20 ANNI DI SICUREZZA INFORMATICA PER PMI ITALIANE

PRIMA DI SPENDERE UN SOLO EURO IN UN "PEN TEST"

Leggi questo. Potrebbe farti risparmiare migliaia di euro —
o farti capire che stai già perdendo soldi ogni giorno senza saperlo.

GUIDA OPERATIVA GRATUITA · KEIDEA S.R.L.

LA COSA SCOMODA CHE NESSUNO TI DICE

Sai qual è il problema numero uno delle PMI italiane in materia di sicurezza informatica?

Non è che non investono. È che **investono male** — convinte di essere al sicuro quando non lo sono.

Il titolare medio di una PMI italiana pensa: *"Ho l'antivirus. Ho il firewall. Ho pagato qualcuno che mi ha detto che va tutto bene."*

E intanto il **75% degli attacchi informatici in Italia colpisce esattamente lui.** Non le banche. Non le multinazionali. Lui. La PMI con 15, 30, 50 dipendenti. Il sito e-commerce che fattura 800.000 euro l'anno. Il portale clienti con anni di dati sensibili dentro.

Il motivo è brutalmente semplice: **le grandi aziende investono seriamente in sicurezza. Le PMI comprano la sensazione di sicurezza.** E c'è un mercato intero costruito per vendergliela.

Noi di Keidea S.r.l. siamo nel settore da **20 anni.** Abbiamo visto questo film centinaia di volte. E ogni volta che una PMI italiana subisce un attacco che avremmo potuto prevenire, ci fa lo stesso effetto.

Questo documento esiste per una ragione sola: darti gli strumenti per capire, da solo, se sei davvero pronto per un pen test professionale — o se stai per buttare soldi in qualcosa che non ti servirà a niente.

Leggilo fino in fondo. Nell'ultima sezione c'è qualcosa che non puoi ignorare — e una finestra temporale che si chiude.

PRIMA DOMANDA SERIA: SAI COSA SEI ANDATO A COMPRARE?

Quando cerchi “pen test” su Google e ricevi preventivi che vanno da 400 euro a 15.000 euro per lo stesso servizio, una delle due cose è vera:

O c'è qualcuno che ti sta facendo pagare troppo. O c'è qualcuno che ti sta vendendo qualcosa di completamente diverso da quello che pensi di comprare.

Nella stragrande maggioranza dei casi, è la seconda.

✓ PEN TEST PROFESSIONALE	✗ VULNERABILITY SCAN AUTOMATICO
Simulazione manuale di un attacco reale condotta da un professionista certificato con metodologia OWASP	Software automatico che confronta la tua configurazione con un database di problemi noti e genera un PDF
Concatena le vulnerabilità — verifica cosa succede davvero se qualcuno vuole fare del male alla tua azienda	Non verifica se le vulnerabilità sono realmente sfruttabili nel tuo contesto specifico

Report operativo con priorità di remediation personalizzate	Report generico — spesso pre-compilato prima ancora di iniziare

Noi consigliamo sempre — prima ancora di parlare di costi — di fare una **valutazione seria della propria situazione.** Un pen test fatto nel momento sbagliato, o fatto male, non ti protegge: ti dà un falso senso di sicurezza. E il falso senso di sicurezza è più pericoloso di non avere nessuna sicurezza.

SEZIONE 1 — SEI DAVVERO PRONTO PER UN PEN TEST?

La checklist che i tuoi fornitori non vogliono che tu faccia

Rispondi onestamente. **Sì o no.** Niente “dipende”, niente “più o meno”.

DOMANDA 1 — CMS E PLUGIN AGGIORNATI

Il tuo CMS e tutti i plugin installati sono aggiornati all'ultima versione disponibile?

■ *Sì* ■ *No* ■ *Non lo so*

> *Se hai risposto No o Non lo so: il 60% delle violazioni su siti PMI italiani sfrutta vulnerabilità note in plugin non aggiornati — già documentate pubblicamente, trovabili su Google in 30 secondi. Aggiorna prima. Poi torna qui.*

DOMANDA 2 — AUTENTICAZIONE A DUE FATTORI

Hai il 2FA attivo su tutti gli accessi critici: pannello hosting, area admin, email aziendale, gestionale, VPN?

■ *Sì* ■ *No* ■ *Solo su alcuni*

> *Se hai risposto No o Solo su alcuni: la tua porta principale è aperta. Un pen test che trova vulnerabilità sofisticate mentre la password dell'admin è “NomeDitta2024!” è un esercizio accademico. Prima chiudi le vulnerabilità banali.*

DOMANDA 3 — BACKUP TESTATO E FUNZIONANTE

Hai un backup recente (max 7 giorni), completo e testato dei tuoi sistemi?

