Webroot: sempre più machine learning (e consapevolezza) per mettere al sicuro le aziende

Claudio Panerai, Achab

Claudio Panerai, CTO e Tech Evangelist di Achab, ci spiega la ricetta per mettere in sicurezza le aziende: approccio multistrato, educazione e machine learning. Si aprono tante nuove opportunità per gli MSP

Webroot, azienda del gruppo Carbonite specializzata in sicurezza degli endpoint e distribuita in Italia da Achab, ha di recente pubblicato i risultati del suo ultimo Threat Report: Mid-Year Update, uno studio relativo alla prima metà del 2019 su come sta evolvendo il panorama della cybersecurity. Il messaggio importante emerso dal report è la necessità sempre più stringente di una educazione informatica trasversale a tutti i livelli della società, e a maggior ragione delle aziende, e la sempre maggiore personalizzazione degli attacchi da parte dei cybercriminali.

A partire dai principali dati emersi abbiamo riflettuto insieme a Claudio Panerai, CTO e Tech Evangelist di Achab, su come sta evolvendo il crimine informatico, soffermandoci anche su quali sono i problemi che contraddistinguono le aziende italiane lato sicurezza.

Sulla base di questo scenario Panerai si è poi focalizzato sulla proposta di Webroot, antivirus installato in Italia su circa 300 mila endpoint, per capire come funziona e perché gli strumenti di AI e Machine Learning sono sempre più importanti, passando infine ad esaminare qual è il ruolo del canale in tutto questo, interrogandosi in particolare sulle opportunità per i Managed Service Provider (MSP).

Il report rilasciato lo scorso mese da Webroot parla chiaro. La situazione pare piuttosto allarmante…

“Sia a livello italiano che a livello internazionale la quantità di attacchi, virus e ransomware è in perenne crescita. Un dato curioso è come gli attacchi a Windows 7, per il quale da gennaio Microsoft cesserà gli aggiornamenti gratuiti, siano aumentati del 71%, a dimostrazione del fatto che effettivamente Windows 7 deve scomparire dalle scrivanie aziendali.

Un altro risultato molto interessante è che 1 link su 50 è risultato essere malevolo. E considerando che in una giornata lavorativa il dipendente clicca in media su 25 link ne consegue che entro due giorni ciascuno di noi va incontro ad un link malevolo.

Va poi sottolineato come oggi nemmeno la dicitura del protocollo HTTPS vale più come una effettiva discriminante per capire se un sito web è malevolo oppure no dal momento che circa il 29% dei siti di phishing utilizza proprio il protocollo HTTPS per ingannare gli utenti".

Come muoversi all'interno di questo panorama?

"Bisogna agire su tre fronti. In primo luogo occorre rendersi conto che l'approccio alla sicurezza deve essere multistrato: il singolo antivirus, il singolo firewall, il singolo sistema anti-spam non sono sufficienti da soli a tutelare i dati più preziosi per le aziende. E' necessario mettere in pista tutte le tecnologie, armonizzate ad arte".

Già qui entrano in gioco gli MSP. E' giusto?

"Assolutamente sì perché i grandi nomi come Google, Amazon, Accenture, solo per citarne alcuni, si dedicano quasi esclusivamente a clienti enterprise mentre la fascia di piccole e medie aziende, che come sappiamo rappresentano la stragrande maggioranza del tessuto imprenditoriale italiano, vengono lasciate in balia di se stesse. Ecco che allora questo spazio può e deve essere colmato dagli MSP, che con la loro attività di formazione, consulenza e gestione dell'infrastruttura IT sgravano l'impresa che in questo modo può dedicarsi completamente al perseguimento del suo core business".

Il secondo ingrediente per la ricetta di una maggiore cybersicurezza invece qual è?

"Oltre all'approccio multistrato diventa fondamentale ricorrere all'uso sempre più spinto di tecniche di intelligenza artificiale e machine learning. La quantità di dati da analizzare, consumare ed elaborare è infatti tale che l'unica cosa da fare è quella di cercare di metterli a fattor comune, analizzandoli e utilizzandoli per fare una previsione su quello che probabilmente potrà accadere".

