Insurance Review
01-LUG-2019
da pag. 32
foglio 1
Dir. Resp.: Maria Rosa Alaggio
www.datastampa.it
Tiratura: 4000 - Diffusione: 0 - Lettori: 0: da enti certificatori o autocertificati
Superficie: 67 %

AGIRE NEI PANNI DELL'HACKER

di MARIA MORO

CONOSCERE IL NEMICO PER PREVENIRE LE SUE MOSSE È LA LINEA SEGUITA DA ALMAVIVA NELLA CREAZIONE DI UNA PIATTAFORMA CHE RICERCA ONLINE I PUNTI DI DEBOLEZZA DEI SISTEMI INFORMATICI DELLE AZIENDE, CON L'INTENTO DUPLICE DI FORNIRE UNA MAPPA DEL RISCHIO E DI QUOTARLO IN MANIERA CORRETTA

Lo scenario è quello di una maggiore digitalizzazione delle Pmi, che porta con sé una crescita dell'esposizione al rischio di attacchi cyber e, per effetto di questa, un reale aumento degli stessi. Cresce in parallelo la consapevolezza delle Pmi sui rischi legati alla cyber security, ma vengono messe in atto politiche di sicurezza che risultano inadeguate.

Almaviva ha presentato i risultati di una propria analisi svolta su 500 Pmi, scelte tra le 148mila aziende italiane con più di 10 dipendenti e fatturato compreso tra 2 e 50 milioni di euro. La selezione delle 500 *Italian top performing company* è stata effettuata in base ai risultati di crescita e redditività, con particolare riguardo alla capacità di integrazione continua di nuove tecnologie e l'orientamento a *Industria 4.0*.

I risultati illustrati da **Roger Cataldi**, head of cybersecurity practice di Almaviva, sono il frutto dell'analisi di informazioni raccolte non tramite interviste e audit, ma grazie alla piattaforma *Joshua*. Lo strumento utilizza nuove metodologie di *open source intelligence* per ricercare online informazioni di libero accesso, rese involontariamente disponibili dalle imprese stesse per una carenza di politiche di sicurezza. Delle 500 imprese "visitate" da Joshua via web, il 13% espone applicazioni pericolose, l'84% usa ed espone applicazioni obsolete, il 74% rende accessibili applicazioni intranet (dando così visibilità a dati strategici), il 16% delle imprese ha ancora attive applicazioni abbandonate, segnale che indica debolezza sia nella sicurezza, sia nella gestione dei propri asset informatici.

***Roger Cataldi**, head of cybersecurity practice di Almaviva*

PIÙ CONSAPEVOLEZZA DELLE CRITICITÀ

L'obiettivo che si è posta Almaviva è di risolvere la consueta carenza di informazioni in fase di assunzione e quindi di quantificazione del rischio. L'utilizzo di una piattaforma di intelligence consente di ottenere una valutazione profilata dell'azienda rispetto al suo rischio cyber, permettendo a compagnie e intermediari assicurativi di conoscere in modo oggettivo l'esposizione al rischio prima della sua assunzione e, di conseguenza, di modellare su basi condivisibili con il cliente un'offerta di protezione realizzata sulle effettive esigenze e il relativo *pricing*.

Il *perito virtuale* Joshua si prefigge di analizzare i clienti target, creare classi di rischio, storicizzare il rischio esterno per monitorare la messa in sicurezza. L'approccio di *cyber intelligence* del *tool* segue il punto di vista di ipotetici attaccanti, rendendo manifesti i punti deboli del sistema e fornendo così informazioni utili alla sicurezza. "Oggi chi attacca non è interessato a far saltare la porta blindata ma a entrare dalla porta di servizio che è rimasta incustodita. Con Joshua noi ci poniamo con le stesse tecniche con cui gli attaccanti profilano il cliente". Gli obiettivi stanno cambiando, e oggi la maggior parte delle azioni di pirateria informatica orientate a creare un danno sono rivolte verso target con peso politico. Gli hacker oggi non sono interessati a colpire direttamente le imprese, ma a mettere a disposizione di un determinato mercato il valore della vulnerabilità, che potrà interessare qualcuno che vuole ottenere un vantaggio. Operare in maniera furtiva e duratura è il nuovo trend dei pirati informatici che rende necessaria una vigilanza continua sulla sicurezza.