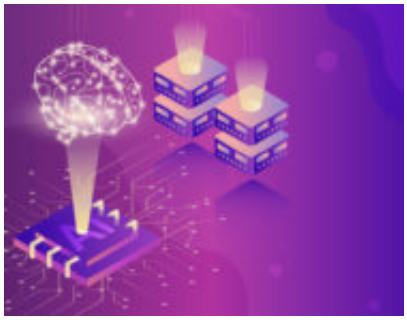
Intelligenza artificiale: un supporto indispensabile per la sicurezza digitale

Author : Redazione

Date : 2 Aprile 2019



Sai che il livello di protezione dei tuoi dati aziendali potrebbe non essere adeguato, come rivela la maggioranza dei professionisti IT? Non è una nostra opinione, ma la risposta sincera fornita da un'elevata percentuale (62%) di professionisti IT di tutto il mondo, che ha riferito di disporre di un'infrastruttura di sicurezza le cui lacune consentirebbero agli hacker di superare le linee di difesa aziendali.

La rivelazione non è che uno degli allarmanti risultati emersi dal recente rapporto dell'istituto Ponemon sulle lacune della sicurezza IT e sul contributo che intelligenza artificiale e machine learning possono offrire per colmarle. Dal rapporto emerge anche che:

- Il 45% degli intervistati ha difficoltà nel proteggere perimetri IT evanescenti, nell'era dell'Internet of Things, del BYOD, del mobile e dello storage cloud.
- Il 46% degli intervistati annovera la persistenza, le capacità sempre più sofisticate, l'esperienza e i finanziamenti degli hacker tra le principali ragioni per la straordinaria diffusione delle violazioni a danno dei dati.
- Il 64% degli intervistati, infine, individua nelle nuove tecnologie quali intelligenza artificiale e machine learning la strada obbligata per rilevare, comprendere e contrastare le minacce.

Innovazioni come l'IA offrono l'opportunità di anticipare le mosse dei criminali informatici esterni all'azienda e i metodi sempre nuovi che usano per estorcere, manipolare e distruggere i dati strategici.

Nuove difese per contrastare nuove minacce

Eseguire regolarmente il backup di sistemi, applicazioni e file è tuttora il miglior metodo per limitare l’interruzione delle attività aziendali e disporre di una strategia di disaster recovery più affidabile. La capacità dei cybercriminali di adeguarsi a queste forme di difesa resta tuttavia elevata. Numerosi sono infatti oggi gli attacchi malware, in particolare quelli ransomware, che

puntano ai file, al software e agli agenti di backup per eliminare qualsiasi possibilità di ripristinare i sistemi senza dover pagare il riscatto richiesto.

Un'efficace protezione dei dati aziendali non può quindi prescindere da una soluzione di protezione moderna e proattiva, progettata per far fronte ai rischi odierni e capace di contrastare le principali minacce che gravano sull'intero ambiente dati per difendere tanto i file originali quanto quelli di backup.

Intelligenza artificiale: cosa offre in termini di sicurezza

Acronis Active Protection, funzionalità inclusa in tutte le soluzioni di backup Acronis sia per uso personale che per gli utenti business, adotta modelli di intelligenza artificiale e machine learning per riconoscere e contrastare in tempo reale gli attacchi ransomware.

I modelli di machine learning vengono generati nell'infrastruttura di intelligenza artificiale cloud dedicata di Acronis, dove vengono analizzati centinaia di migliaia di processi informatici, tanto legittimi quanto dannosi. Questi modelli vengono quindi incorporati in Acronis Active Protection, che monitora i sistemi in tempo reale e analizza i comportamenti di ogni processo per rilevare attività insolite, come la crittografia non autorizzata.

Non appena viene identificato un processo sospetto, la tecnologia Acronis arresta l'attacco e invia una notifica immediata agli utenti o agli amministratori IT, garantendo un netto risparmio di tempo e accelerando le eventuali reazioni agli attacchi.

Modelli di machine learning funzionali al rilevamento delle minacce

Le soluzioni che si basano sulla ricerca di ceppi di ransomware noti riescono a proteggere i sistemi solo da un gruppo limitato di attacchi, lasciando i dati aziendali vulnerabili alle violazioni sferrate dai ransomware di nuova generazione.

Acronis Active Protection svolge un'attività di analisi continua dei dati che consente di riconoscere le nuove minacce prima che gli esperti del settore possano identificarle e sviluppare sistemi di difesa adeguati. I nostri modelli di machine learning definiscono le minacce in base a comportamenti sistematici e non al codice che le caratterizza; questa differenza permette di riconoscere i processi anormali in tempo reale.

Il modello, applicabile a tutti i dispositivi, i sistemi e i file di backup, impedisce agli hacker di danneggiare la soluzione Acronis, il contenuto del file di backup e il record di avvio principale nei computer Windows.

Ripristino automatizzato e difesa gestita

Commentando la ricerca Ponemon, gli esperti di sicurezza concordano che i maggiori benefici offerti dalle soluzioni basate su intelligenza artificiale vanno individuati nella riduzione del tempo e dell'impegno necessario per svolgere indagini sui rischi di sicurezza. Acronis Active Protection anticipa questo aspetto segnalando con notifiche immediate l'avvio di un attacco e fornendo

possibili azioni per una reazione istantanea; il prodotto offre soluzioni anche per gli altri aspetti evidenziati dalla ricerca.

Il campione intervistato individua tra gli altri vantaggi la riduzione dei falsi allarmi, l'arresto degli attacchi prima che provochino danni e l'automazione delle attività di ricerca e reazione agli attacchi.

I modelli di machine learning, che consentono alla tecnologia Acronis di arrestare un attacco in tempo reale, sono già concepiti per ridurre i falsi allarmi. Vengano aggiornati frequentemente ma gli amministratori possono intervenire ulteriormente con una whitelist intuitiva e di facile utilizzo, alla quale è possibile aggiungere i programmi che devono eseguire determinate azioni, così che possano funzionare normalmente senza essere erroneamente contrassegnati come ransomware.

Acronis Active Protection è già un passo avanti anche in termini di automazione della risposta agli attacchi: qualora i file vengano modificati o danneggiati durante un attacco, la difesa può ripristinarli automaticamente, recuperandone la copia pulita dai file di backup.

La possibilità di automazione ottimizzata integrata nella difesa di Acronis consente agli amministratori IT di riportare i sistemi in operatività prima ancora che chiunque altro possa realizzare che è stato sferrato un attacco.

Considerazioni finali

I criminali informatici adeguano continuamente i propri metodi di attacco per infiltrarsi nei sistemi di difesa più moderni. Con il progredire delle loro strategie, saranno necessarie soluzioni nuove e innovative per contrastarne l'operato. Acronis Active Protection, integrata in tutte le soluzioni di backup di Acronis, utilizza metodi di intelligenza artificiale e machine learning all'avanguardia per individuare e difendere attivamente la tua azienda da queste minacce, prima che possano mettere a rischio i tuoi dati.