

# Il cybercrime produce in Italia un danno di oltre 30 miliardi l'anno

**Ma è ancora scarsa la percezione del rischio e della perdita nelle grandi aziende**

Occhio al frigorifero. Alla Smart tv. O alla macchinetta del router che lampeggia su quella mensola. Il nemico è subdolo ed è già arrivato ad usare gli elettrodomestici più innocenti. Per quello che riguarda i privati, le loro abitazioni. Figuratevi a che punto si è evoluto il cybercrime se l'oggetto di interesse sono le grandi imprese, le istituzioni, le grandi. Un think tank di peso - Luiss business school, Formiche.net, Ibm, Equis e Ernst and Young - prova a mettere a fuoco il fenomeno del crimine informatico (cybercrime) per mettere a punto più efficaci protocolli nella cybersicurezza e più formazione per chi la deve gestire. Sapendo di dover scontare, anche nelle aziende più evolute, la sensazione che un cyberattacco non sia poi qualcosa di così terribile. Nel 2014 sono stati calcolati, solo in Italia, 875 milioni di dollari di perdite in un anno per danni diretti; 8,5 miliardi (0,6% del Pil) per danni di immagine, costi di riparazione e perdita di business. Altri 9 miliardi sono stati spesi per la perdita di dati sensibili e 14 sono i miliardi persi per l'interruzione dei sistemi operativi. Essere, vivere e lavorare digitale fa correre il mondo, lo migliora, spesso lo semplifica - non sempre - ma come ogni cosa ha il suo prezzo. Molto più alto, in questo caso, di quello che si possa immaginare perchè un cyberattacco non è come lo scippo delle borse. I danni si realizzano dopo, tra un po'. Quando se ne sono assommati anche altri. Ben l'88% delle aziende intervistate ritiene di non avere un sistema di sicurezza delle informazioni all'altezza delle reali necessità di protezione del proprio business. Cir-

ca il 40%, delle aziende reputa necessario fare ulteriori investimenti in cyber security. Mentre il 36% degli intervistati afferma di non essere in grado di identificare un attacco sofisticato, un altro 36% non ha attivato processi di *cyber-threat intelligence* (controsospionaggio interno) e il 47% non ha un *service operation center* (controllo interno).

Più della metà delle aziende (57%, era il 53% nel 2014) sostiene che la mancanza di risorse qualificate è uno dei principali ostacoli per efficacia ed efficienza delle iniziative di sicurezza. Oltre al Centro studi presso la Luiss, il settore delle cybersecurity avrà a giorni anche un specifico organo di informazione, la Cyberaffairs, la prima agenzia di stampa interamente dedicata alla sicurezza cibernetica. Il notiziario sarà prodotto tramite Askanews.

**Nuovo Centro di formazione alla Luiss e un'agenzia di stampa dedicata**