



fowhe.com

Security Assessment

Soluzioni e servizi di Cyber Security per le piccole e medie imprese



Contenuti

»» Perchè	→	Pagina 3
»» Esempi tipici di attacchi	→	Pagina 4
»» Il Security Assessment	→	Pagina 5
»» Il nostro approccio	→	Pagina 6
»» Chi siamo	→	Pagina 7
»» Contatti	→	Pagina 8



Perchè

Le piccole imprese e gli studi professionali sono vittime frequenti di phishing, ransomware e data breach. Compromettere i dati dei clienti comporta, oltre al blocco operativo ed al disagio interno, anche il danneggiamento della reputazione costruita in anni di lavoro.

Secondo SpyHunter, almeno il 50% delle piccole imprese ha subito un attacco informatico nell'ultimo anno ed in Italia, secondo Confartigianato, il 15,8 % delle imprese ha sperimentato almeno un incidente cui è seguita un'interruzione dei servizi ICT, distruzione o divulgazione dati.

50%

Le aziende che hanno subito un attacco nell'ultimo anno (1)

15%

Le imprese che hanno sperimentato almeno un blocco (2)

60%

Le aziende che hanno subito danni a causa di attacchi (3)

45%

La crescita delle denunce di reati informatici contro imprese tra 2019-2023 (4)

1) SpyHunter – “36 Important Small Business Cybersecurity Statistics (2025) - [Fonte SpyHunter](#) | **2)** Confartigianato - [Fonte Ansa](#) |
3) Global Data Protection Index / Dell Technologies - [Fonte Topvendors.it](#) | **4)** Confartigianato [Fonte Federprivacy](#).

Il Security Assessment è il primo passo da compiere per conoscere i punti deboli della propria infrastruttura e proteggerla.

Inoltre, la maggior parte degli attacchi informatici va a segno a causa della mancanza di formazione del personale.





Esempi tipici di attacchi

Eccovi tre esempi tipici, basati su fatti reali e su dati aggregati, che servono come "campanelli d'allarme", di attacchi informatici frequenti con i quali avrai già fatto conoscenza:



Phishing / Compromissione email aziendale

Contesto / vittima: Studio professionale con dipendenti che usano posta elettronica per fatturazione e contatti clienti

Come è avvenuto l'attacco: Mail fasulla inviata all'amministratore che sembra proveniente da fornitore; click su link, credenziali rubate

Conseguenze: Accesso abusivo, invio di false fatture, perdita reputazione, tempo per ripristinare l'account compromesso



Ransomware via vulnerabilità non patchata

Contesto / vittima: Piccola azienda con server locale / workstation non aggiornate

Come è avvenuto l'attacco: Malware penetrato via vulnerabilità nota non corretta, cifratura dei dati inclusi backup locale

Conseguenze: Blocco attività per giorni, richiesta di riscatto, perdita di alcuni dati non recuperabili



Data breach / perdita dati da sistema cloud mal configurato

Contesto / vittima: Studio che utilizza servizi cloud per archiviare dati sensibili

Come è avvenuto l'attacco: Cartelle condivise erroneamente configurate "pubbliche", nessun monitoraggio accessi

Conseguenze: Dati clienti accessibili da estranei, obblighi legali + sanzioni GDPR, danno reputazionale



Le PMI sono particolarmente vulnerabili: la maggior parte degli attacchi ransomware colpisce aziende con fatturato inferiore ai 250 milioni di euro. **Gli attacchi basati su fattore umano (es. phishing, credenziali compromesse) continuano ad essere tra i vettori più usati.**



Il Security Assessment

Cos'è

Il Security Assessment è il **primo passo da compiere per conoscere i punti deboli della propria infrastruttura IT** e proteggere i propri dati e sistemi. Fowhe propone un servizio mirato ed accessibile, che abbiamo il piacere di illustrarti.

Qual'è l'obiettivo

Verificare la sicurezza della vostra infrastruttura IT (server, workstation, rete LAN/Wi-Fi, servizi cloud, applicazioni web, backup, policy e consapevolezza del personale), produrre osservazioni tecniche, priorità di mitigazione, un piano di remediation, soluzioni di firewalling e backup resiliente e, soprattutto, **formazione del personale**.