Cosa significa questo?

"Un esempio calzante arriva dagli States, dove stanno facendo molti passi in avanti nella diagnostica dei tumori ai polmoni proprio grazie all'ausilio delle macchine. Come? Sottoponendo ai computer un numero infinito di immagini di polmoni sani e malati affinché la macchina impari a capire su un nuovo paziente, con un ragionevole grado di precisione e affidabilità, se questo è sano o malato.

Lo stesso discorso si applica alla sicurezza informatica, dove la macchina deve sapere essere in grado di dire se un certo oggetto sia un virus o no ancora prima che questo cominci a fare dei danni".

E il terzo elemento?

"Il terzo elemento, che rimane fondamentale e imprescindibile, è la consapevolezza o training. L'utente non è ancora consapevole dei rischi che corre e, senza fare terrorismo, bisogna evangelizzarlo per renderlo consapevole appunto che qualsiasi cosa fa può avere effetti devastanti per lui e per la sua azienda".

Focalizzandoci sulle aziende italiane, sulla base di queste premesse, in cosa sono carenti dal punto di vista della cyber sicurezza?

"Le aziende italiane soffrono un po' del "tanto a me non succede". Sembra che le cose debbano sempre succedere agli altri. Spesso a fare notizia sono solo i grandi nomi ma occorre capire che gli attacchi sono trasversali e quindi più vicini di quanto si pensi alla nostra realtà quotidiana. Il principale difetto delle aziende italiane è proprio quindi la mancanza di consapevolezza".

E dal punto di vista della tecnologia come sono messe?

"C'è una grande disparità. C'è chi è ancora abituato a lavorare col fax, tanto per intenderci, mentre c'è anche chi ha capito che la tecnologia, sia di sicurezza che di altro tipo, è un fattore abilitante per lo sviluppo dell'azienda stessa. Si va quindi a due velocità".

All'interno di questo scenario Achab ha sempre puntato, come mi diceva, su approccio multilivello. Fiore all'occhiello della sua proposta è la soluzione Webroot. Di cosa si tratta?

“Webroot è stato il primo antivirus sul mercato a funzionare senza firme quindi ribaltando il modello tradizionale, basando la sua intelligenza sul cloud, dove risiedono dei modelli di machine learning che lavorano in funzione predittiva. Quindi quando un oggetto va in esecuzione, Webroot non lavora per controllare se quello è malevolo o benevolo perché Webroot, in autonomia, prova a fare delle previsioni, snellendo di molto i tempi e la velocità della macchina. E quanto migliori saranno questi modelli di machine learning tanto sarà ovviamente migliore la protezione lato utente, all’interno di un approccio multistrato”.

Quindi quali sono i vantaggi per chi eroga servizi IT?

“Un tempo chi erogava servizi IT doveva installare dentro ogni rete del cliente un server o un servizio che scaricasse gli aggiornamenti dal produttore per poi distribuirli a pioggia sui client. Con Webroot invece ogni macchina, server, pc è collegata direttamente al ‘cervellone’ sul cloud di Webroot, così che l’MSP dalla sua console centralizzata è in grado di controllare tutte le macchine dei clienti senza muoversi dalla scrivania”.

In cosa si differenzia il modello degli MSP da quello tradizionale?

“In un modello tradizionale l’azienda che fornisce servizi IT vive in un certo senso alle spalle del disastro altrui fornendo un’assistenza di tipo classica e quindi intervenendo fisicamente in loco quando si verifica un problema presso il cliente, che dal canto suo va incontro a ‘incidenti’ come il fermo delle attività, con un conseguente incremento dei costi. In questo modo però il fornitore IT lavora solo quando qualcosa non va, non c’è nessuna progettualità e nessuna stima di quanto sarà possibile guadagnare in un certo arco di tempo”.

Invece per gli MSP come funziona?

