Cybersecurity-Check per PMI

Versione 4.0, 8. dicembre 2025

PMI nel mirino dei ciberattacchi

Le piccole e medie imprese (PMI) sono sempre più bersaglio della cibercriminalità. Secondo *Netzwoche*, nel primo trimestre 2025 il numero dei ciberattacchi in Svizzera è aumentato del 113% rispetto all'anno precedente – un incremento estremamente allarmante. Particolarmente preoccupante è la crescita degli attacchi supportati dall'intelligenza artificiale, come tecniche di deepfake usate per tentativi di frode del tipo CEO fraud (Fonte: *Portale PMI della SECO*).

Le cause più frequenti dei ciberattacchi riusciti sono:

- protezione insufficiente dei sistemi e dei processi
- sistemi informatici non aggiornati
- manipolazione delle persone (social engineering)
- preparazione insufficiente agli incidenti di cibersicurezza

Il sito www.cybersecurity-check.ch è stato sviluppato nel 2020 nell'ambito della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC). La versione 4.0 (stato: novembre 2025) è stata elaborata insieme ai seguenti partner: ADSS, UFCS, BDO, digitalswitzerland, EXPERTsuisse, Gobugfree, ISSS, SATW, SISA, SNV, SQS, Suissedigital, SVV.

Uno strumento pratico per la protezione delle PMI

Il Cybersecurity-Check offre alle PMI raccomandazioni concrete e attuabili per aumentare il loro livello di cibersicurezza. Tiene conto di: minacce attuali, nuove tecnologie, requisiti legali, esigenze specifiche delle PMI. La struttura modulare e l'orientamento alla praticità ne facilitano l'utilizzo anche senza conoscenze tecniche.

Grazie al self-check integrato, le imprese possono valutare:

- quali misure tecniche, organizzative, procedurali e relative al personale sono già state implementate
- dove è necessario intervenire per garantire un livello minimo di cibersicurezza

Nota: Il Cybersecurity-Check non sostituisce una consulenza personalizzata, ma rappresenta un solido punto di partenza per le PMI.

Indice dei contenuti

1 Organizzazione e processi

Perchè è importante?

Gli incidenti di cibersicurezza possono colpire aziende di qualsiasi dimensione.

Determinante non è solo la capacità di reagire all'emergenza, ma anche la prevenzione e il miglioramento continuo del livello di sicurezza organizzativa.

Un buon livello organizzativo di cibersicurezza richiede:

- responsabilità definite
- backup regolari delle informazioni critiche
- gestione accurata dei diritti di accesso
- un piano d'emergenza aggiornato e testato (incl. canali di comunicazione alternativi)

Cosa posso fare?

- ☑ Inventariare e proteggere tutte le risorse IT e i processi critici.
- ☑ Implementare backup regolari e automatizzati.
- ☑ Rafforzare la gestione utenti con diritti basati sui ruoli e autenticazione a due fattori (2FA).
- ☑ Testare regolarmente un piano d'emergenza basato sulle minacce attuali (es. modelli del UFCSe di BDO).

2 Personale & Sensibilizzazione

Perchè è importante?

Il social engineering è uno dei principali fattori che rendono efficaci i ciberattacchi. Secondo l'Ufficio federale della cibersicurezza (UFCS), oltre l'80% degli incidenti di cibersicurezza nelle aziende svizzere coinvolge il fattore umano. Una forza lavoro sensibilizzata rappresenta la difesa più importante.

Un buon comportamento di sicurezza include:

- riconoscimento dei segnali sospetti
- uso corretto di password e informazioni sensibili
- rispetto delle linee guida IT
- formazione e esercitazioni regolari

Cosa posso fare?

- ☑ Rendere la **sensibilizzazione** parte della cultura aziendale.
- ☑ Garantire **password** sicure e l'uso di 2FA ove possibile.
- ☑ Stabilire **linee guida** chiare per e-mail, internet, social media e dispositivi mobili.

3 Misure tecniche di protezione

Perchè è importante?

Le misure tecniche sono il fondamento della cibersicurezza. Senza sistemi aggiornati, protezioni adeguate e comunicazioni cifrate, l'azienda rimane vulnerabile.

Nel 2025 gli attacchi si sono intensificati tramite: scansioni automatizzate basate su IA, sfruttamento dei servizi Cloud, abuso di dispositivi obsoleti (router, IoT, accessi remoti).

