

Per una WebNavigazione Sicura nel Mare di Internet

«La posta elettronica per la sua intrinseca fragilità è il tallone d'Achille di molte aziende». Maurizio Caltabiano, Country Manager SurfControl, fa il punto sulla dimensione internazionale del rischio.

Il mondo delle minacce web si presenta come una dimensione per definizione transnazionale, internazionale...

Avere una dimensione “worldwide” significa sondare le differenti tipologie di minacce presenti in regioni diverse, infatti pur essendo il web per definizione “extra-territoriale”, a Paesi diversi corrispondono vulnerabilità differenti. SurfControl si caratterizza come la prima compagnia che si è interessata di controllo navigazione web. Nel 1996 esce SurfControl sul mercato. Le successive acquisizioni portano ad allargare la suite con il controllo della posta elettronica. Oggi SurfControl è dispiegata in una dimensione “worldwide”: Usa, Giappone, Singapore, Australia, Israele, Europa: una *global company* che può contribuire all'innovazione avendo una dimensione e una percezione del mercato su scala mondiale. Una società che è molto attenta alle diversificazioni, alle varie onde e ai segnali deboli del mercato. Dallo “spam” al “phishing”, allo “spyware”, seguendo le successive ondate delle minacce web. Questa filosofia di grande attenzione alla dimensione internazionale del rischio ci ha portati verso l'acquisizione di una società cinese che ha portato nuova fibra alla tecnologia, e recentemente abbiamo acquisito anche una società israeliana con una altissima tecnologia dedicata a contrastare il pericolo degli “spyware”.

Qual è la dimensione italiana del pericolo legato alla navigazione?

Il “phishing” per noi in Italia è un problema molto presente anche a causa della bassa scolarizzazione dell'italiano medio, una sorta di analfabetismo informatico che aiuta il fenomeno delle truffe informatiche. Purtroppo nel mercato italiano si sono venute a sovrapporre due tendenze antitetiche: da una parte una tendenza troppo conservatrice a cui fa da *pendant* una voracità estrema con una spinta a consumare tecnologia anche in assenza di garanzie, basti pensare all'abuso di “freeware”.

L'informatica in azienda sconfina molte volte ai bordi dell'illegalità e del codice penale...

Nella sicurezza non esiste una tecnologia in grado di affrontare “a tutto tondo” le complesse questioni che impattano con la gestione della privacy e con le delicate questioni aziendali. Fughe di notizie dall'azienda, utilizzo improprio del terminale aziendale per frequentare siti a rilevanza penale, basti pensare alla pedofilia, sono situazioni più frequenti di quanto sembri. La posta elettronica per la sua intrinseca fragilità è il tallone d'Achille di molte aziende. La posta certificata e la firma digitale sono la nuova frontiera per garantire una autentica affidabilità della comunicazione in rete. Il nostro intervento non può essere delimitato entro un quadro esclusivamente tecnologico, infatti frequentemente al nostro ingresso in azienda è fondamentale chiarire all'azienda quali possono essere i limiti in termini legali. Il lavoro preliminare con il cliente è fondato su un periodo in cui si va a monitorare gruppi di utenti in un significativo periodo di tempo producendo una dettagliata reportistica, ovviamente nei

limiti prestabiliti da un protocollo di intesa con la divisione delle risorse umane. Specialmente il navigatore italiano è molto iterativo nella frequentazione del web, c'è chi naviga per organizzarsi le ferie, chi si aggiorna continuamente sullo sport preferito, gli appassionati del gioco in rete. La navigazione di siti riconducibili alla pedofilia o altre attività "borderline" sono molto frequentate proprio nel contesto dell'attività di lavoro per garantirsi l'anonimato. La stragrande maggioranza dell'attività della pedofilia avviene in ufficio. Si prende possesso della macchina di qualcun altro e si naviga in modo anonimo. Ci avvaliamo di moduli basati sull'intelligenza artificiale che consentono di operare una analisi semantica dei contenuti provenienti da web e di un team a livello "worldwide" per la loro classificazione, garantendo la cosiddetta "Day Zero Protection". Una difesa a trecentosessanta gradi dalle minacce web che non garantisce il cento per cento, ma certamente rassicura chi deve navigare professionalmente sul web.

Intervista a cura di Vittorio Raschetti