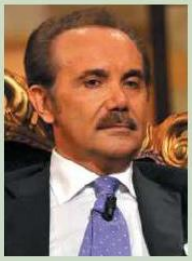
ItaliaOggi
QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO

IL PUNTO DI MAURO MASI*

Truffe online, l'arma è l'attenzione

Tra i più rilevanti side-effects (effetti collaterali) della pandemia da Covid 19 c'è stato il forte incremento del traffico in rete. Tale incremento non è scemato con la fine del contagio, anzi. Ciò dimostra che le motivazioni di crescita dei volumi in rete non sono solo connesse ai lockdown: ad esempio la crescita esponenziale delle attività di Amazon è derivata anche, e forse soprattutto, dalla bontà del modello di business «Bezos» oltre che dai vincoli alla mobilità. Tuttavia, insieme all'esplosione dei volumi in rete è cresciuto in diretta proporzionalità il fenomeno del cybercrime in particolare attraverso violazioni e furto di dati sensibili.



Mauro Masi

Si era già assistito a un balzo di questo tipo di crimini con lo sviluppo della «Internet of Things» (la rete delle cose, che sta collegando milioni di dispositivi diversi, sensori e macchine) ora lo shock in rete da pandemia sta rendendo il fenomeno ancora più preoccupante. Ce ne stiamo accorgendo un po' tutti; chiunque frequenti la rete anche occasionalmente può constatare direttamente come sia divenuta un inferno di trojan, backdoor, worm. Malware (che poi è l'abbreviazione di «maliciuos software» software dannoso) di ogni tipo e contenuto che tenta di carpire tutto quello che può approfittando della sostanziale impunità che può garantire la rete (con qualche importante eccezione, come ancora dimostrano le cronache italiane di questi giorni).

Si stima che a livello mondiale vengano immessi sul mercato dai 2.000 ai 3.000 nuovi malware al giorno; gli antivirus bloccano solo quelli che conoscono, se si crea un nuovo malware è possibile che passi ed ottenga il proprio scopo. C'è un modo per difendersi? La risposta ovvia è che più si sta lontani da Internet, meno si usano gli smartphone e più si è al sicuro. Naturalmente nel mondo contemporaneo è molto difficile farlo; purtuttavia è bene tenere presente alcuni punti fermi. Intanto partire dall'assunto che i cyberattacks vengono fatti sia attraverso e-mail sia tramite social media e instant messengers (questi ultimi tendono a essere preferiti dai malintenzionati perché, in genere, sono ritenuti più affidabili dalle potenziali vittime). Bisogna quindi tentare di distinguere bene, prestando molta attenzione al contesto (chi sta scrivendo? Perché? Il messaggio è atteso? Lo stile del messaggio è normale? Ci sono precedenti?), un attacco di phishing (la truffa informatica proprio rivolta a carpire dati personali e/o sensibili) da una e-mail o da un messaggio social legittimi. Naturalmente la difesa è più facile se si riduce la potenziale superficie di attacco nel senso che non è (forse) possibile uscire del tutto dalla rete ma è certo possibile eliminare la nostra presenza da quelle piattaforme non strettamente necessarie; pulire regolarmente le app non utilizzate; cambiare periodicamente le password.

Tutto ciò è ben lungi dal garantire la protezione totale dai cybercrimes ma almeno renderà la vita più difficile ai malintenzionati. Anche se, forse, per molti italiani potrebbe già essere troppo tardi: per dare solo un recente esempio, sembra che una variante del noto banking trojan Emotet abbia compromesso solo poco tempo fa numerosi e importanti account di posta elettronica anche istituzionali del nostro Paese.

*Delegato italiano alla proprietà intellettuale
Contatti: mauro.masi@bancafucino.it