Un adeguato livello tecnico significa:

- aggiornamenti continui
- software di sicurezza
- cifratura delle comunicazioni
- protezione dei dispositivi connessi

Cosa posso fare?

- ☑ Utilizzate hardware e **software** adeguati (ad es. firewall e software antivirus) per aumentare la vostra sicurezza.
- ☑ Assicuratevi di **aggiornare regolarmente** il vostro software e i vostri dispositivi.
- ☑ Non collegate **dispositivi obsoleti** per i quali non sono disponibili aggiornamenti software e collegate a Internet solo i sistemi strettamente necessari.

Nota: Le misure tecniche di protezione non sono **un progetto una tantum, ma un processo** continuo. Effettuate controlli regolari o rivolgetevi a specialisti IT esterni e fornitori certificati per individuare e colmare eventuali lacune.

4 Protezione dei dati & Aspetti legali

Perchè è importante?

La protezione dei dati personali non è solo un fattore di fiducia nei confronti dei clienti, ma è anche prescritta dalla legge. Le violazioni delle leggi sulla protezione dei dati possono comportare multe elevate, conseguenze legali e danni ingenti alla reputazione, in particolare se sono riconducibili a incidenti informatici.

Dall'entrata in vigore della revisione della legge svizzera sulla protezione dei dati (LPD) nel 2023 e dall'attuazione in corso del Regolamento generale sulla protezione dei dati (GDPR) dell'UE per le aziende svizzere che hanno rapporti con l'UE, chiunque tratti dati personali deve adottare misure tecniche e organizzative adeguate a garantirne la sicurezza. In caso di violazioni della protezione dei dati, i dirigenti possono essere ritenuti personalmente responsabili.

Un trattamento conforme dei dati personali richiede:

- trasparenza verso le persone interessate
- protezione contro accessi non autorizzati e perdite
- responsabilità chiare e documentate
- accordi di trattamento dati con fornitori (Modello)
- conoscenza e applicazione degli obblighi di notifica obbligatoria in caso di violazioni (Guida)

Cosa posso fare?

- ☑ Verificare che la gestione dei dati sia conforme alla nLPD e, se applicabile, alla DSGVO.
- ☑ Documentare quali dati vengono raccolti, trattati e conservati, e con quale finalità.
- ☑ Implementare misure tecniche e organizzative adeguate (autorizzazioni, cifratura, backup).

Nota: La protezione dei dati riguarda l'intera azienda, non solo l'IT (es. sito web, CRM, HR).
Risorse utili: https://www.edoeb.admin.ch/it/protezione-dei-dati oppure https://www.kmu.admin.ch/kmu/it/home/fatti-e-tendenze/digitalizzazione/protezione-dei-dati.html.

5 Partner esterni & Fornitori

Perchè è importante?

Oggi molte PMI si affidano a fornitori di servizi IT esterni, fornitori di servizi cloud o soluzioni software specializzate. Si tratta di una scelta sensata, poiché i partner qualificati apportano competenze, esperienza e tecnologie moderne che spesso non sono disponibili internamente nella stessa misura. Una collaborazione di successo con fornitori esterni è quindi un elemento fondamentale per una solida strategia di sicurezza informatica.

Allo stesso tempo, rimane importante stipulare accordi chiari, definire le responsabilità e verificare regolarmente il rispetto degli standard di sicurezza. Infatti, anche se alcune attività sono esternalizzate, la responsabilità della sicurezza dei dati e dei sistemi rimane dell'azienda stessa.

Una collaborazione sicura con partner esterni richiede:

- scelta di fornitori qualificati
- accordi chiari e documentati
- processi condivisi di gestione delle emergenze
- gestione rigorosa e limitata dei diritti di accesso

Cosa posso fare?

- ☑ Lavorare con partner certificati (es. CyberSeal, SN EN ISO/IEC 27001).
- ☑ Documentare chiaramente i requisiti tecnici e organizzativi.
- ☑ Integrare i partner nella pianificazione d'emergenza.
- ☑ Verificare regolarmente il rispetto degli standard di sicurezza

Nota: Anche se un fornitore «si occupa di tutto», la responsabilità rimane comunque dell'azienda (anche per quanto riguarda la garanzia del backup e la ripristinabilità dei dati). Verificate regolarmente che i vostri partner rispettino le misure di sicurezza adeguate al vostro settore e alle dimensioni della vostra azienda.

