

**IL CASO**

# Poche difese per i cyber attacchi in Italia colpita un'azienda su due

**LE INTRUSIONI DIGITALI NON RIGUARDANO SOLO LA GUERRA DI SPIE TRA GLI STATI MA ANCHE NUMEROSE IMPRESE. LA MAGGIOR PARTE NON È PREPARATA E NEMMENO PRESENTA DENUNCIA**

**Milano**

Non solo Russia contro Ucraina. La cyberwar è una guerra mondiale che coinvolge tutti: dagli stati alle pubbliche amministrazioni fino alle aziende e ai privati cittadini. La scorsa settimana un malware ha preso di mira la Maschio Gaspardo, azienda di Campodarsego, nel padovano, che produce ed esporta in tutto il mondo macchine per la lavorazione della terra. La società ha deciso di denunciare l'attacco e di sospendere le attività per tre giorni disattivando tutti i sistemi informativi. La rivelazione al pubblico di aver subito un attacco fatta da Maschio Gaspardo è un fatto più unico che raro nel panorama italiano, dove spesso si preferisce non denunciare, nel timore di ritorsioni e di danni reputazionali. Eppure in gioco ci sono i dati personali di tutti gli individui e quelli delle società che hanno rapporti con l'azienda colpita da malware.

Secondo quanto emerge dall'ultimo rapporto Clusit sulla cybersecurity in Italia, omertà e incompetenza la fanno ancora da padrone. Gli esperti della sicurezza hanno scandagliato la rete e fat-

to indagati presso aziende e pubblica amministrazione: ebbene in Italia un'azienda su due nel corso del 2016 ha subito almeno un attacco informatico. Oltre al danno, Clusit ha registrato anche la beffa. Perché in media le imprese si accorgono dopo 140 giorni di essere finiti in trincea. E solo pochissimi denunciano gli attacchi alle autorità.

Nel mirino ci sono tutte quelle società che trattano dati personali. In particolare il rischio di cyber attacchi si rivela molto elevato nella sanità (+106% rispetto all'anno precedente), nelle banche (+64%) e nelle infrastrutture (+15%). L'anno scorso in Italia, stando alle stime del Garante per la privacy, gli attacchi ai nostri dati personali hanno provocato circa 9 miliardi di euro di danni.

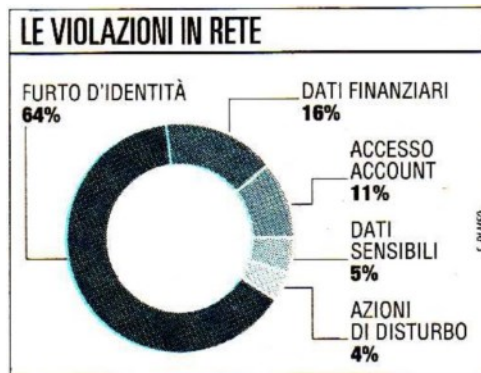
Nonostante il ripetersi delle cyber intrusioni, solo il 20% delle aziende nazionali investe in sicurezza. Inoltre il 77% delle violazioni amministrative contestate dal Garante per la protezione dei dati personali è stata proprio la omessa comunicazione di data breach da parte degli operatori coinvolti ai diretti agli interessati.

Secondo i dati raccolti dall'Osservatorio Information & security del Politecnico di Milano, le nostre imprese, e in particolare le Pmi, si presentano con le armi spuntate nelle trincee della cyber

guerra. L'investimento complessivo in sistemi di sicurezza in Italia si attese a 900 milioni di euro, una barriera ancora troppo ridotta contro il rischio di attacchi informatici. E il prossimo bersaglio si chiama industria 4.0: in quelle fabbriche dove cominciano a entrare i robot usati nei processi produttivi, sempre più connessi fra loro e con il web, che potrebbero diventare un facile target dei pirati della Rete a causa di sistemi operativi vulnerabili e procedure di autenticazione deboli.

Tuttavia, a livello europeo si registra una buona notizia. Infatti il costo delle violazioni sta diminuendo. E questo fatto, a detta degli esperti, deriva dall'impegno di quelle aziende che si stanno conformando al nuovo regolamento europeo sulla data protection. Il rapporto Ibm - Ponemon Institute ha registrato un drastico calo (in decrescita al 26%) dei costi del data breach nei paesi europei. E si tratta di una netta inversione di rotta dopo anni di crescita ininterrotta. I curatori del report affermano infatti l'esistenza di una stretta correlazione tra la risposta ai requisiti normativi in Europa e il costo totale di una violazione dei dati. I fattori principali che stanno riducendo il costo di una violazione sono l'aumento degli investimenti in sicurezza, la crittografia e una migliore formazione del personale. (ch.be.)

© RIPRODUZIONE RISERVATA



Oltre gli attacchi hacker per i furti d'identità, un'quota rilevante delle intrusioni riguarda gli accessi ai sistemi informatici delle imprese che non sono sempre preparate

