CYBER CRIME? SEMPLICE ESTORSIONE

Non c'è nulla di affascinante negli hacker che chiedono un riscatto per sbloccare l'operatività della rete aziendale o i dati dei clienti. L'articolo 629 del Codice Penale parla chiaro e rende evidente che si tratta di semplici criminali. Anche in questo ambito è compito dell'intermediario rendere consapevole il cliente

Le denunce presentate quest'anno in relazione a estorsioni legate al mondo digitale sono più che decuplicate rispetto allo stesso periodo del 2020. Sono questi gli allarmanti dati contenuti nel dossier diffuso dal Viminale, in occasione del tradizionale *Comitato nazionale per l'ordine e la sicurezza pubblica* dello scorso 15 agosto.

Il riferimento è ovviamente ai crimini effettuati attraverso la *rete*, ma proviamo, per una volta, a non utilizzare parole come *cyber* o *hacker*, evocativi termini anglosassoni che richiamano, ingiustamente, alla mente straordinarie capacità tecniche o il fascino di uomini ribelli e solitari che sfidano i grandi poteri e la tecnologia matrigna. Si tratta, al contrario, di qualcosa di molto più vile ed elementare: delinquenti, quasi sempre affiliati alle grandi *famiglie* della malavita organizzata che, mediante una minaccia, per procurarsi un profitto costringono le proprie vittime a fare qualche cosa (e questa è, quasi letteralmente, la definizione di estorsione del nostro Codice).

Dimentichiamo il fascino di Robin Hood

Un ricatto vero e proprio, probabilmente il reato più subdolo per ottenere un vantaggio, perché agisce sulla condizione di fragilità, anche emotiva, del *violato* per arricchirsi.
Non c'è alcuna intuizione alle spalle, non chiamiamoli geni del male. Nessun discutibile obiettivo ideale, dimentichiamoci *Anonymous*. Sono solo criminali, spesso analfabeti (quantomeno dal punto di vista informatico) che utilizzano strumenti predefiniti, facilmente accessibili, per mettere in difficoltà ed estorcere denaro.
Appare decisamente interessante come, mentre l'incidenza di questi delitti esplode del 1000%, risulti diminuito l'impatto delle altre forme di agire criminale che, nello stesso periodo, si è ridotto o, al limite, è rimasto stabile. Le organizzazioni mafiose – quelle che uccidono, vendono armi o spacciano droga – hanno imparato a fare business in questo settore, sfruttando da una parte i ritardi giuridici e le difficoltà legate all'individuazione della competenza territoriale del reato e, dall'altra, la totale, masochistica, incapacità delle vittime di opporsi, se non all'infrazione delle strutture tecnologiche della propria impresa, quanto meno alla limitazione delle conseguenze che questa violazione porta con sé.

Competenza, non solo copertura

La copertura assicurativa – ammesso che un imprenditore sia già entrato nella modalità d'acquisto e che il nostro mercato sia pronto a dare una risposta consona (cosa non ovvia, in un periodo di confuso *hard market* come quello che stiamo vivendo) – non è in alcun modo sufficiente.
L'analisi e gestione dei rischi informatici per un'azienda è assolutamente necessaria e, probabilmente, prioritaria rispetto a qualsiasi altro *rischio* aziendale.
Il consulente assicurativo deve supportare questo sforzo, premendo per un cambio di mentalità. Deve aiutare i propri clienti a tirare fuori la testa dalla sabbia, proponendo strumenti di diagnosi e percorsi di consulenza specifica.
La sensibilizzazione è il primo punto che deve sviluppare il consulente: il cliente ce ne sarà grato.