Per domande sulla scelta dei fornitori adeguati o sulla stesura dei contratti, potete rivolgervi alle piattaforme nazionali quali UFCS - Informazioni per le imprese, Alleanza Sicurezza Digitale Svizzera - CyberSeal, ITSec4KMU o alle associazioni di categoria del vostro settore.

6 Penetration Testing & Analisi delle vulnerabilità

Perchè è importante?

Anche le misure di sicurezza ben intenzionate sono efficaci solo se funzionano davvero. Le vulnerabilità nei sistemi, nelle reti o nelle applicazioni spesso passano inosservate fino a quando non vengono sfruttate dagli hacker. Per questo motivo è fondamentale testare regolarmente la propria infrastruttura IT, idealmente tramite terzi qualificati e indipendenti.

Proprio nel 2025, anno in cui gli hacker utilizzano sempre più spesso scansioni automatizzate e basate sull'intelligenza artificiale per identificare in modo mirato i punti deboli delle aziende, è fondamentale adottare un approccio proattivo. Un penetration test (in breve: pentest) simula attacchi reali in modo

controllato e tracciabile, con l'obiettivo di individuare e risolvere tempestivamente i punti deboli.

Un test professionale offre:

- chiarezza sulle effettive lacune di sicurezza,
- valutazione realistica del rischio,
- raccomandazioni concrete per il miglioramento.

Cosa posso fare?

- ☑ Effettuare analisi delle vulnerabilità regolarmente, internamente o tramite specialisti.
- ☑ Eseguire ogni anno un pentest dei sistemi critici o dopo modifiche importanti.
- ☑ Correggere e documentare sistematicamente le vulnerabilità individuate.

Nota: Per le PMI più piccole, anche le scansioni standardizzate delle vulnerabilità possono rappresentare un primo passo importante. Piattaforme come GoBugFree oder ITSec4KMU offrono un supporto pratico. Chi desidera andare oltre può identificare i fornitori adeguati con i partner della rete di sicurezza informatica (ad es. SCD-DNA, Alleanza Sicurezza Digitale Svizzera - CyberSeal).

Info-Box: Penetration Testing vs. Ethical Hacking

Penetration Testing (Pentest)

Un test chiaramente delimitato, strutturato e mirato, che si concentra su un'area definita (ad es. applicazione web, segmento di rete). L'obiettivo è identificare i punti deboli tecnici e valutarli.

Hacking etico (hacking amichevole)

Un approccio più ampio e meno rigidamente strutturato che agisce come un vero aggressore, ma in modo autorizzato. Vengono esaminati i punti deboli tecnici, organizzativi e concettuali dell'intera azienda.

Un pentest può essere parte di un progetto di hacking etico più ampio, ma è significativamente più ristretto e metodicamente standardizzato.

7 Autovalutazione sulla cibersicurezza

La vostra azienda è adeguatamente protetta e preparata contro gli attacchi provenienti dal ciberspazio? Verificate subito se soddisfate i requisiti fondamentali.

1. Organizzazione e processi	si	**no**	**non lo so**
Sono note le persone di riferimento per la cibersicurezza (interne o esterne)?			
La cibersicurezza è trattata regolarmente nelle riunioni di direzione?			
È parte integrante del vostro risk management?			
Avete inventariato tutte le risorse IT e i processi critici?			
Avete backup indipendenti da sistemi e fornitori?			
Conservate almeno una copia di backup offline e in luogo sicuro?			
Testate regolarmente il ripristino dei backup?			
Utilizzate account separati per attività amministrative e normali?			
I diritti di accesso sono assegnati basandosi sul principio del minimo privilegio?			
Utilizzate solo account personali, senza account condivisi?			
Le password degli account comuni vengono cambiati quando un dipendente lascia?			
Gli account vengono disattivati tempestivamente in caso di uscita o cambio ruolo?			
Avete identificato e documentato sistemi, dati e informazioni critiche?			
Esistono soluzioni di fallback (dispositivi sostitutivi, accordi con fornitori)?			
Il piano d’emergenza è disponibile offline?			
Sono definiti ruoli e responsabilità in caso di incidente?			
Eseguite esercitazioni regolari sul piano d’emergenza?			
ono note le persone di riferimento per la cibersicurezza (interne o esterne)?			
La cibersicurezza è trattata regolarmente nelle riunioni di direzione?			
È parte integrante del vostro risk management?			

