SCENARIO Un effetto dell'attuale pandemia è stata la necessità da parte delle imprese di attivare al massimo la modalità di "**lavoro agile"**, utilizzando sovente sistemi non ancora consolidati ed a volte assolutamente non testati.

Questa nuova operatività sta esponendo le aziende a **maggior rischio di violazione dei propri sistemi informatici**, in quanto si ha un enorme flusso di accessi ad infrastrutture aziendali anche da dispositivi personali e con l'utilizzo di connessioni *vpn* sovente poco testate sul carico e non aggiornate su vulnerabilità critiche di sicurezza.

RIMEDI Le aziende devono, quindi, prevedere un **puntuale *cyber assessment*** con supporto specialistico indirizzato prevenire eventuali attacchi sui punti deboli ed affiancare una **copertura assicurativa** a copertura delle spese, dei danni e delle perdite a seguito di violazione del proprio sistema informatico.

COPERTURA ASSICURATIVA

COSA COPRE

- Responsabilita' verso terzi: **Risarcimento di danni a terzi,** compresi i costi di difesa conseguenti ad una falla nella sicurezza del sistema informatico (intrusione, accesso non autorizzato, *malware*, perdita di dati per furto/smarrimento di *devices*) e violazione di informazioni riservate
- Danni propri:
  1) **Diminuzione dell'utile netto,** comprese le maggiori spese per prosieguo dell'attività e/o per diminuire e ridurre le perdite, a seguito di sospensione o interruzione del servizio fornito dal sistema informatico e/o impossibilità di accedere ai dati, a causa di cancellazione o danneggiamento dei dati, anche se causata da **errore di un dipendente**.
  2) **Costi** relativi a sevizi di assistenza legale, servizi informatici, ripristino dati, tutela reputazione, a seguito di violazione di informazioni riservate, falla nella sicurezza del sistema informatico, disfunzione operativa (**errore di un dipendente**) e danneggiamento o distruzione del sistema informatico causato da **evento accidentale esterno.**
  3) **Somma di denaro** o altro pagato a seguito di una minaccia di attacco informatico (**Cyber estorsione).**

FORMULAZIONE PREVENTIVO

Per ottenere un preventivo e' sufficiente la compilazione del questionario allegato

INDICAZIONE DI PREMIO

Un premio base di riferimento per un Istituto medio è di circa **€ 1.500,00/€ 2.000,00**

OPERATIVITA'

Al verificarsi di un evento previsto dalla polizza e' prevista l'attivazione **del servizio di pronto intervento** che prevede accesso, in emergenza, a un team di consulenti che possono fornire supporto critico e una risposta coordinata. Risposta entro un'ora dalla violazione dei sistemi, i consulenti informatici, legali e di pubbliche relazioni si attivano per contenere il rischio reputazionale e per contenere il danno.

Sella Broker S.p.A.