tnsolutions.it
FINE TECHNOLOGY



GUIDA 03 · CYBERSECURITY

Cybersecurity per PMI: proteggere rete, persone, dati e continuità operativa

Per le PMI: firewall e segmentazione, protezione endpoint, MFA, monitoraggio, vulnerability management e responsabilità dell'impresa, con le misure prioritarie.

REVISIONE TECNICA **Marco Ursoleo** CEO TN Solutions

Per: Titolari, direzioni e IT Manager di PMI, imprese manifatturiere, aziende di servizi e organizzazioni con più sedi

Versione 1.0 · 14/11/2026

IN QUESTA GUIDA

La sicurezza informatica assoluta non esiste, ma la differenza tra un'azienda preparata e una impreparata è enorme: nella probabilità di subire un attacco, nei danni che provoca e nel tempo necessario a ripartire. Questa guida mette in ordine le misure che contano di più.

1. Il problema: la PMI è un bersaglio, anche se "non ha niente da rubare" 3

2. Rete: firewall e segmentazione 4

3. Protezione endpoint, identità e accessi 5

4. Monitoraggio, gestione degli eventi e vulnerability management 6

5. Responsabilità cyber dell'impresa e rischi economici 7

6. Hector LIS e i servizi TN Solutions 8

7. Checklist delle misure prioritarie 9

A chi è rivolta

Titolari, direzioni e IT Manager di PMI, imprese manifatturiere, aziende di servizi e organizzazioni con più sedi.

Come usarla

Leggi i capitoli nell'ordine, poi compila la checklist finale: le voci con priorità alta sono quelle da affrontare per prime.

Download libero

Questa guida è gratuita e non richiede registrazione. Puoi condividerla con il tuo team.

Contenuti verificati da Marco Ursoleo, CEO di TN Solutions

Revisione tecnica completata il 14/11/2026. TN Solutions opera con sistema di gestione certificato ISO 9001 e ISO/IEC 27001. Per domande su questa guida: info@tnsolutions.it · 02 95 17 550.

1. Il problema: la PMI è un bersaglio, anche se “non ha niente da rubare”

Molti imprenditori pensano che gli attacchi informatici riguardino banche e grandi gruppi. In realtà gran parte degli attacchi è automatizzata: strumenti che scandagliano Internet alla ricerca di sistemi vulnerabili, campagne di phishing inviate a migliaia di indirizzi, credenziali rubate provate su servizi di posta e accesso remoto. Non serve essere un obiettivo “interessante”: basta essere raggiungibili e poco protetti.

I danni più comuni

Ransomware
dati e server cifrati, attività ferma, richiesta di riscatto.

Compromissione della posta
un account violato usato per frodi su pagamenti e fatture verso clienti e fornitori.

Furto di dati
informazioni di clienti, progetti, offerte e dati personali esfiltrati e talvolta pubblicati.

Fermo di produzione
nelle imprese manifatturiere, anche i sistemi collegati alle linee possono essere coinvolti.

In sintesi

La sicurezza non è un prodotto da installare una volta: è un insieme di misure tecniche, organizzative e di controllo che vanno mantenute nel tempo. Nessuna misura da sola è sufficiente; insieme riducono il rischio in modo significativo.



Schema originale: la difesa a livelli. Ogni strato compensa le debolezze degli altri.

2. Rete: firewall e segmentazione

Il firewall come punto di controllo

Il router fornito dall'operatore serve a collegarsi a Internet, non a proteggere l'azienda. Un firewall professionale permette di decidere quale traffico è ammesso, ispezionarlo, gestire accessi remoti sicuri e registrare gli eventi. Va però **configurato, aggiornato e controllato**: un firewall con regole "tutto aperto" o firmware vecchio offre una falsa sensazione di sicurezza.

Segmentazione della rete

Segmentare significa dividere la rete in zone separate (ad esempio con VLAN e regole tra di esse), in modo che un problema in una zona non si propaghi a tutte le altre.

Zona	Cosa contiene	Perché separarla
Utenti	PC e notebook del personale	Limitare la propagazione da una postazione infetta
Server	Gestionale, file server, database	Esporre solo i servizi necessari agli utenti
Ospiti	Visitatori e fornitori	Nessun accesso alle risorse interne
Dispositivi	Stampanti, telecamere, IoT	Spesso poco aggiornabili e vulnerabili
Produzione (OT)	Macchinari e sistemi di linea	Proteggere processi che non possono fermarsi
Gestione	Interfacce di amministrazione	Ridurre chi può raggiungerle

Accessi remoti

Desktop remoto esposto direttamente su Internet è una delle cause più frequenti di intrusione. Gli accessi da fuori sede devono passare da VPN o da soluzioni equivalenti con MFA, con permessi limitati a ciò che serve davvero.

3. Protezione endpoint, identità e accessi

Endpoint: oltre l'antivirus

Le soluzioni moderne di protezione degli endpoint (spesso indicate come EDR, Endpoint Detection and Response) non si limitano a riconoscere file noti: osservano i comportamenti sospetti, permettono di isolare un dispositivo e di ricostruire cosa è successo. Il loro valore dipende dalla **gestione centralizzata**: qualcuno deve ricevere gli avvisi e intervenire.

