L'INTELLIGENZA ARTIFICIALE NELLA CYBERSECURITY AZIENDALE

Indice

Necessità di cybersecurity

Il sistema di prevenzione del rischio nella sicurezza informatica aziendale è composto dalle politiche ed i processi progettati per proteggere le informazioni e i sistemi da attacchi che potrebbero compromettere l'immagine o il business dell'impresa. La cybersecurity in un'azienda è cruciale per garantire che il proprio business non venga interrotto o compromesso da attacchi, qualsiasi sia la grandezza dell'azienda. Anche se si possiede una PMI non si è esenti dal problema, ma anzi, i criminali sembrano aver concentrato la loro attenzione su questo tipo di organizzazioni, poiché altamente redditizie negli ultimi anni. Questo avviene poiché tali società possono essere inesperte o ignare del pericolo a cui vanno incontro. Infatti, il 58% delle vittime di attacchi informatici nel 2018 sono state proprio PMI.[1]

Secondo IBM ed il Ponemon Institute Cost of a Data Breach report 2020, il costo medio globale di una violazione dei dati ha raggiunto 3,86 milioni di dollari per violazione nel 2020[2]. Rimanere scarni di protezioni può comportare non solo perdite di cassa, ma anche danni di immagine e furto di dati importanti, quali informazioni dei propri clienti e segreti industriali.

Dovrebbe quindi essere ormai universalmente accettato che soluzioni di protezione dei dati e sicurezza informatica sono imprescindibili per un'azienda sotto il profilo della cybersecurity, incarnando le tre principali caratteristiche che approfondiremo più avanti: robustezza, resilienza e reattività.

[1] (**en**) Verizon, DBIR_2018_Report.pdf
[2] (**en**) IBM, Cost of a Data Breach Report 2020

Introduzione all'intelligenza Artificiale

L'intelligenza artificiale è l'abilità di una macchina di mostrare capacità umane quali il ragionamento e l'apprendimento[3]. L'IA può imparare a completare un compito specifico passando attraverso grandi quantità di dati in modo indipendente, un processo che è chiamato apprendimento automatico, aspetto che può essere fondamentale applicato alla sicurezza informatica aziendale.

- **Elaborazione**

  Le statistiche sui Big Data mostrano che sono stati prodotti 40 trilioni di gigabyte di dati nel 2020[4]; l'intelligenza artificiale permette di setacciare terabyte di dati eterogenei, fondamentale per il riconoscimento di un attacco alla nostra rete.

- **Velocità**

  La velocità di analisi dei dati, soprattutto dopo aver appreso come vengono generati e cosa cercare in essi, non è neanche lontanamente paragonabile a quella umana. Mentre un dottore può fare una diagnosi in circa dieci minuti, un sistema d'IA ben addestrata può arrivare a farne un milione nello stesso tempo.

- **Precisione**

  L'intelligenza artificiale non solo ci permette di avere una velocità di elaborazione considerevole, ma anche precisione nell'analisi finale, fondamentale per ottenere gli effettivi vantaggi di questa tecnologia. Rimanendo in campo medico, un algoritmo di previsione del cancro al seno, addestrato su più di 38 mila immagini di 9 mila donne, è stato in grado di dare una diagnosi ad un livello paragonabile a quello dei radiologi[5].

È importante notare che l'IA non è un sostituto per i lavoratori del settore, ma anzi, deve integrarsi con gli esperti di sicurezza informatica, togliendo loro parte del carico di lavoro ed operare insieme per creare migliori strumenti di sicurezza.

[3] Parlamento Europeo, "*Che cos'è l'intelligenza artificiale e come viene usata*?"
[4] (**en**) Ibm, Netezza and IBM Cloud Pak for Data: A knockout combo for tough data - Journey to AI Blog
[5] (**en**) Johnson, 2021, Precision Medicine, AI, and the Future of Personalized Health Care

IA nella cybersecurity

Avendo queste potenzialità, l'uso dell'intelligenza artificiale diventa cruciale per la sicurezza di un'impresa, qualsiasi sia la loro grandezza di business. Per aspetti quali:

- **Identificazione e previsione delle minacce**

  I comuni sistemi di sicurezza si basano sull'accertamento di minacce con metodologie già note, come agisce ad esempio un antivirus, che controlla su un database di virus noti se il nostro download è già stato identificato come una minaccia. Nei modelli di IA si possono rilevare potenziali minacce alla sicurezza, vulnerabilità e attività dannose anche con tipi di attacchi non noti, per fermarle prima che causino qualsiasi danno.

