurandovi che https:// compaia prima dell'indirizzo nel browser.
- Non scaricate programmi sconosciuti da Internet.
- Utilizzate il vostro smartphone come hotspot invece di una rete WLAN pubblica e non protetta. Questo vale soprattutto per l'online banking. Le connessioni non protette non sono sicure e c'è il rischio che terzi accedano ai vostri dati.

– Fate attenzione quando ricevete le e-mail e prestate particolare attenzione ai seguenti punti:
    - In caso di e-mail dubbie (ad esempio, indirizzi di mittenti anomali, errori di ortografia, tonalità e loghi), non aprite i documenti o i programmi allegati e non cliccate sui link.
    - In caso di dubbio, non divulgate mai informazioni riservate e cercate di contattare il mittente con altri mezzi (ad esempio per telefono) per verificare l'attendibilità dell'e-mail.
    - Esaminate in modo critico anche i messaggi che provengono da una persona conosciuta o da un dipendente senior dell'azienda. I truffatori potrebbero avere accesso alla casella di posta elettronica di questa persona e inviare e-mail a suo nome.

## Sicurezza grazie a misure tecniche adeguate

### Perché è importante?

Le lacune nella sicurezza possono consentire a persone non autorizzate di penetrare nei vostri sistemi. I dati possono essere distrutti e manipolati, oppure la vostra infrastruttura IT può essere manipolata per scopi criminali. Gli aggiornamenti del software colmano queste lacune di sicurezza.

Un firewall aggiornato può proteggere il computer da accessi non autorizzati. Un software antivirus aggiornato protegge i vostri dati da virus, worm e trojan.

I criminali possono leggere e persino manipolare il traffico di dati se la comunicazione non è crittografata.

### Cosa posso fare?

o Utilizzare un software adeguato (ad es. firewall, software antivirus) per aumentare la sicurezza.

o Assicuratevi di aggiornare regolarmente il software.

o Non collegare a Internet dispositivi obsoleti che non dispongono di aggiornamenti software.

### Come posso procedere?

#### Aumentare la sicurezza con gli ausili tecnici: Software e hardware adatti

– Aggiornare regolarmente i sistemi operativi, i firewall e le altre applicazioni.
– Controllare regolarmente gli aggiornamenti del vostro computer e aggiornarlo per colmare le lacune di sicurezza.
– Utilizzare le funzioni di aggiornamento automatico quando possibile. Questo vale anche per tutti i prodotti software e i dispositivi connessi a Internet, come sistemi, stampanti, controlli di edifici, elettrodomestici o smartphone.
– Scollegare da Internet o mettere fuori uso i dispositivi per i quali non vengono forniti aggiornamenti.
– Installare un software antivirus aggiornato e aggiornarlo regolarmente (di solito avviene automaticamente). Per una protezione ancora maggiore, utilizzate uno scanner antivirus di due diversi produttori per rilevare la più ampia gamma possibile di minacce.
– Proteggere le vostre comunicazioni con una buona crittografia (ad es. Virtual Private Network, VPN).

## La cybersicurezza come parte della protezione dei dati

### Perché è importante?

La vostra azienda è responsabile della gestione sicura dei dati personali e della proprietà intellettuale. In caso di perdita di dati o di violazione della protezione dei dati, c'è il rischio di azioni penali, multe salate e gravi danni all'immagine. Le conseguenze possono minacciare la vostra esistenza.

Dal 2018 è in vigore il nuovo Regolamento generale sulla protezione dei dati (GDPR) dell'UE, che si applica in parte anche alle aziende svizzere. Le aziende e i siti web svizzeri che trattano dati di cittadini dell'UE o che hanno come gruppo target tali cittadini sono interessati dal GDPR. Ciò vale anche, ad esempio, per i siti web che utilizzano i cosiddetti cookie per valutare il comportamento di navigazione dei loro visitatori provenienti da altri Paesi dell'UE.

La cybersicurezza e protezione dei dati vanno di pari passo: i criminali possono ottenere dati sensibili attraverso un attacco informatico.

### Cosa posso fare?

o Adottando misure di cybersicurezza si contribuisce al rispetto della legge sulla protezione die dati personali.

### Come posso procedere?

#### Trattare i dati secondo quanto prevista dalla legge: Protezione dei dati

- Non appena trattate in qualsiasi modo i dati di persone (ad esempio clienti o dipendenti), dovete proteggerli adeguatamente (o semplicemente raccogliere i dati).
- Qualsiasi trattamento di dati personali è considerato un'elaborazione, in particolare l'ottenimento, la memorizzazione, la conservazione, l'utilizzo, la modifica, la divulgazione, l'archiviazione, la cancellazione o la distruzione.
- Verificate se siete interessati dal GDPR: Online-Check Economiesuisse, Faktenblatt DSGVO

## Sicurezza in un ambiente digitale

### Perché è importante?

Se uno dei vostri fornitori o provider di servizi viene colpito da un attacco hacker, potreste essere colpiti anche voi, ad esempio in caso di perdita dei dati dei vostri clienti. È quindi importante che anche i terzi con cui lavorate implementino le misure di cybersicurezza più importanti.

Se esternalizzate l'IT o la sicurezza IT a terzi, è importante che teniate d'occhio il vostro fornitore e che chiariate con lui i punti più importanti.

### Cosa posso fare?

☐ Esigere che i **partner e i fornitori di outsourcing** implementino misure minime di cybersicurezza.

☐ Quando si esternalizzano servizi IT e di sicurezza IT, prestare attenzione ai certificati e alla conformità con le misure di sicurezza più importanti.

## Come posso procedere?

### Esigere sicurezza al di fuori della propria azienda: Partner e fornitori di outsourcing

Eseguite il test rapido di cybersicurezza con i provider e i fornitori di servizi (partner di outsourcing) e assicuratevi che soddisfino anche i requisiti imposti alla vostra azienda. Chiarite i seguenti punti, tra gli altri:

- I backup vengono eseguiti regolarmente e conservati in un luogo esterno?
- Esiste un piano di emergenza?
- Esistono linee guida per gli utenti e vengono rispettate?
- Esistono linee guida per l'amministrazione degli utenti?
- I dipendenti sono sensibilizzati al tema della cybersicurezza (ad esempio, e-mail di phishing, uso delle password)?
- I sistemi operativi, i firewall e le altre applicazioni sono aggiornati regolarmente?
- Viene utilizzata una comunicazione criptata?
- Il software antivirus viene utilizzato e aggiornato regolarmente?

### Sicurezza al momento dell'esternalizzazione dei servizi di sicurezza: Provider di sicurezza informatica

Assicuratevi che il fornitore di servizi IT o di sicurezza informatica soddisfi i requisiti di sicurezza più importanti: Eseguite con loro un test rapido o verificate se dispongono di un certificato adeguato (ad esempio CyberSeal per i fornitori di servizi IT, ISO 27001 per i fornitori di sicurezza IT).

## A cosa ci riferiamo

Riferimenti

BNC: Cybersecurity und Datenschutz

EDOEB: Datenschutz

IT-Sicherheit für KMU

KMU-Portal: Zehn Regeln für die Informationssicherheit im KMU

NCSC: Merkblatt Informationssicherheit für KMU

NCSC: Informationen für Unternehmen

Tagblatt: Datenschutzgesetz

UBS: Phishing