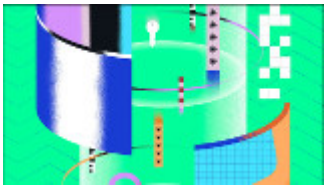
Per difendersi dalle minacce informatiche bisogna investire su IA e automazione. Il punto di Reply

https://www.hwupgrade.it/i/n/Reply_automazione_720.jpg,



A livello globale verranno investiti circa 300 miliardi per potenziare la sicurezza informatica e una parte significativa sarà destinata all'automazione in quattro aree: sicurezza delle applicazioni, degli endpoint, dei dati e, infine, dei dispositivi IoT

di Alberto Falchi pubblicata il **30 Maggio 2022**, alle **13:01** nel canale Security

intelligenza artificialeReply

Il panorama delle minacce informatiche si fa sempre più variegato e complesso. Una sfida per le aziende, che devono tenere sotto controllo un perimetro sempre più ampio e difendersi da un numero di attacchi informatici sempre crescente. A crescere, però, non è solo il numero di tentativi di hacking, ma anche la complessità degli attacchi. A fare il punto sulla situazione una ricerca di **Reply** intitolata ***Cybersecurity automation*** secondo la quale per mettere i propri asset al sicuro è necessario **sviluppare soluzioni automatizzate e basate sull'intelligenza artificiale**.

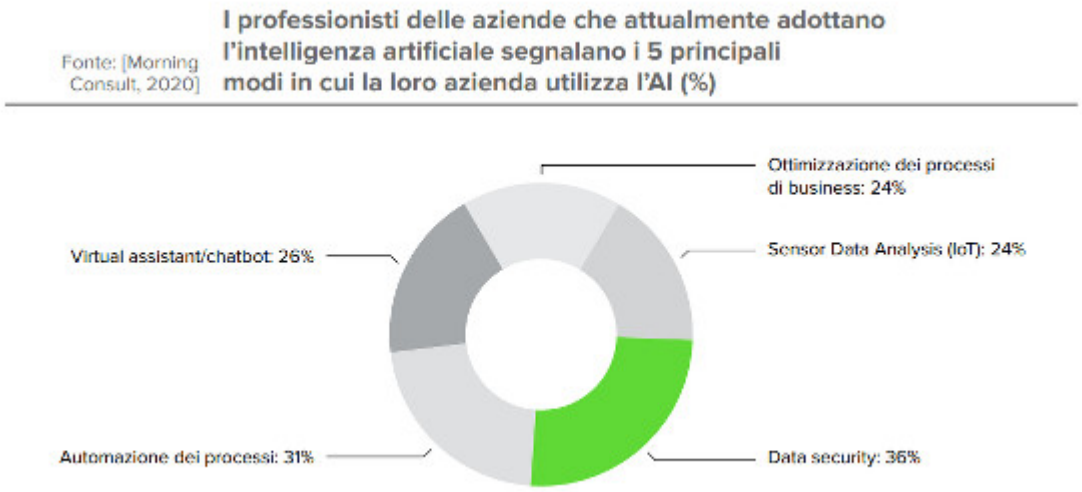
L’automazione è la chiave per migliorare i tempi di rilevamento e risposta alle minacce informatiche

Secondo lo studio di Reply, entro il 2026 **gli investimenti a livello globale per mettere in sicurezza le applicazioni tramite soluzioni automatizzate supereranno i 3,5 miliardi di euro** e solo in Europa si prevede una spesa di circa 669 milioni di euro. A questo si aggiungono gli investimenti per la sicurezza degli **endpoint** (3,7 miliardi, 757 milioni in Europa), dei **dati** (4,6 miliardi, di cui 1 in Europa) e dell’**IoT** (4,4 miliardi, 915 milioni per il Vecchio

Continente).

