



Vulnerability Assessment Penetration test

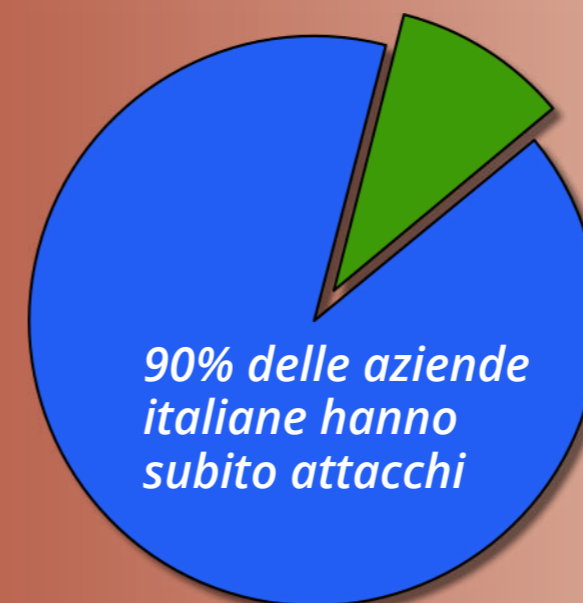
Verifica la **sicurezza** del tuo reparto IT

Individua le minacce prima che diventino un problema

Implementa soluzioni per aumentare la protezione



I tuoi dati sono a rischio.
I dati della tua azienda sono a rischio.
I dati dei tuoi clienti sono a rischio.
Puoi sostenere il contrario?



Fonte: [Il Sole 24 Ore](#)

Le aziende Italiane sembra abbiano un problema, non prendono abbastanza sul serio la sicurezza informatica: **il 90% di esse ha subito un attacco andato a buon fine.**

La soluzione? **Progettare un piano di prevenzione efficace**, che permetta di intercettare le minacce e mitigare gli attacchi in breve tempo.

Secure Online Desktop offre diversi servizi per la gestione della sicurezza aziendale.

I principali, che ogni azienda di medie dimensioni dovrebbe implementare sono:

Vulnerability Assessment & Penetration testing



Il nostro approccio

Come indicato nel grafico qui accanto, l'approccio si divide in una **prima fase di Vulnerability Assessment**, grazie alla quale viene effettuata una scansione del sistema e vengono **individuate le potenziali minacce**. Questa fase include i passaggi da 1 a 3 nello schema.

Se l'intervento non prevede un Penetration Test, allora **viene radatto un rapporto con quello che è stato individuato**, vengono consigliate delle soluzioni per tentare di eliminare i problemi, ma la loro messa in pratica è lasciata al cliente.

Nel caso che l'intervento lo preveda, una volta individuate le potenziali minacce, **vengono testate e messe alla prova tramite un Penetration Test** per verificare le problematiche e individuare a quali tecniche il sistema sia più vulnerabile.

Il sistema è messo alla prova da un team di hacker etici che verificano se ci sia la possibilità di penetrare nel sistema in un qualunque modo.

Alcune delle tecniche utilizzate per i test

- **Network Sniffing:** Intercettazione analisi dei pacchetti intercettati
- **IP port scanning:** Scansione della rete per individuare vie di accesso
- **ARP spoofing:** Attacchi di tipo man-in-the-middle ai danni della rete
- **Deduzione password:** Tentativi di carpire e dedurre password di sistema
- **Controllo dei sistemi:** Tentativo di controllo remoto dei sistemi coinvolti



Come funziona il processo di ingaggio di Secure Online Desktop



Il cliente richiede supporto tramite il sito



La richiesta viene valutata e genera una proposta di intervento



La proposta viene sottoposta al cliente e accettata



Iniziano Vulnerability Assessment e Penetration Test



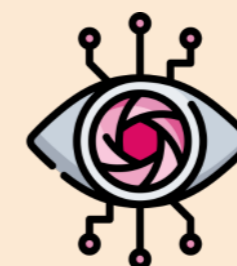
Le minacce vengono mitigate e le brecce riparate (opzionale)