- **Sicurezza della rete**

  Ci sono due aspetti importanti sulla sicurezza della rete: le impostazioni di sicurezza e la topografia della sottorete aziendale. Le prime aiutano a differenziare le connessioni legittime e maligne, mentre la seconda riduce l'effetto dei dispositivi disabilitati sulle prestazioni della rete.

  L'uso dell'IA nella cyber-sicurezza può aiutare ad automatizzare queste procedure utilizzando adeguati modelli di traffico di rete.

- **Autenticazione**

  L'uso dell'intelligenza artificiale nella sicurezza informatica aziendale può anche aiutare ad arginare le problematiche dolose. Con le verifiche biometriche e le password univoche ad ogni impiegato, possiamo ridurre il numero di accessi non autorizzati e identificare il responsabile di qualsiasi azione.

- **Tracciabilità**

  L'IA ci dà la possibilità di immagazzinare i dati elaborati per rianalizzarli con il nostro gruppo di esperti, in seguito o più in dettaglio.

Tutto ciò, accentuando i punti di forza delle tre caratteristiche fondamentali della cybersecurity accennate sopra, robustezza, resilienza e reattività, ma sollevando problematiche etiche.

Robustezza

La robustezza può essere intesa come la capacità di un sistema di resistere agli attacchi senza cambiare struttura. L'intelligenza artificiale può auto-apprendere ed intanto monitorare il comportamento della rete per identificarne l'atteggiamento e convalidare le operazioni successive come comportamenti corretti. Inoltre, può quindi scansionare le vulnerabilità del sistema e valutarne la robustezza, per permettere di migliorarla e tenerla sempre aggiornata. Questo implica che l'IA sia in grado di eseguire il rilevamento delle anomalie e il profiling di tutto ciò che è vagamente diverso. Va notato, tuttavia, che questo approccio può creare un sacco di rumore da rilevamenti benigni e falsi negativi quando gli aggressori sofisticati si nascondono mimetizzandosi con i normali comportamenti osservati.

Resilienza

La resilienza può essere intesa come la capacità di un sistema di resistere e tollerare un attacco, facilitando il rilevamento di minacce e anomalie. In altre parole, un sistema è resiliente quando può adattarsi alle sfide interne ed esterne, cambiando i suoi metodi di funzionamento, mentre continua ad operare. La resilienza del sistema, implica, a differenza della robustezza, qualche cambiamento fondamentale nelle attività principali del sistema, che deve adattarsi al nuovo ambiente. Come accennato in precedenza, in passato era comune usare le firme per classificare gli attacchi maligni, sfruttando database di minacce conosciute. Tali misure, tuttavia, stanno diventando molto meno efficaci contro gli ultimi ceppi di malware avanzato, che si evolvono ogni secondo.

Le soluzioni di IA per la sicurezza informatica consentono un passaggio fondamentale, da un rilevamento basato sulla firma, ad un monitoraggio più flessibile e continuo della rete, che si discosta dai suoi normali comportamenti. Inoltre, l'intelligenza artificiale è utilizzata per creare analisi in tempo reale e specifiche per il cliente, migliorando la percentuale totale di malware identificati e riducendo i falsi positivi. Infine, le organizzazioni stanno usando l'analisi predittiva basata sull'IA per determinare la probabilità di attacchi, migliorando la difesa della rete di un'impresa attraverso disposizioni di dati quasi in tempo reale. Lo studio predittivo può aiutare a elaborare in tempo reale dati da varie fonti e identificare i vettori di attacco aiutando a gestire i big data, filtrando automaticamente i duplicati, categorizzando le informazioni e suggerendo a quale falla dare la priorità. In questo modo l'analisi predittiva riduce gli errori umani ed il carico di lavoro degli analisti della sicurezza.

Risposta

La resilienza e la risposta del sistema sono profondamente connesse ma logicamente interdipendenti, poiché, per rispondere ad un attacco informatico, è necessario sia rilevare ciò che si sta verificando, sia sviluppare e distribuire una risposta appropriata. La prevenzione dei cyber-attacchi sta andando sempre più nella direzione di sistemi in grado di implementare soluzioni in tempo reale alle vulnerabilità di sicurezza. L'IA può aiutare a ridurre il carico di lavoro degli esperti di cybersecurity dando priorità alle aree che richiedono maggiore attenzione e automatizzando alcuni dei loro compiti. Questo aspetto è particolarmente rilevante se si considera la carenza d'offerta di professionisti nel settore della cybersecurity, che attualmente è stimata in quattro milioni di lavoratori[6].