2. Personale & Sensibilizzazione	si	no	non lo so
Effettuate una formazione di base per tutti i dipendenti sulla cibersicurezza?			
La formazione include phishing, CEO fraud, deepfake?			
La formazione viene ripetuta regolarmente (es. annualmente)?			
Evitate collegamenti non controllati (es. smartphone via USB)?			
Promuovete una cultura “no blame” per segnalazioni interne?			
La cibersicurezza è visibile internamente (poster, newsletter, video)?			
Le password hanno almeno 12 caratteri e complessità adeguata?			
Utilizzate o consigliate password manager?			
Applicate la 2FA ovunque possibile?			
Verificate se password aziendali compaiono in violazioni note (Have I Been Pwned)?			
Le linee guida per e-mail, internet, social media e dispositivi mobili sono definite?			
È vietata la condivisione delle credenziali?			
Avvisate sui rischi degli hotspot Wi-Fi pubblici?			
Regolate l’installazione di app e software?			
Anche la direzione è sensibilizzata e funge da modello?			
Effettuate una formazione di base per tutti i dipendenti sulla cibersicurezza?			
La formazione include phishing, CEO fraud, deepfake?			

3. Misure tecniche di protezione	si	no	non lo so
Gli aggiornamenti automatici sono attivati su sistemi e applicazioni?			
Verificate regolarmente il livello di aggiornamento (incl. router, stampanti, IoT)?			
Utilizzate strumenti centralizzati di patch management?			
Escludete o isolate dispositivi non aggiornabili?			
Utilizzate soluzioni di endpoint protection?			
La firewall è attiva?			
Usate Mobile Device Management (MDM) per dispositivi mobili?			
Le connessioni esterne sono cifrate (VPN)?			
Per accessi esterni imponete autenticazione forte (2FA, Passkey)?			
La rete è segmentata (es. contabilità separata dal Wi-Fi ospiti)?			
Porte non utilizzate (USB, Bluetooth) sono disattivate?			
I locali server sono fisicamente protetti?			

4. Protezione die dati & Aspetti legali	si	no	non lo so
Avete un inventario dei dati personali trattati?			
È documentato lo scopo di ogni trattamento?			
È definita la base giuridica del trattamento?			
Applicate alle informazioni personali le stesse misure di sicurezza dei dati aziendali?			
Solo persone autorizzate possono accedervi?			
La vostra pagina web dispone di un'informativa sulla privacy?			
Le persone interessate possono esercitare i loro diritti (accesso, rettifica, cancellazione)?			
Avete un processo interno per gestire violazioni dei dati?			
Potete notificare violazioni al IFPDT entro 72 ore?			
Le persone interessate vengono informate se necessario?			
Avete accordi di trattamento dati con tutti i fornitori?			
I fornitori soddisfano standard adeguati (es. CyberSeal)?			

5. Partner esterni & Fornitori	si	no	non lo so
Quando scegliete fornitori IT e cloud, prestate attenzione ai certificati di sicurezza riconosciuti (es. CyberSeal),			
Richiedete regolarmente prove delle misure di protezione attuali, come la gestione delle patch, i backup e le procedure di emergenza?			
Utilizzate strumenti come il test rapido sulla sicurezza informatica per le PMI per chiarire i requisiti con i potenziali fornitori?			
Esistono accordi scritti, compresi gli accordi sul livello di servizio (SLA), per la collaborazione con partner esterni, in particolare per quanto riguarda il trattamento dei dati o l'accesso ai sistemi?			
In essi avete definito i diritti di accesso, gli obblighi di segnalazione in caso di incidenti di sicurezza e il luogo di trattamento dei dati (ad es. Svizzera, UE, paesi terzi)?			
I partner esterni sono coinvolti nella vostra pianificazione di emergenza (ad es. chi viene informato, quando e come)?			
Pianificate e conducete esercitazioni o test di sicurezza congiunti (ad es. reazione al phishing o ai guasti)?			
Ricevete regolarmente aggiornamenti proattivi sulla situazione della sicurezza dai vostri fornitori di servizi?			
Le persone esterne ricevono solo i diritti di accesso minimi necessari (principio del diritto minimo)?			
Documentate chiaramente chi ha accesso a quali sistemi, compresa la durata e lo scopo?			
Gli accessi degli esterni vengono immediatamente rimossi quando non sono più necessari (ad es. dopo il completamento del progetto)?			

