Dalla ricerca Grant Thornton emerge che nel mondo gli attacchi cyber alle imprese sono passati dal 15% al 21%. Sono aumentati i crimini legati alle infrastrutture aziendali, alle estorsioni online e alle blackmail

Grant Thornton Consultans S.r.l.
Via Salaria, 222
00198 Roma
Italy

T 0039 (0) 6 – 89162274
F 0039 (0) 6 – 8552023
E info.roma@it.gtc.com
W www.ria-grantthornton.it

COMUNICATO STAMPA

6 Dicembre 2016. Nuove analisi di Grant Thornton rivelano che negli ultimi 12 mesi le estorsioni e le blackmail sono le forme più diffuse tra gli attacchi cyber rispetto alla frode di dati o di proprietà intellettuali. Per gli esperti di Grant Thornton sono cambiate in un anno le tipologie di minacce e reati cibernetici con effetti sulle persone, imprese e business, mentre le risposte per difendersi tendono a rimanere resilienti.

Dall'International Business Report (IBR)di Grant Thornton emerge che nel mondo più di un business su cinque (21%) ha dovuto affrontare una forma di attacco cyber negli ultimi 12 mesi, rispetto al 15% dichiarato dagli stessi intervistati un anno fa nel 2015. Il panel di ricerca è composto da 2.600 Ceo e altri alti dirigenti intervistati in 37 economie nel mondo.

La ricerca Grant Thornton mette in luce che sono aumentate le percentuali di business che subiscono attacchi cyber sia nelle economie del Nord America (dal 18% nel 2015 al 24% nel 2016) sia nell'Unione Europea (da 19% a 32%), così come in Africa (da 10% a 29%) e in Asia e Pacifico (da 9% a 13%).

Tra gli intervistati che hanno subito attacchi, la forma più comune di attacco cyber citato è stato il danneggiamento di infrastrutture aziendali (citate dal 22% delle organizzazioni intervistate). Altre forme di cyber-attack sperimentate sono state l'utilizzo di blackmail o estorsioni per ottenere denaro (17%), la frode di informazioni finanziari legate ai clienti (12%) o di proprietà intellettuale (11%).

Francesco Pastore – Amministratore delegato di Grant Thornton Consultants – commenta:.*"I tentativi di estorsioni online tendono a crescere in termini di volumi, con inizialmente un impatto finanziario sottostimato. Nel tempo le organizzazioni dovranno metter in conto costi complessivi ben maggiori dovuti a diversi effetti collaterali, tra cui i danni reputazionali, quelli collegati alle frodi di dati sensibili dei clienti e sulle proprietà intellettuali, i danni alle infrastrutture tecnologiche e fisiche."*

Il rapporto mette in luce la necessità e opportunità per i leader aziendali di essere più veloci e proattivi nelle strategie e piani nel prevenire e gestire gli attacchi informatici. Tra gli elementi chiave emergono la reale capacità di comprensione del valore dei

dati sensibili da proteggere e di quanto siano accurate le strategie messe in atto da tutta l'organizzazione.

"La ricerca internazionale ha messo in evidenza" – ***continua Francesco Pastore di Grant Thornton Consultants*** – *"che a livello mondiale nei 37 paesi analizzati, tra i 2.600 business leaders intervistati che hanno subito un attacco informatico negli ultimo 12 mesi, circa uno su otto (13%) ha percepito il reato in corso dopo più di una settimana mentre per il 4% degli intervistati la notizia è giunta dopo più di un mese. Queste ricerche e risultati confermano che in molti casi le strategie e gli investimenti in cyber security non sono efficaci e che le aziende sono esposti a rischi finanziari complessivamente sottostimati e non contabilizzati. Pensiamo a cosa può succedere ad esempio ad una banca internazionale che viene citata al telegiornale per aver subito attacchi informatici con impatto sui conti online anche di un solo cliente".*

Risultati della ricerca in Europa e Italia.
I ceo e gli altri leader intervistati alla domanda se hanno subito un attacco cyber negli ultimi 12 mesi hanno risposto in queste percentuali: UE 32%; Italia 34%; France 24%, Spagna 31,7%, Ireland 42%; Germany 40%; UK 37%. Riguardo ai settori più colpiti secondo le risposte dei leader intervistati in UE: Education e social services 36%; Electricity, gas, water e utilities, 35%, Professional Services, 28%; Oil and Gas, 20%, Tech, 20%, Financial services (18%).

Per i leader italiani intervistati i principali effetti negative da attacchi informatici sono stati in ordine di importanza: perdita di reputazione, perdita di consumatori, tempo speso dal management, impatto diretto sui ricavi, cambio di comportamento dei consumatori, competitività dell'organizzazione, costi legati a risolvere i danni causati dagli attacchi informatici. Il 52,9% dei leader italiani intervistati ha dichiarato che gli attacchi informatici hanno avuto un effetto diretto sui ricavi.