L'intelligenza artificiale può facilitare le risposte agli attacchi schierando, per esempio, esche semiautonome che creano una copia dell'ambiente in cui gli aggressori intendono infiltrarsi. Questi li ingannano ed aiutano a capire i payload (i componenti dell'attacco responsabili dell'esecuzione di un'attività per danneggiare l'obiettivo). Le soluzioni d'IA possono anche segregare dinamicamente le reti per isolare le risorse in aree controllate o reindirizzare un attacco lontano dai dati di valore. Inoltre, I sistemi di intelligenza artificiale sono in grado di generare honeypots adattivi (sistemi informatici destinati a imitare probabili obiettivi degli attacchi informatici [7]) e honeytokens (pezzi di dati resi attraenti ai potenziali aggressori). Le honeypots adattive sono più complesse delle tradizionali nella misura in cui cambiano il loro comportamento in base all'interazione con gli attaccanti. Sulla base della reazione dell'aggressore alle difese, è possibile capire le

[6] (**en**) (isc)[2], (2019), "Cybersecurity Workforce study strategies for building and growing strong cybersecurity teams"
[7] (**en**) Kaspersky, "What is a honeypot?"

sue abilità e i suoi strumenti. La soluzione d'IA arriva a imparare il comportamento dell'attaccante attraverso questo strumento, in modo da riconoscerlo e affrontarlo durante i futuri attacchi.

Problematiche etiche

Il ruolo che l'Intelligenza Artificiale potrebbe svolgere per la robustezza, la risposta e la resilienza del sistema porta con sé sfide etiche che potrebbero ostacolare la sua adozione nella sicurezza informatica. Inoltre, se le questioni non sono adeguatamente affrontate attraverso processi e politiche governative, si potrebbero creare problematiche significative per la nostra società.

Come menzionato all'inizio di questo capitolo, la robustezza del sistema è migliorata usando l'IA per il test del software e per progettare un software che sia capace di auto-testarsi e auto-ripararsi. L'autotest si riferisce alla capacità di un sistema o componente di monitorare il suo comportamento dinamico di adattamento ed eseguire test di runtime in anticipo o come parte del processo di adattamento. In questo contesto, quindi, l'intelligenza artificiale può consentire la verifica continua dei sistemi e l'ottimizzazione del loro stato e rispondere rapidamente a condizioni mutevoli, apportando le opportune correzioni. Ma chi controlla il sistema artificiale? Infatti, anche se l'articolo 22 del GDPR afferma che "nessuna decisione importante riguardante un individuo, come la profilazione, deve essere presa esclusivamente da un sistema autonomo"[8], rimane poco chiaro, ed è lasciato alle aziende, decidere dove finisce il controllo umano ed inizia l'automazione. Inoltre, rimane ad interpretazione come assicurarsi che il sistema si stia comportando secondo le aspettative. Come già detto, l'intelligenza artificiale può migliorare notevolmente la risposta dei sistemi, per esempio riparando automaticamente le vulnerabilità. Allo stesso modo, può anche offrire opzioni offensive per la risposta alle minacce. Ci sono sistemi di sicurezza informatica autonomi e semi-autonomi che offrono una serie di risposte predeterminate a un'attività specifica, permettendo il dispiegamento di risposte offensive specifiche. L'IA può affinare le strategie e lanciare contro-operazioni più aggressive, che potrebbero facilmente sfuggire al controllo dei suoi utenti e alle intenzioni del progettista. Questo potrebbe sfociare in un'intensificazione dei cyber-attacchi e delle contro-risposte, che, a loro volta, comportano un serio rischio di escalation in un conflitto catastrofico, minacciando le infrastrutture chiave delle nostre società. Se l'aggiunta di uno strato umano causerà inevitabilmente un ritardo in tali risposte, da un punto di vista sociale questa situazione solleva comunque la questione della responsabilità: come possiamo attribuire le responsabilità ai sistemi di risposta autonomi? Possiamo responsabilizzarli?