Premessa: ciò vale soprattutto per le PMI che sviluppano e gestiscono soluzioni proprie o che sono direttamente collegate a Internet.

6. Test di penetrazione e analisi delle vulnerabilità	si	**no**	**non lo so**
Chiarite in anticipo l'ambito del test (ad es. rete, applicazioni web, accessi remoti, WLAN)?			
Attuate in modo prioritario le misure identificate dalle analisi delle vulnerabilità e dai test di penetrazione, in particolare in caso di rischio elevato?			
Documentate le misure adottate (ad es. aggiornamenti effettuati, modifiche di configurazione)?			
Esegui test di verifica per controllare che le vulnerabilità individuate siano state completamente risolte?			
Esistono criteri chiari che stabiliscono quando eseguire analisi delle vulnerabilità o test di penetrazione (ad es. dopo gli aggiornamenti, ogni anno)?			
Questi test sono parte integrante della tua strategia di sicurezza IT?			

8 Appendice

Link utili

Autorità e uffici pubblici

- **Ufficio federale della cibersicurezza– «Proteggete la vostra PMI»**
  Linee guida ufficiali, liste di controllo, raccomandazioni per le PMI.
  Ufficio federale della cibersicurezza UFCS – Promemoria sulla sicurezza delle informazioni per le PMI
  Ufficio federale della cibesicurezza UCFS – Informazioni per imprese
- **Incaricato federale della protezione dei dati e della trasparenza (IFPDT)**
  Linee guida, modelli, FAQ, disposizioni legali relative alla legge svizzera sulla protezione dei dati (LPD).
  Incaricato federale della protezione dei dati e della trasparenza - Protezione dei dati
- **Modulo di segnalazione die ciberattacchi (UFCS)**
  Segnalazione online di incidenti per le aziende.
  Ufficio federale della cibersicurezza – Formulario di notifica

Offerte di assistenza specifiche per settore

- **CyberSeal – Marchio di qualità dell'Alleanza per la sicurezza digitale Svizzera** Certifica i fornitori di servizi IT che garantiscono un livello di protezione adeguato e aiuta le PMI nella scelta di partner IT affidabili.
  Alleanza Sicurezza Digitale Svizzera – CyberSeal
- **GObugfree – Ehtical Hacking Ethical hacking e piattaforma per la segnalazione delle vulnerabilità**
  Soluzione per le PMI per l'identificazione e la segnalazione delle vulnerabilità.
  GObugfree
- **ITsec4KMU – Prevenzione e difesa dagli attacchi informatici per le PMI svizzere**
  Autovalutazione gratuita e orientata alla pratica e linee guida per le PMI.
  ITSec4KMU
- **Suissedigital – PMI Security Check**.
  Controllo di sicurezza a bassa soglia per le PMI del settore della comunicazione digitale.
  Suissedigital – KMU Security Check
- **Swiss Cyber Defence DNA (SCD-DNA)**
  Modello per la registrazione sistematica e il miglioramento della sicurezza informatica per le PMI
  SWISS CYBER DEFENCE DNA

Sensibilizzazione e materiale didattico

- **Campagna SUPERR**
  Campagna nazionale per la protezione di base della cibersicurezza: consigli di facile comprensione per i collaboratori.
  Agire - Cibersicurezza è S-U-P-E-R.ch
- **Cybernavi**
  Piattaforma interattiva di informazione e formazione sui ciber-rischi, pensata appositamente per le PMI e i loro collaboratori.
  Cybernavi

Norme e standard (utili per la valutazione dei fornitori)

- **SNV – Schweizerische Normen-Vereinigung**
  Informazioni sulle norme ISO/IEC, tra cui 27001, 27002 e 27701.
  Schweizerische Normen-Vereinigung - SNV
- **SQS – Zertifizierungsstelle für Informationssicherheit**
  Certificazioni, modelli di audit e standard di settore (ad es. ISO 27001, standard di protezione dei dati).
  Associazione svizzera per i sistemi di qualità e di gestione | SQS Svizzera

Indirizzi di contatto per le emergenze

Polizia (Cibercriminalità):
Numero di emergenza: 117
Le autorità di polizia cantonali offrono servizi specializzati nella lotta alla cibercriminalità.
https://www.fedpol.admin.ch/fedpol/it/home.html

