

FAUSTO DE MARE \*

# Confcommercio e i cyber reati

**N**el 2017 sono stati oltre 250mila gli esercizi commerciali colpiti da un cyber-attacco per un danno complessivo di circa 1 miliardo e 800mila euro. Anche nella nostra regione, come ha reso noto il recente rapporto della Polizia Postale e Comunicazioni, si sono registrate nell'ultimo anno 160 transazioni illecite e numerosi casi di intromissioni in rapporti commerciali tra aziende con l'impossibilità di recuperare somme incassate illecitamente specie in Paesi extra Ue. Altro allarme quello lanciato in occasione dell'inaugurazione dell'Anno Giudiziario, sabato scorso: da noi i reati informatici in crescita del 19,4%. È, dunque, anche da noi elevata la vulnerabilità degli esercizi commerciali. È questa l'indicazione della ricerca "La cyber-criminalità contro gli esercizi commerciali in Italia" realizzata da Confcommercio in collaborazione con Intellegit, start up sulla sicurezza dell'Università degli studi di Trento. Alcuni dati della ricerca: nel 96,3% dei casi, è a rischio cyber-criminalità così come risultano poco o per nulla sicuri quasi la metà dei siti internet delle stesse attività commerciali; quasi un commerciante su due non è consapevole di questi rischi e la misura di protezione più utilizzata (nel 90% dei casi circa) è costituita da software antivirus e firewall, mentre la meno utilizzata è la copertura assicurativa. Inoltre, solo il 44,4% di questi episodi è stato denunciato alle autorità competenti.

Insomma, le cyber-minacce sono in continua evoluzione e destinate a crescere in un mondo sempre più connesso e digitalizzato e questa tendenza non risparmia il settore del commercio che subisce attacchi sia contro gli strumenti informatici dell'attività commerciale (malware, attacchi DoS e black hat hacking), sia contro l'attività commerciale stessa attraverso strumenti informatici, come le frodi tramite email di phishing.

L'indagine ha individuato tre tipologie di costi derivanti dagli attacchi della cyber-criminalità al commercio: di protezione (sostenuti dai commercianti per dotarsi di sistemi di sicurezza contro le cyber-minacce), diretti (perdite monetarie subite da un commerciante nel caso sia stato vittima di un cyber-attacco) e indiretti (quantificazione monetaria di una serie di danni immateriali cui un commer-

ciante può incorrere come conseguenza di un episodio di cyber-criminalità). In totale, negli ultimi 12 mesi, i costi di protezione stimati sostenuti dai commercianti ammontano a 885.600.000 euro, quelli diretti oltre 854.000.000 euro, mentre tra i possibili costi indiretti, è stato possibile calcolare il valore monetario delle ore che i commercianti che hanno subito un cyber-attacco hanno perso per risolvere il problema, pari ad oltre 54.460.000 euro.

Complessivamente, quindi, nell'ultimo anno la cyber-criminalità ha arrecato ai commercianti italiani costi pari a circa 1 miliardo e 800 milioni di euro. Una cifra che è comunque sicuramente stimata per difetto perché non include le perdite indirette diverse dalle ore di lavoro impiegate per risolvere il problema. Dai risultati del sondaggio è emerso che il 96,3% delle attività commerciali è a rischio cyber-criminalità, facendo uso di un qualche tipo di strumento informatico. Quasi un commerciante su due, però, non conosce le minacce. In media il 6,9% dei commercianti è stato vittima di un cyber-attacco negli ultimi 12 mesi. La situazione, però, è diversa da città a città.

Con l'indagine intendiamo mettere in guardia i titolari delle pmi non solo commerciali tenuto conto che in media solo il 44,4% degli episodi di cyber-criminalità è stato denunciato alle autorità competenti. La misura di protezione contro la cyber-criminalità più utilizzata dai commercianti è costituita dai software antivirus e firewall; la meno utilizzata le coperture assicurative per i danni dovuti a cyber-attacchi. I commercianti sono particolarmente esposti ai rischi legati ai ransomware (meno della metà crea con regolarità copie di backup dei file utilizzati per l'attività) e alle truffe tramite email di phishing. Una delle falle più sfruttate dai cyber-criminali per attaccare un sito internet riguarda la vulnerabilità dei CMS (Content Management System, programmi di gestione dei siti Internet) quando questi non vengono utilizzati nella loro versione più aggiornata (e per questo più sicura).

L'analisi ha evidenziato che un sito su tre (il 34,2%) dei commercianti che fanno uso di CMS è un bersaglio particolarmente vulnerabile ad eventi di cyber-criminalità dal momento che utilizza una versione arretrata e obsoleta.

[\* Presidente Confcommercio Imprese Italia Potenza]

