LA SEMANTICA CHE AIUTA NEL CYBER

ANALIZZARE IL WEB PER INDIVIDUARE GLI ASSET DIGITALI DELL'AZIENDA E LE RELATIVE ESIGENZE ASSICURATIVE. QUESTO L'APPROCCIO DI CERVED SPAZIODATI AL RISCHIO INFORMATICO

Ridurre le asimmetrie informative, sia per il prospecting sia per l'underwriting. Con questo obiettivo, **Cerved SpazioDati** ha ideato una metodologia per il cyber risk che utilizza la semantica e i big data.
"Abbiamo indicizzato tutto il web e costruito algoritmi che capiscono se un sito web appartiene o meno a un'azienda", racconta **Gabriele Antonelli** di Cerved SpazioDati. Un'analisi che riguarda settimanalmente 300 milioni di pagine web corporate, diventando tanto un patrimonio per le aziende, quanto uno strumento di analisi su diverse tematiche. Tra queste, il rischio cyber, un tema in continua evoluzione su cui, però, c'è ancora una scarsa protezione, "sia perché una prevenzione assoluta non può esistere, e sia perché spesso mancano anche le necessarie competenze degli assicuratori e un'offerta adeguata per le Pmi".
Il principale ostacolo allo sviluppo di questo mercato è dato dall'asimmetria informativa: non vi è, infatti, uno stato dell'arte sulle azioni preventive intraprese dalle imprese sul cyber risk, dove rilevante risulta anche il *rischio multiparte* nel web, legato all'interconnessione tra i soggetti.

UN UNIVERSO DI FONTI ETEROGENEE

I big data utilizzati da Cerved SpazioDati provengono da molteplici fonti:

- quelle riferite ai 6 milioni di aziende italiane;
- gli open data messi a disposizioni dalle amministrazioni pubbliche e incrociati con quelli delle imprese;
- 1 milione di siti web di compagnie;
- le informazioni non ufficiali che arrivano dalla rete (70mila notizie giornaliere e social).

Gabriele Antonelli, *Cerved SpazioDati*

COSA SI NASCONDE DIETRO A UN WEBSITE

Proprio dalla riduzione delle asimmetrie informative potrebbe arrivare la spinta a una maggiore copertura cyber, ad esempio analizzando la rete per capire quali sono gli asset digitali che l'azienda detiene, e quale sia l'esigenza assicurativa.
"Su questo abbiamo fatto un esperimento – rivela Antonelli – per capire cosa si nasconde dietro ai website delle imprese. E lo abbiamo fatto partendo da due parole chiave: *Cialis* e *Viagra*". Sono risultate 2.328 aziende che contengono queste parole nel loro sito, a riprova del fatto che sono state hackerate. Di queste, l'85% è un'impresa media (con oltre 20 dipendenti), oltre il 50% possiede, oltre al sito web, almeno un account social attivo, ma nonostante ciò, nessuna si è accorta di aver subìto un hackeraggio. "Ne abbiamo dedotto che più di un quarto delle aziende (comprese le medie e grandi) hanno sistemi di gestione dei contenuti non aggiornati da oltre di due anni".
Ecco, quindi, che l'approccio proposto da Cerved, denominato *Atoka,* pur non essendo risolutivo, consente di eseguire il prospecting e valutare il peso degli asset digitali delle imprese (valutazione ranking dei website, analisi canali web e social utilizzati, trend di crescita), di identificare nuclei e sottoreti esposte al *multipart risk* e di operare un *security check* preventivo. ***L.S.***