MFA e gestione degli accessi

L'autenticazione a più fattori (MFA) richiede, oltre alla password, una seconda prova di identità. È una delle misure con il miglior rapporto tra costo e riduzione del rischio, soprattutto su:

- posta elettronica e servizi cloud;
- accessi remoti e VPN;
- account amministrativi e console di gestione.

Approfondisci nella pagina dedicata all'autenticazione a due fattori in azienda.

Il principio del privilegio minimo

- Ogni utente ha solo i permessi necessari al proprio ruolo.
- Gli amministratori usano un account separato per le attività di gestione.
- Gli account di chi lascia l'azienda vengono disattivati il giorno stesso.
- Gli accessi di fornitori e consulenti sono nominativi, limitati e a scadenza.

Da dove cominciare?

Una prima telefonata gratuita con TN Solutions aiuta a capire quali misure hanno la priorità nel tuo contesto, senza impegno.

Richiedi una prima valutazione delle esigenze di sicurezza →

4. Monitoraggio, gestione degli eventi e vulnerability management

Monitorare per accorgersi in tempo

Firewall, server, endpoint e servizi cloud producono registri (log) e avvisi. Raccoglierli e analizzarli permette di accorgersi di comportamenti anomali: accessi da paesi insoliti, tentativi ripetuti di login, processi sospetti. Più velocemente si individua un incidente, più è contenuto il danno.

Per una PMI la domanda chiave non è "quale piattaforma comprare", ma **chi guarda gli avvisi e cosa fa quando arrivano**, anche fuori dall'orario di ufficio.

Vulnerability management

Le vulnerabilità sono difetti nei software e nei dispositivi che un attaccante può sfruttare. Gestirle è un ciclo continuo:

1. **Inventario**: sapere quali sistemi e software ci sono.
2. **Rilevazione**: verificare periodicamente le vulnerabilità note, ad esempio con un vulnerability assessment.
3. **Valutazione**: classificare il rischio, considerando gravità ed esposizione del sistema.
4. **Correzione**: aggiornare, mitigare o isolare, con priorità ai sistemi esposti su Internet.
5. **Verifica**: controllare che la correzione sia efficace.

> **Vulnerability assessment e penetration test**
>
> Un **vulnerability assessment** individua le vulnerabilità note in modo ampio e sistematico. Un **penetration test** simula un attacco reale su un perimetro concordato, per verificare cosa un attaccante potrebbe effettivamente ottenere. Sono attività diverse, da pianificare con obiettivi, perimetro e autorizzazioni scritte.

5. Responsabilità cyber dell'impresa e rischi economici

Una responsabilità della direzione

La sicurezza delle informazioni non è solo un tema tecnico. Il GDPR richiede misure tecniche e organizzative adeguate al rischio per proteggere i dati personali. Per i soggetti che rientrano nel suo ambito, la normativa NIS2 (recepita in Italia con il D.Lgs. 138/2024) attribuisce responsabilità precise anche agli organi di amministrazione. Anche quando un'azienda non rientra direttamente in questi obblighi, sempre più clienti e capofila chiedono ai fornitori evidenze sulla gestione della sicurezza.

Verificare se e come una specifica normativa si applica alla tua azienda richiede un'analisi caso per caso, anche con il supporto dei consulenti legali.

Le voci di costo di un incidente

Senza inventare medie, è utile conoscere le voci che compongono il danno, per valutarle sulla propria realtà:

Voce	Esempi
Fermo operativo	Ore di lavoro perse, ordini non evasi, penali contrattuali
Ripristino tecnico	Interventi straordinari, hardware, ricostruzione dei sistemi
Perdita di dati	Lavoro da rifare, informazioni non più recuperabili
Aspetti legali	Consulenze, eventuali notifiche e adempimenti
Reputazione	Fiducia di clienti e partner, opportunità perse
Frodi	Pagamenti dirottati tramite email compromesse

ESPERIENZA SUL CAMPO

Tra i casi pubblicati da TN Solutions ci sono il progetto NIS2 per una PMI manifatturiera, dall'assessment alla governance, e un progetto di infrastruttura IT e sicurezza per uno studio legale. Il sistema di gestione di TN Solutions è certificato ISO/IEC 27001 per la sicurezza delle informazioni.

6. Hector LIS e i servizi TN Solutions

TN Solutions affianca le aziende con servizi di sicurezza informatica e consulenza che coprono progettazione, gestione e verifica: firewall gestiti, protezione endpoint, vulnerability assessment e penetration test su perimetri concordati, supporto alla conformità.

> **Hector Lis: la prevenzione H24**
>
> Hector Lis è il componente di sicurezza dell'ecosistema Hector sviluppato da TN Solutions. È il motore della sicurezza gestita (SOC) prevista nei contratti di assistenza: monitoraggio attivo 24 ore su 24 basato su intelligenza artificiale, integrato con i firewall gestiti da TN Solutions, con processi tracciati secondo la certificazione ISO/IEC 27001.

