LA SICUREZZA CIBERNETICA…COSE DA SAPERE

Tra settembre 2015 e settembre 2016 il 45,2% delle imprese italiane ha subito almeno un attacco cibernetico che ha provocato danni;

Il numero di attacchi è in continua crescita, così come il loro livello di complessità;

il motivo degli attacchi è lo spionaggio industriale e commerciale, il "mercato nero" delle informazioni o la volontà di arrecare un danno a in concorrente.

Le minacce al cyberspace hanno oggi forme diverse e coinvolgono diversi attori: professionisti della cyber intelligence, attivisti o hacktivist, vere e proprie bande criminali, nonché violazioni "dall'interno" delle aziende.

Il processo di digitalizzazione comporta senza dubbio nuove opportunità per privati, aziende e istituzioni dando origine a straordinarie capacità sempre più immateriali.
In questo scenario vengono scambiate ogni giorno notizie, conoscenze, dati, presentazioni professionali ma anche relazioni personali e interessi: una quantità infinita di informazioni esclusive che permette di vivere meglio la vita sociale e professionale ma che, al tempo stesso, può costituire anche un vantaggio competitivo per chiunque ne venga a conoscenza.
In un sistema socio-economico aperto ed estremamente dinamico quale quello attuale, al crescere delle opportunità corrisponde un analogo incremento delle minacce.

Il rischio cibernetico esiste.
Da attacchi e violazioni possono derivare danni economici rilevanti.
Si comincia quindi a valutare la sicurezza cibernetica come un fattore di stabilità per i Paesi ed un asset per le singole imprese.
Alcuni Paesi inoltre stanno introducendo, per la partecipazione alle gare o successivamente agli appaltatori, il deposito delle misure di sicurezza cibernetica adottate ai sensi della policy aziendale di sicurezza logica.
L'Unione Europea, nel luglio 2016, ha varato la **Direttiva NIS** (Network and Information Security) sui requisiti minimi per la sicurezza informatica delle reti e delle informazioni.
La Direttiva prevede l'istituzione di una "Autorità" nazionale, che potrà imporre standard di sicurezza alle aziende e sanzionarle in caso di inosservanza.
Le aziende avranno l'obbligo legale di adeguarsi entro **maggio 2018**.
Le aziende devono comunque essere già conformi alle misure minime di sicurezza previste dalla legge sulla privacy (196/2003).

Cosa può offrire Sicuritalia:

- competenza ed esperienza per supportare le aziende nel processo di miglioramento della sicurezza logica;
- soluzioni e prodotti a norma ISO 27000 da fornire alle aziende;
- sviluppo di altre soluzioni personalizzate;
- applicazione di un metodo efficace per controllare la sicurezza del sistema informativo aziendale.