Tiratura: 20.000 Diffusione: 19.000

giornale delle Assicurazioni

Mensile

Data 04-2018
Pagina 27
Foglio 1

Crimine informatico in crescita e nuove norme UE. Le soluzioni (assicurative) ci sono

Federico Capuzzo

Il crimine viaggia sempre più online, al punto che l'anno appena trascorso è stato quello dell'impennata degli attacchi. L'incremento deriva in larga parte dalle sempre più evolute tecniche di hackeraggio, in grado di ampliare a dismisura la platea delle vittime. Tuttavia mai come in questi mesi sta aumentando l'attenzione generale sul "cyber risk", concetto un tempo considerato prerogativa di pochissimi. Ma nonostante imminenti e stringenti novità legislative, la consapevolezza di Aziende e Professionisti italiani è ancora scarsa. Alcuni player italiani del settore assicurativo come AEC sono, però, già in grado di soddisfare le richieste di Professionisti ed Aziende, dalle PMI alle grandi Corporation in merito alle coperture cyber. Ne discutiamo con Federico Capuzzo, Responsabile dell'Intermediazione di AEC Spa.

D. Gli ultimi due anni sono stati gli anni orribili della sicurezza informatica. Il 2018 sarà migliore?

R. Secondo gli esperti no. Negli ultimi anni il cyber crime a livello mondiale ha raggiunto un giro d'affari che supera 500 miliardi di Euro l'anno, poco dietro il narcotraffico, per avere un'idea dell'entità del fenomeno. In Italia ha costanti incrementi a due cifre, ad esempio nel bilancio diffuso dalla Polizia Postale si contano nel 2017 ben 28.522 tentativi di intrusione, un numero cinque volte superiore alle segnalazioni del 2016. Crescono soprattutto gli attacchi con finalità estorsive o di arricchimento diretto. Le grandi corporation lo stanno iniziando a capire, ma nel nostro Paese, dove prevale il modello della PMI, questa sensibilità è ancora poco diffusa: il rischio c'è ed è sottovalutato. Gli analisti ci dicono che il 2018 sarà caratterizzato da attacchi alle infrastrutture, ransomware, furti di capitali elettronici e, soprattutto, furti di dati.

D. Il nuovo quadro normativo potrà aiutare a diffondere una cultura del rischio cyber anche in Italia?

R. Sicuramente si, ma solo se insieme all'adeguamento a queste nuove norme - operative da maggio 2018 - si coltiverà una nuova mentalità che veda il rischio cyber non come un evento remoto e lontano, ma come una latente possibilità che può quotidianamente produrre danni gravi e insidiosi a tutti noi. È importante evidenziare che il rischio cyber riguarda tutti i settori, non solo quello dell'informatica come si potrebbe pensare.
Secondo noi di AEC occorre agire d'anticipo, tutelandosi anzitutto dal punto di vista assicurativo ed anche con azioni di mitigazione, prevenzione e monitoraggio del rischio, come la nostra offerta è in grado di fare abbinando ad una polizza cyber performante un pacchetto di servizi volti proprio a questo.

D. Quali saranno queste nuove norme in vigore da maggio?

R. Siamo convinti che uno dei driver più forti in tema IT security è rappresentato proprio dall'evoluzione normativa che la UE imporrà sul tema, in particolare, con il Reg. 679/2016 che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018. La nuova regolamentazione tra le altre cose determinerà: obbligo di designare una "Data Protection Officer" (per alcuni soggetti); incremento delle Responsabilità del titolare del trattamento dei dati personali; regolamentazione del contratto di appalto tra titolare dei dati e responsabile del trattamento; rafforzamento dell'obbligo di notifica da parte del titolare dei dati personali all'autorità competente e all'interessato in caso di violazione dei dati personali; creazione da parte del titolare dei dati personali di un registro di attività di trattamento svolte; inasprimento delle sanzioni; nuovi poteri all'autorità di controllo.

D. Quali sono le categorie oggi meno coperte dalle polizze e per quale motivo?

R. Per quanto riguarda l'Italia sicuramente le più esposte sono le PMI, basti pensare che nel 2017 gli attacchi diretti alle PMI italiane sono aumentate del 7% e che il 47% di queste sono già state colpite. In primo luogo, sono le più esposte perché sono le realtà produttive più diffuse; secondo, ritengono di essere "immuni" da tali attacchi, considerandosi poco appetibili; ultimo, in quanto le PMI sottovalutano gli oneri economici e di ricaduta che un attacco hacker e la conseguente perdita dei dati, potrebbe avere sulla solo solidità. Sembrerà banale ma, sicuramente, più aumenta la cultura del rischio e più si assisterà a un progressivo ingrandimento del mercato, sia in termini di soluzioni offerte che di premi complessivamente raccolti.

D. Come pensate di sensibilizzare le imprese alla sottoscrizione di polizze?

R. Vogliamo sviluppare lo small/middle market per consentire a tutte le piccole e medie aziende, agli studi associati di professionisti e agli Enti Pubblici interessati da questi rischi di poter accedere a una offerta di base che prevede un premio minimo imponibile di 600 euro, franchigie a partire da 500 eurp e un questionario di appena 8 domande. Per fare questo, abbiamo realizzato video informativi, organizzato eventi di settore nonché creato un sito interamente dedicato al tema (www.polizzacyber.it) costantemente aggiornato con news sul tema. Infine, per quei soggetti per i quali è obbligatoria l'istituzione di questa figura, abbiamo sviluppato una copertura assicurativa ad hoc per il "Data Protection Officer".