Restiamo a disposizione per ulteriori interventi e verifiche



Al termine sono redatti dei report consegnati al cliente



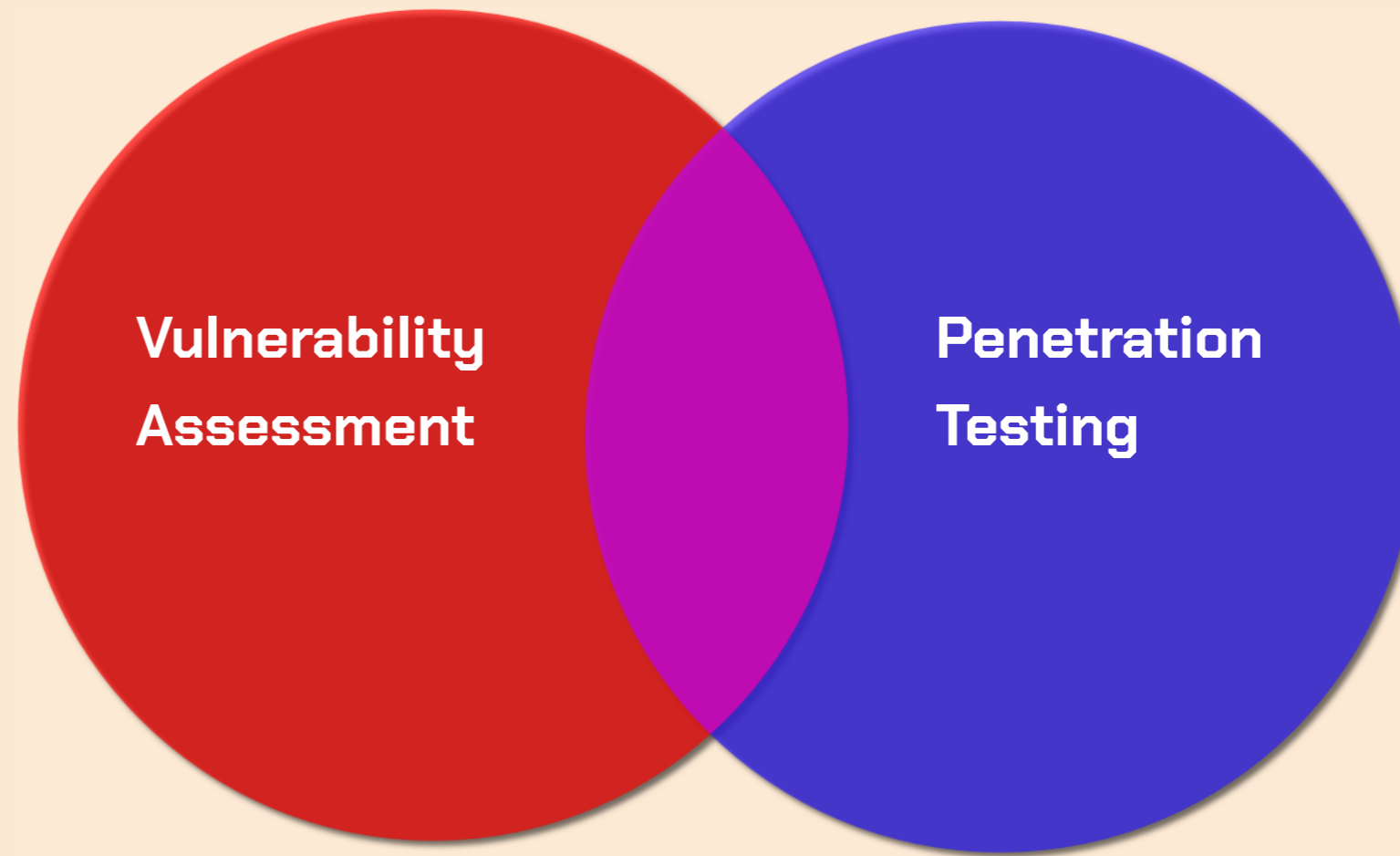
Minacce e falle di sistema sono individuate e testate



Vulnerability Assessment vs. Penetration Testing

Scegliere come procedere

Quando si tratta di scegliere se svolgere uno solo dei procedimenti o entrambi, **bisogna valutare sulle basi dei risultati richiesti**. Se si vuole solo avere una panoramica generale, allora ci si può fermare con un VA. Nel caso in cui si scelga di **umentare la sicurezza generale del sistema**, il consiglio è di svolgere VA regolari nel tempo e PT saltuari come verifica, magari dopo un aggiornamento.



	Vulnerability Assessment	Penetration test
Scopo	Scoprire i punti deboli del sistema	Scoprire e sfruttare punti deboli
Risultati prodotti	Lista di possibili brecche e debolezze	Lista delle vulnerabilità, come sfruttarle e raccomandazioni
Passi successivi	Prioritizzare azioni per arginare le falle	Arginare le falle e riparare il sistema

Scegli la sicurezza per la tua azienda

**Dal 2011 ci occupiamo di tecnologia Cloud e di sicurezza,
affidati a dei professionisti esperti!**

Scopri il servizio sul sito

Per ulteriori informazioni, i nostri contatti sono:

Via Zacchetti 6, 42124 - Reggio nell'Emilia (RE)

www.secure-od.com

Tel. +39 0522 1685330

Fax. +39 0522 015371

E-mail: info@secure-od.com

Pec: secure-od@pec.it