Inoltre, delegare il rilevamento delle minacce completamente ai sistemi di intelligenza artificiale sarebbe un errore poiché potrebbe portare a una diffusa dequalificazione di esperti. Anche allo stato dell'arte della tecnologia, i sistemi di IA non sono ancora in grado di comprendere completamente attacchi e minacce complessi. L'interazione umana è necessaria per valutare i risultati, combinare gli allarmi, ricostruire l'attacco che ha avuto luogo, identificare le opzioni di risposta e per valutare e selezionare la migliore. In questo contesto, gli esperti di cybersecurity dovrebbero continuare a trovare le vulnerabilità e rilevare le minacce nello stesso modo in cui i radiologi devono continuare a leggere le radiografie o i piloti che fanno atterrare gli aerei, in modo da essere ancora in grado di farlo se l'IA fallisce o sbaglia. È interessante notare

[8] (**en**) GDPR Commissione Europea, (27 aprile 2016), Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

che, negli ultimi anni, la Marina degli Stati Uniti ha ripreso ad insegnare ai marinai a navigare secondo le stelle, per mezzo dei crescenti timori di cyber-attacchi sui sistemi di navigazione elettronica. [9]

Un esempio concreto: DarkTrace

Fondata nel 2013 da matematici ed esperti di cyber intelligence governativi, Darktrace è stata la prima azienda ad applicare l'IA alla sfida della sicurezza informatica aziendale.

Qualcosa in più del classico multi-layer security, ossia protezioni diverse per ogni livello della pila di protocolli TCP/IP piuttosto che ISO/OSI, agisce come un sistema immunitario, poco invasivo e non manipolabile, ma in grado di mettersi in movimento in caso di attacco, interno o esterno**.**

Il software registra pacchetto per pacchetto ciò che è successo negli ultimi cinque mesi, permettendo ai tecnici di controllare se un brute force è andato a buon fine ed inoltre esportando i file su wireshark, di appurare le finalità dell'attaccante e cosa abbia fatto con i nostri dati. Alcuni esempi di utilizzo concreto possono quindi essere:

- **Identificare un data exfiltration**

  Se un dipendente malevolo dovesse caricare su mega una cartella, questo viene segnalato grazie al log, il quale avverte in tempo reale che una grossa quantità di dati è in upload su un sito di file sharing.

- **Rilevare dispositivi compromessi come IoT devices che non possiedono antivirus**

  Sempre tramite il log, il software percepisce che un dispositivo compromesso cambia comportamento e lo blocca (in circa un minuto, a differenza dei circa due mesi delle soluzioni canoniche)

- **Investigare attività passate per determinare se c'è stato un data breach**

  Una funzione fondamentale, poiché per questioni di conformità, un'azienda deve poter stabilire e comunicare ai propri clienti se i loro dati sono stati esposti.

  Avendo abilitato i log su tutti i dispositivi, l'Intelligenza artificiale analizza, con un controllo incrociato, i dati, per capire se c'è stato un data breach.

Le tecnologie principali che DarkTrace mette a disposizione dei propri clienti sono 3, che rispecchiano a pieno le tre caratteristiche base di robustezza, resilienza e risposta viste in precedenza:
Entreprise immune system: autoapprendimento che rileva nuovi attacchi e minacce interne nella loro fase inziale, osservando gli utenti, dispositivi ed i flussi di lavoro apprende "in corso d'opera" tutto ciò che è normale per l'organizzazione.

[9] (**en**) Seaman S. Apprentice e Jordan Ripley (2019), "Navigating by the Stars"

Antigena: difesa contro le minacce informatiche in corso, arrestandone prima che si verifichi qualsiasi danno, per questo è fondamentale che il software agisca in tempo reale ed aggiornate ripetutamente attraverso l'osservazione continua delle minacce non appena si diffondono

AI Analyst: consulente per un'indagine qualificativa della sicurezza aziendale, in grado di correlare intelligentemente dati eterogenei all'interno della nostra azienda e di mettere in luce problematiche ad alta priorità prima ancora che avvengano.

Darktrace è attualmente utilizzato da parecchie multinazionali ed aziende con grossa esposizione ad attacchi, quindi ben intenzionate a curare il processo di cybersecurity, come Allianz, AirMalta e Samsung per citarne alcune. Sembra quindi che l'azienda inglese abbia avuto una visione lungimirante sul futuro della sicurezza e si stia muovendo nella direzione giusta per dominare il settore.

Bibliografia

- (**en**) Pupillo, Fantin, Ferreira, Polito (2021), Artificial Intelligence and cybersecurity (CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf)
- Visionary Day Swiss, Lugano. *Intelligenza artificiale e Machine learning al servizio della cyber security*. (2020). Alberto Redi, Corrado Broli, Mariana Pereira e Jacopo Maria Tavaroli. (YouTube video)