Perchè farlo ora

Ogni giorno le piccole e medie imprese sono bersaglio di attacchi informatici che possono bloccare l'attività, compromettere i dati dei clienti e **danneggiare la reputazione costruita in anni di lavoro**. Investire subito nella sicurezza digitale significa ridurre i rischi, proteggere il proprio valore e garantire continuità al proprio business.





Il nostro approccio

Il Security Assessment viene svolto all'incirca entro un mese dall'ingaggio (tempo che varia ovviamente in funzione delle dimensioni aziendali e dell'infrastruttura IT) e si sviluppa nei seguenti step:



Step 1

Presentazione presso la vostra sede della strategia di Security Assessment, raccolta documentazione ed autorizzazioni. Inventory e redazione del preventivo.

Step 2

Ricognizione passiva e scan non invasivo, analisi vulnerabilità e test controllati. Interazione con il/i vostro/i referente/i informatico/i e fornitori di servizi IT.

Step 3

Test fisico Wi-Fi / social engineering (se autorizzati). Verifica efficacia sistemi di backup e firewall, se presenti.

Step 4

Redazione report tecnico, remediation plan, proposte di upgrade infrastrutturale. Consegna e formazione.

Tutte le attività verranno effettuate senza interrompere l'operatività dell'azienda ma è essenziale che il vostro tecnico informatico si renda disponibile a collaborare per fornire le informazioni necessarie all'inventory e che il vostro personale partecipi attivamente alla formazione finale.

Chi siamo



www.fowhe.com/it/index



Fowhe è dal 2007 fornitore di servizi ed operatore di TLC, focalizzato sul settore business che progetta ed implementa soluzioni IT, favorendo la transizione digitale delle piccole e medie imprese e delle PA del territorio. Il team di Fowhe è costituito da **Ingegneri informatici, Ingegneri delle telecomunicazioni, tecnici specializzati nel settore dei sistemi e delle reti.**

Fowhe dispone di risorse di rete e datacenter sul territorio Pugliese e, secondo l'analisi 2025 di Plimsoll Italia sulle 524 aziende del settore, Fowhe si posiziona 31a tra le imprese del settore con maggior margine di profitto (www.plimsoll.it).



1 E' operatore di TLC

Fowhe è autorizzata dal 2007 ai sensi dell'articolo 25 del Decreto Legislativo n. 259/2003 e ss.mm.ii. del Codice delle comunicazioni elettroniche, è titolare di autorizzazione generale per l'offerta al pubblico di servizi di comunicazione elettronica, è titolare di autorizzazione generale per l'installazione e la fornitura di reti pubbliche di comunicazioni.

2 E' Autonomous System

Fowhe è Autonomous System con numero AS60443, presente nei principali Internet Exchange Point nazionali e dispone di risorse IT/TLC sul territorio Pugliese. Questo gli consente di essere un operatore di rete indipendente che implementa ed eroga i migliori servizi disponibili.

3 E' parte dell'ecosistema di Internet

Fowhe è socia dei consorzi e delle associazioni che rappresentano l'ecosistema di Internet come il Roma Internet Exchange Point (NAMEX), il Regional Internet Registry for Europe (RIPE), l'Associazione di Provider Internet Indipendenti Italiani (Assoprovider).

4 E' costantemente aggiornata

Il Team di Fowhe partecipa ai principali eventi e conferenze che interessano il mondo dell'informatica e delle telecomunicazioni restando sempre al passo con le innovazioni e le tendenze del settore.



Contatti

Website

www.fowhe.com/it/index

Telefono

+ (39) **06 90285189**

E-mail

business@fowhe.com

Social Media

www.linkedin.com/company/fowhe-s-r-l

Head quarter

Via A. Salandra 18 - ROMA

Sedi operative

Via Assunta 19 - MARTANO (LE)

Viale Donato De Leonardis zona ASI - BARI