■ *Sì, testato* ■ *Sì, non testato* ■ *No*

> *Un backup non testato non è un backup: è una speranza. Se un attaccante sfrutta le vulnerabilità prima che tu le corregga e non hai un ripristino funzionante, il pen test ti dice solo come sei stato distrutto.*

DOMANDA 4 — MAPPA DEI SERVIZI ESPOSTI

Sai esattamente quali porte, servizi e sottodomini della tua azienda sono esposti su internet in questo momento?

■ *Sì, ho una mappa* ■ *Più o meno* ■ *No*

> *Uno dei pattern più comuni: servizi dimenticati esposti su internet. Un vecchio ambiente di test, un sottodominio di sviluppo, una porta aperta su un server non più in uso. Non puoi testare la sicurezza di qualcosa che non sai di avere.*

DOMANDA 5 — INCIDENTI NEGLI ULTIMI 12 MESI

Hai già subito un incidente informatico, un accesso anomalo o una mail di phishing andata a buon fine negli ultimi 12 mesi?

■ *No, mai* ■ *Sì, risolto* ■ *Sì, non sono sicuro*

> *Se hai risposto Sì e non sono sicuro: il pen test smette di essere consigliabile e diventa urgente. Un attaccante che ha già avuto accesso ai tuoi sistemi potrebbe aver lasciato una backdoor. Sapere se è così non è una scelta.*

DOMANDA 6 — REQUISITI DI SUPPLY CHAIN

I tuoi clienti principali ti hanno chiesto documentazione sulla sicurezza informatica come requisito per lavorare insieme?

■ *No, mai* ■ *Qualche volta* ■ *Sì, requisito esplicito*

> *Se hai risposto Sì, è diventato un requisito esplicito: non stai più scegliendo se fare sicurezza informatica. Il mercato lo sta scegliendo per te. Chi non ha documentazione perde contratti. Punto.*

DOMANDA 7 — REFERENTE PER LA REMEDIATION

Hai un referente (interno o esterno) che può gestire la fase di correzione delle vulnerabilità dopo il pen test?

■ *Sì* ■ *No*

> *Un pen test senza remediation è un referto medico che non porti mai dal dottore. Identificare le vulnerabilità è il primo passo, non l'ultimo. Se non hai nessuno che le corregge, il documento che ricevi vale zero.*

DOMANDA 8 — MODIFICHE INFRASTRUTTURALI RECENTI

Hai effettuato migrazioni o modifiche infrastrutturali significative nell'ultimo anno?

■ *No* ■ *Modifiche minori* ■ *Cambiamenti rilevanti*

> *Ogni cambiamento rilevante reimposta il perimetro di rischio. Ciò che era sicuro prima potrebbe non esserlo più dopo. Se hai cambiato qualcosa di importante, il tuo ultimo pen test potrebbe già essere obsoleto.*

IL RISULTATO DELLA TUA CHECKLIST

Conta i Sì alle domande 1, 2, 3, 4, 5, 7.

DA 0 A 4 SÌ

IL PEN TEST È PREMATURO

Non perché non ne hai bisogno — probabilmente ne hai più bisogno di chi ne ha 6 su 6 — ma perché farlo adesso significa spendere soldi per scoprire problemi che puoi correggere da solo, questa settimana, gratuitamente.

Aggiorna tutto il software. Attiva il 2FA. Testa il backup. Mappa i servizi esposti. Poi torna a questa checklist.

Se non sai da dove iniziare, chiamaci. La valutazione preliminare con Keidea è gratuita e senza impegno.

DA 5 A 8 SÌ

SEI PRONTO. ORA IL PROBLEMA È ASPETTARE.

Hai le basi. Hai fatto il lavoro preparatorio. Ora il rischio non è sprecare soldi in preparazione inutile.

Il rischio è aspettare.

Leggi la Sezione 3 su NIS2. È la parte più importante di questo documento — e contiene una finestra temporale che si sta chiudendo.

SEZIONE 2 — QUANTO COSTA DAVVERO UN PEN TEST PER UNA PMI ITALIANA

Secondo le nostre analisi — basate su 20 anni di lavoro con PMI italiane — questi sono i range reali nel 2025–2026.

TIPO DI PMI	OGGETTO DEL TEST	RANGE REALE
Sito vetrina / brochure	Web app semplice, nessun login	**1.500 – 3.000 €**
E-commerce / SaaS semplice	Web app + checkout + login	**3.000 – 5.500 €**
Portale con area riservata clienti	Web app + autenticazioni + dati sensibili	**4.000 – 7.000 €**
PMI manifatturiera rete esposta	Network esterno (20–50 IP)	**3.500 – 6.000 €**
Software house / SaaS articolato	Web app + API + ambienti multipli	**6.000 – 12.000 €**
Infrastruttura complessa	Full pen test (rete + app + social eng.)	**12.000 – 20.000 €**

TRE SEGNALI CHE STAI PER COMPRARE FUFFA

- **Preventivo sotto i 1.500€** per qualsiasi web application test. Matematicamente impossibile per un lavoro manuale serio.

