

# Il Security Workshop

## L'importanza della consapevolezza del rischio in azienda

Essere professionisti nella moderna Net-Economy significa accedere quotidianamente ai sistemi e ai dati presenti nella propria rete aziendale e ad Internet.

Stiamo assistendo ad una corsa sfrenata all'ammodernamento dei sistemi e delle infrastrutture informative per rendere tutti i dati condivisibili e raggiungibili velocemente. Tutte operazioni che tendono ad allargare il proprio business.

Ma quante aziende sono preparate a prevenire e identificare

anche gli attacchi alla propria rete informatica, o a capire se sono state vittime di furto di dati sensibili a scopo fraudolento?

NEST2 nella piena consapevolezza che gli attacchi informatici non possono essere sottovalutati, ha studiato un servizio di consulenza rivolto ai responsabili IT per diffondere la consapevolezza del rischio e l'educazione alla sicurezza informatica, in modo da trasmettere i principi basilari su cui deve poggiare una corretta politica dei sistemi informatici aziendali.

### Premessa

Pensiamo ai dati e alle informazioni scambiate tutti i giorni con clienti, partner e fornitori attraverso i mezzi informatici.

Non è così inverosimile sentir sempre più spesso parlare di violazioni di sistemi quali banche, attività commerciali o strutture governative.

Senza la consapevolezza del rischio che si nasconde nella Rete, non è possibile attuare una **corretta politica aziendale volta alla difesa del proprio sistema informatico**.

Sempre più aziende sentono la necessità di trovare sul mercato soluzioni efficaci per la sicurezza informatica, per non esporre la propria rete ad attacchi informatici o pericoli che possono alla lunga danneggiarla.

La **sicurezza informatica** sta quindi diventando uno dei maggiori elementi di valutazione nella gestione aziendale.

### Obiettivi

Per diffondere la consapevolezza del rischio e l'educazione alla sicurezza informatica, **NEST2** propone alle aziende il **Security Workshop**.

Si tratta di un servizio di consulenza, assistito dagli esperti della Divisione Sicurezza di NEST2, della durata di una giornata, finalizzato all'introduzione dei principi basilari su cui deve poggiare una corretta politica della sicurezza informatica.

Il Security Workshop si rivolge principalmente al **personale tecnico IT** o comunque al personale che riveste ruoli di responsabilità per la sicurezza informatica aziendale.

È un momento di studio ed analisi progettato per fornire un **metodo di paragone tra lo stato effettivo della sicurezza di una rete e lo stato "a regola d'arte"**, ma soprattutto per **identificare le aree a rischio** che necessitano di interventi immediati.



L'organizzazione del servizio viene stabilita e personalizzata secondo le reali necessità del cliente, ma è possibile definire un'agenda tipica che include i seguenti argomenti:

1 Introduzione al Security Workshop	4 Politiche di sicurezza informatica	7 Valutazione rischio/danno e costi
2 Panoramica sulla sicurezza informatica (gli elementi chiave)	5 Lo standard di sicurezza BS7799	8 Le soluzioni di sicurezza informatica
3 I fattori critici di successo	6 Analisi della sicurezza informatica	9 Conclusioni e passi successivi

## Vantaggi

Il **Security Workshop di NEST2** è uno strumento formativo che può apportare in azienda i seguenti vantaggi:

- Ottenere migliori conoscenze dei problemi più attuali in ambito di sicurezza informatica
- Conoscere le migliori tecniche di difesa e prevenzione
- Identificare le aree ad alto rischio nella propria infrastruttura IT
- Ottenere informazioni specifiche sulle priorità attribuibili agli interventi per la riduzione dei rischi informatici

## Applicazioni

Possono organizzare un Security Workshop sia aziende che possiedono un'infrastruttura ICT, sia aziende (p.e. la piccola azienda che si rivolge prevalentemente a fornitori esterni) che vogliono comunque acquisire la conoscenza dei rischi effettivi che possono minacciare l'integrità o la confidenzialità dei propri dati e/o della propria rete, in modo da disporre di sufficienti informazioni per una prima valutazione di eventuali azioni preventive.