Secondo **Wolfgang Schwab**, Head of Cybersecurity di PAC, che ha contribuito alla ricerca di Reply, *"L'automazione della sicurezza basata sull'intelligenza artificiale è la "next big thing" nella sicurezza informatica. Anche se le offerte attuali non sono perfette, aprono la strada a una maggiore automazione e consentono agli analisti della sicurezza umana di concentrarsi maggiormente su problemi complessi. La cybersecurity completamente automatizzata non sarà praticabile nel prossimo futuro, ma il monitoraggio, il rilevamento e parti delle azioni di risposta possono e saranno automatizzati nell'interesse della disponibilità dei talenti"*.

Perché l'automazione è così efficace? Perché la maggior parte degli attacchi fa leva sull'errore umano, sulla tendenza delle persona a farsi "ingannare" da e-mail di phishing, soprattutto quelle mirate. Ma anche perché gli esperti di sicurezza sono alle prese con un'enorme quantità di informazioni e alert da gestire. **L'integrazione di processi di Robotic Process Automation permetterebbe ai team IT di concentrarsi su dettagli di maggiore importanza**, limitando il più possibile i lavori ripetitivi e monotoni, che possono portare a errori e distrazioni.



Il passo successivo, poi, è quello di **adottare l'intelligenza artificiale anche nelle fasi di risposta agli attacchi, così da limitare i tempi di mitigazione**. "*Attualmente, la maggior parte delle aziende non utilizza questi sistemi dopo aver identificato minacce o comportamenti insoliti, ma trasmette le informazioni a un analista della sicurezza umano, che decide se la minaccia è reale o se il comportamento richieda ulteriori indagini: le conseguenti decisioni comportano l'attivazione manuale delle azioni appropriate*", si legge nel report.

Lo studio di Reply si sofferma su come adottare l'IA nelle varie aree. Per quanto riguarda la sicurezza delle applicazioni, è importante orientarsi su una collaborazione serrata con i team operations e security per formare DevSecOps, un modello che pone l'accento sull'integrazione delle misure di sicurezza durante l'intero ciclo di vita dello sviluppo delle applicazioni. "*Automatizzare i test in ogni fase è fondamentale per diminuire il numero di vulnerabilità in un'applicazione, e molti strumenti di test e analisi stanno integrando ulteriormente l'intelligenza artificiale per aumentare la loro precisione o capacità*", sottolinea l'analisi di Reply e PAC.

Per mettere al sicuro endpoint, invece, le aziende investiranno maggiormente su soluzioni **EDR** (Endpoint detection and response) e **XRD** (Extended endpoint detection and response), anche queste progettate per ridurre al minimo il lavoro manuale delegando i compiti più ripetitivi agli algoritmi.

Nell'ambito della protezione dei dati, l'IA permetterà di semplificare le procedure per la messa in sicurezza, ma anche di snellire e automatizzare la *discovery* (scoprire quali sono i dati sensibili e dove si trovano) nella classificazione.

La maggior parte degli investimenti, in ogni caso (4,6 miliardi nel mercato dei Big 5 USA, Regno Unito, Brasile, Cina, India e 1 miliardi in Europa) **sarà destinata al settore IoT**, che oggi sono alla base di sistemi OT critici, come le infrastrutture per l'energia, le fabbriche, ma anche a breve smart city e il settore automotive. Non stupisce, considerati i potenziali pericoli, che sia proprio su questo ambito che si concentra la spesa.

"*La crescita significativa del settore cybersecurity a cui stiamo assistendo non è dettata da una moda, ma da una necessità*", afferma **Filippo Rizzante**, CTO di Reply. "*Ogni giorno attacchi informatici colpiscono servizi pubblici e privati, sistemi governativi e sanitari, provocando enormi danni e costi; pertanto, risulta più urgente che mai riconsiderare le strategie di sicurezza e raggiungere nuovi livelli di maturità tramite l'automazione, ricordando che se l'intelligenza artificiale ha potenziato la pericolosità dell'hacker, è sempre sfruttando le opportunità dell'intelligenza artificiale che i cyberattacchi si possono prevenire e contrastare*".

Read More