■ **Nessuna fase di scoping** prima del preventivo. Chi non ti fa domande non sa cosa sta quotando. Sta sparando un numero a caso.

■ **Report consegnato in meno di 48 ore** dalla fine del test. Significa che era già pronto prima di iniziare.

SEZIONE 3 — LA SCADENZA CHE NON PUOI IGNORARE

Qui smettiamo di essere gentili.

La Direttiva NIS2, recepita in Italia con il **D.Lgs. 138/2024**, ha una scadenza operativa concreta: **ottobre 2026.**

Se la tua PMI ha più di 50 dipendenti o supera i 10 milioni di euro di fatturato in un settore critico — energia, sanità, logistica, manifattura, servizi digitali, IT — sei **direttamente obbligato. Punto.**

Ma anche se sei sotto queste soglie, c'è un fatto che quasi nessuno ti sta dicendo chiaramente: **se lavori come fornitore di un'azienda che è nel perimetro NIS2, quella azienda è obbligata a valutare la tua postura di sicurezza.** Il che significa che potresti perdere contratti importanti non perché sei stato attaccato, ma perché non riesci a dimostrare di essere sicuro.

■ ARTICOLO 23 — D.LGS. 138/2024

La legge stabilisce la **responsabilità personale dei vertici aziendali.** Non dell'IT. Non del consulente esterno. Non del sistemista che "gestisce tutto lui."

Tua. Dell'Amministratore Delegato. Personalmente.

In caso di mancata conformità, i dirigenti possono essere soggetti a sospensione temporanea dall'esercizio delle funzioni. Le sanzioni arrivano a **7 milioni di euro** per i soggetti importanti.

LA MATEMATICA DEI MESI RIMASTI

ORA	4–6 MESI	OTT 2026
Valutazione preliminare scoping e planning	Assessment + Pen test remediation + retest	Scadenza operativa misure di sicurezza NIS2

Ottobre 2026 sembra lontano. Non lo è. Un percorso di adeguamento serio per una PMI richiede mediamente 4–6 mesi. I fornitori qualificati stanno già ricevendo richieste in aumento. Chi aspetta la primavera del 2026 si troverà con fornitori saturi, tempi più lunghi e prezzi più alti.

Il momento giusto per muoversi è **adesso.** Non perché lo diciamo noi. Perché la matematica dei mesi rimasti lo dice.

L'UNICA COSA CHE TI CHIEDIAMO DI FARE ADESSO

Hai la checklist. Hai i range di costo reali. Hai la mappa delle scadenze normative. Hai tutto quello che ti serve per non farti vendere qualcosa che non vale.

Adesso manca un pezzo solo: qualcuno che ti dica esattamente dove si trova la tua azienda in questo momento — e cosa fare per portarla dove deve essere.

Noi di Keidea S.r.l. facciamo questa cosa da **20 anni.** Non vendiamo prodotti. Non abbiamo software proprietari da piazzarti. Vendiamo competenza, metodologia e risultati verificabili su PMI italiane reali, con budget reali, con problemi reali.

POSTI LIMITATI OGNI MESE — ECCO PERCHÉ

Ogni mese apriamo un numero limitato di sessioni di valutazione preliminare gratuita con un nostro consulente tecnico senior. Non un commerciale. Non uno che legge uno script.

Perché limitiamo i posti? Perché ogni sessione richiede la preparazione di un consulente dedicato. Non è una trovata pubblicitaria: è il modo in cui garantiamo che ogni azienda che si siede con noi riceva attenzione reale — non una chiacchierata generica da call center.

I posti per questo mese si stanno esaurendo.

Se stai leggendo questo documento e hai già risposto alla checklist, hai già fatto il lavoro più difficile: hai capito dove stai. Il passo successivo richiede trenta secondi.

CONTATTACI ORA — PRIMA CHE I POSTI FINISCANO

■ Chiamaci direttamente:

0835 239514

Lun–Ven, orario ufficio — risponde un consulente, non un centralino

✉ Scrivici subito:

info@keideasrl.it

Oggetto: "Checklist Pen Test — Richiesta Valutazione"

Ti risponderemo entro 24 ore lavorative per fissare la tua sessione gratuita.

Keidea S.r.l. — 20 anni di sicurezza informatica per PMI italiane

Non vendiamo sicurezza sulla carta. La costruiamo insieme.