Cosa ottieni da un percorso strutturato

- Una fotografia chiara dei rischi principali e delle misure già presenti.
- Un elenco di interventi con priorità, tempi e risorse stimate.
- Configurazioni documentate e verificabili.
- Un interlocutore che segue l'evoluzione delle minacce e aggiorna le misure nel tempo.

7. Checklist delle misure prioritarie

Misure di sicurezza per PMI	
☐ MFA attiva su posta, servizi cloud, VPN e account amministrativi	Alta
☐ Nessun servizio di desktop remoto esposto direttamente su Internet	Alta
☐ Sistemi operativi, firewall e applicazioni esposte aggiornati	Alta
☐ Protezione endpoint centralizzata con avvisi gestiti	Alta
☐ Backup con almeno una copia immutabile o offline	Alta
☐ Account amministrativi separati da quelli di uso quotidiano	Alta
☐ Firewall professionale configurato e documentato	Media
☐ Rete segmentata: utenti, server, ospiti, dispositivi	Media
☐ Vulnerability assessment periodico sui sistemi esposti	Media
☐ Raccolta e analisi dei log con una persona responsabile	Media
☐ Procedura scritta di gestione degli incidenti	Media
☐ Formazione periodica del personale su phishing e frodi	Media
☐ Verifica degli accessi di fornitori e consulenti	Bassa

⚠ Nessuna promessa di sicurezza totale

Queste misure riducono in modo significativo la probabilità e l'impatto degli incidenti, ma nessuna combinazione di tecnologie può garantire l'assenza di rischi. Per questo, accanto alla prevenzione, servono sempre backup verificati e un piano di risposta.

COME LAVORIAMO

Dal download alla soluzione, senza impegno nei primi passi

1 Download gratuito

Hai scaricato questa guida senza registrazione: usala per una prima autovalutazione.

2 Telefonata gratuita

Un incaricato TN Solutions ascolta le tue esigenze e ti aiuta a capire le priorità. È conoscitiva e senza impegno.

3 Audit avanzato (facoltativo, a pagamento)

Se serve un'analisi approfondita, con sopralluogo concordato, ricevi prima un preventivo dedicato. L'audit parte solo dopo che hai accettato il preventivo.

4 Proposta commerciale

Ricevi una proposta per i soli servizi necessari, con priorità e fasi di intervento.

Parla con noi
Prima telefonata gratuita e senza impegno

02 95 17 550 · info@tnsolutions.it · www.tnsolutions.it

Chi è TN Solutions

System integrator B2B con sede a Melzo (MI), operativo in Lombardia e da remoto su tutto il territorio nazionale. Dal 2001 progettiamo, integriamo e gestiamo infrastrutture IT per PMI, studi professionali, aziende di servizi, startup e imprese manifatturiere. L'azienda è guidata da **Marco Ursoleo**, CEO di TN Solutions.

Il sistema di gestione aziendale di TN Solutions è certificato **ISO 9001** (qualità) e **ISO/IEC 27001** (sicurezza delle informazioni). Le certificazioni riguardano i processi dell'azienda, non i singoli prodotti di terze parti citati in questa guida.

Servizi collegati a questa guida

Sicurezza Informatica
/it/sicurezza-informatica/

Hector Lis — prevenzione H24
/it/ecosistema-hector/hector-lis/

Contratto di sicurezza gestita (SOC)
/it/assistenza-informatica/contratti-assistenza-informatica/contratto-sicurezza-soc/

Installazione e gestione firewall aziendale
/it/sicurezza-informatica/gestione-firewall-e-installazione/

Autenticazione a due fattori in azienda
/it/autenticazione-due-fattori-mfa-azienda/

NIS2 per le PMI: cosa cambia
/it/nis2-cosa-cambia-per-le-pmi/

PROSSIMO PASSO

Vuoi capire come migliorare l'infrastruttura IT della tua azienda?

TN Solutions può aiutarti a valutare le esigenze, individuare le priorità e progettare la soluzione più adatta.

Richiedi una prima consulenza telefonica gratuita →

tnsolutions.it/it/contatti/

> Vuoi capire quali misure di sicurezza sono prioritarie per la tua azienda? Richiedi una prima valutazione delle esigenze.

TELEFONO 02 95 17 550

EMAIL info@tnsolutions.it

SITO WEB www.tnsolutions.it

SITO WEB

CONTATTI

tnsolutions.it
FINE TECHNOLOGY

TN Solutions · Viale Svezia 3, 20066 Melzo (MI) · 02 95 17 550 · info@tnsolutions.it · www.tnsolutions.it

Contenuto realizzato con il supporto dell'intelligenza artificiale. Revisione e supervisione tecnica: Marco Ursoleo, CEO TN Solutions.

TN Solutions — Guide tecniche per le imprese · Guida 3 · Versione 1.0 · 14/11/2026. Le informazioni hanno carattere divulgativo e non sostituiscono un'analisi tecnica specifica. Le tabelle economiche sono esempi illustrativi, non offerte né medie di mercato. I marchi citati appartengono ai rispettivi titolari.