Ufficio federale della cibersicurezza (UFCS):
Modulo di notifica per incidenti informatici in Svizzera
Segnalazione online: Ufficio - Formulario di notifica

Consulenza legale in caso di ciberattacchi:
Molti Cantoni e associazioni di categoria offrono servizi legali specializzati. In alternativa:

- BDO Cybersecurity & Recht: www.bdo.ch
- Esperti in materia di protezione dei dati: www.edoeb.admin.ch

Glossario

2FA (autenticazione a due fattori)
Livello di sicurezza aggiuntivo che richiede due fattori indipendenti al momento del login (ad es. password + codice SMS o conferma tramite app).

Asset
Oggetto di valore di un'azienda nel contesto IT, ad es. server, software, dati o dispositivi finali.

Backup
Copia di dati importanti che viene memorizzata separatamente dal sistema produttivo per poterla ripristinare dopo un incidente.

Bluetooth
Tecnologia di comunicazione wireless a corto raggio. Le connessioni Bluetooth aperte o non protette possono rappresentare un rischio per la sicurezza.

Servizio cloud
Risorsa IT esterna fornita tramite Internet (ad es. Microsoft 365, Google Workspace). Richiede regole chiare in materia di sicurezza e accesso.

Attacco informatico
Tentativo di compromettere i sistemi IT, rubare o manipolare dati o interferire con il funzionamento.

CyberSeal
Marchio di qualità svizzero che certifica i fornitori di servizi IT che garantiscono ai propri clienti un livello adeguato di protezione dai rischi informatici grazie a misure tecniche e organizzative appropriate.

Violazione della protezione dei dati
Accesso non autorizzato, perdita o divulgazione di dati personali. Soggetto a obbligo di segnalazione se sussiste un rischio per le persone interessate**.**

DLP (Data Loss Prevention)
Strumenti o politiche che impediscono la perdita o la divulgazione non autorizzata di informazioni riservate.

Protezione degli endpoint
Software di sicurezza per dispositivi finali come notebook, smartphone o server. Rilevamento di malware, comportamenti sospetti e attacchi.

Ethical hacking (hacking amichevole)
Scenario di attacco autorizzato in cui vengono verificati tutti i possibili punti deboli (tecnici, organizzativi, procedurali).
→ Il pentesting ne fa parte, ma è più ristretto e chiaramente definito.

Firewall
Componente di sicurezza che monitora il traffico dati e blocca gli accessi non autorizzati.

IoT (Internet of Things)
Dispositivi connessi a Internet come telecamere, sensori o router. Spesso un punto di accesso in caso di aggiornamenti mancanti.

MDM (Mobile Device Management)
Software per la gestione centralizzata e la protezione di dispositivi mobili come smartphone o tablet.

Malware
Software dannoso come virus, trojan o ransomware.

Segmentazione della rete
Suddivisione di una rete in aree separate per limitare gli attacchi (ad es. Wi-Fi per gli ospiti separato dalla contabilità).

Piano di emergenza (Incident Response Plan)
Documento che descrive come un'azienda deve reagire in caso di incidente informatico.

Passkey
Metodo di autenticazione senza password che utilizza chiavi crittografiche. Notevolmente più sicuro delle password classiche.

Patch / Patch Management
Aggiornamento software per colmare le lacune di sicurezza.
Patch Management = aggiornamento sistematico di tutti i dispositivi e le applicazioni.

Pentest (test di penetrazione)
Test mirato e definito che identifica i punti deboli in un'area specifica. Approccio strutturato e metodico.

Phishing
Messaggio manipolativo (di solito e-mail) per ottenere login, dati o denaro.

Ransomware
Malware che crittografa i dati e richiede un riscatto.

Rolling Backup / Backup offline
Backup conservato separatamente dalla rete (ad es. unità esterna, nastro). Protezione dal ransomware.

Social engineering
Manipolazione delle persone per ottenere informazioni riservate o accessi.

VPN (Virtual Private Network)
Connessione crittografata che consente una comunicazione sicura su Internet.

WLAN (Wireless Local Area Network)
Rete wireless. Le reti WLAN pubbliche o scarsamente protette possono facilitare gli attacchi.

Zero Trust
Principio di sicurezza: «Non fidarti di nessuno, controlla tutto». Nessuna fiducia automatica all'interno o all'esterno dell'azienda.