“L’MSP si fa carico di gestire per intero l’infrastruttura IT del cliente per un compenso fisso al mese, informando da subito il cliente su quanto andrà a spendere. Il fornitore di servizi, dal canto suo, ha delle entrate fisse e questo lo spingerà ad agire con una logica opposta a quella del modello tradizionale. A questo punto le uscite in caso di guasti sono infatti un surplus i cui costi vanno a ricadere esclusivamente sul fornitore stesso, che ha quindi tutto l’interesse ad agire in ottica proattiva affinché i problemi non si verifichino. L’MSP mette in atto tutta una serie di attività di monitoraggio e delle best practice per preservare i dati dei clienti, lavorando per evitare l’insorgere dei problemi”.

Proprio per questo sono nati i software RMM (Remote Monitoring Management)?

“Sì, questo tipo di software permette infatti di eseguire da remoto simultaneamente, schedulandole, delle operazioni così che il sistemista può programmare tutta una serie di attività su più macchine, delegando alle macchine stesse il compito di auto-gestirsi. Aumenta così l’efficienza con la possibilità di fare più cose con meno risorse”.

Questa è proprio la filosofia di Webroot…

“In questo approccio Webroot si incarna alla perfezione, sia dal punto di vista del licensing che permette pagamenti mensili, sia sul fronte operativo della gestione delle operazioni da svolgere all’interno della console. L’MSP senza muoversi dalla scrivania può programmare delle attività e può fare dietro le quinte molte operazioni, senza che questo intralci in alcun modo le attività dell’utente, che si troverà protetto senza accorgersene, senza la necessità, ad esempio, di dovere installare gli aggiornamenti.

Agli MSP è delegata la gestione dell’infrastruttura senza che l’azienda debba interagire con l’antivirus. L’MSP diventa quindi un consulente fidato: l’operatività dei computer dell’azienda, l’antivirus, il backup e così via sono nelle sue mani, mani competenti, mentre l’azienda si dedica alle sue attività. Si concorda una tariffa mensile a seconda delle necessità della rete nell’ottica quindi di una strategia win-win.

Un altro lavoro fondamentale, per riagganciarsi ai discorsi di prima, è quello di evangelizzazione”.

Cosa significa?

“Significa che anche l’MSP deve lavorare in maniera incessante per educare le persone ad avere un approccio consapevole alla sicurezza e ai pericoli che derivano dalla rete. E’ un lavoro che non dà riscontri sul breve periodo ma che è fondamentale. Al di là della singola soluzione, gli MSP devono formare e informare l’utente finale sui rischi che si corrono lato security”.

Achab che strumenti mette a disposizione dei partner?

“Prerogativa di Achab è quella di proporsi sul mercato tramite eventi. Si tratta di roadshow e giornate dedicate dove parliamo dei nostri prodotti ovviamente ma dove ci impegniamo anche attivamente per portare delle riflessioni sottoponendo ai partecipanti dei temi di particolare rilievo. Alla base di tutto infatti deve esserci la comprensione di cosa si sta parlando.

Un’altra iniziativa interessante in fase di lancio è la realizzazione di video per gli end user (i clienti dei nostri clienti) dove spieghiamo in pochi minuti ogni volta degli aspetti diversi, dal ransomware al disaster recovery. In questo modo diamo agli MSP degli strumenti per spiegare le cose all’utente finale con una maggiore semplicità”.

Per finire cosa aspettarsi dal prossimo anno?

“Sul fronte sicurezza le cose non potranno che andare peggiorando. I virus moderni sono dei veri e propri attacchi latenti che studiano i comportamenti dell’utente per poi scagliare degli attacchi mirati e personalizzati. Ma non è possibile ovviamente avere anche degli antivirus personalizzati. Da qui la necessità di ricorrere sempre più spesso a sistemi di machine learning.

Un altro aspetto da non sottovalutare è quello legato a una maggiore consapevolezza nell’uso delle password.

L’utilizzo della stessa password per l’accesso a diversi account è pericolosissimo perché se veniamo ‘bucati’ una volta i cybercriminali avranno libero accesso a tutte le nostre informazioni.

Per cui il perimetro tra virus e credenziali rubate è molto sottile. I due aspetti vanno a convergere. Quindi ancora una volta: consapevolezza!”.