Cyber security, intrusion detection systems e intelligenza artificiale

di Caterina Patrizia Morano

Abstract

L'enorme mole di dati che circolano nel mondo digitale – fatto di computer, smartphone e tablet interconnessi tra loro – rappresenta un'occasione per le organizzazioni criminali. I punti di forza di chi vuole penetrare in un sistema informatico (che sia un computer o che sia un complesso insieme di dispositivi tecnologici di una grande organizzazione) sono molteplici data anche la difficoltà nel coprire tutte le potenziali vulnerabilità dei sistemi stessi. In questo breve saggio Caterina Patrizia Morano, ricercatrice e consulente informatica, introduce, con un linguaggio chiaro e semplice, alcuni temi chiave della sicurezza cyber evidenziando, in particolare, la necessità di adottare strumenti e comportamenti che proteggano le dotazioni informatiche delle aziende secondo gli standard internazionali.

Profilo dell'autore

Caterina Patrizia Morano è laureata in informatica, ha completato la formazione presso il Research Centre On Software Technology, lavorando in progetti di ricerca di cibernetica, intelligenza artificiale, sicurezza informatica. Svolge attività di consulenza informatica per importanti aziende e ha scritto per le più importanti riviste a tiratura nazionale di informatica, pubblicando numerosi articoli su sicurezza informatica e testi per i programmatori italiani del linguaggio PHP.

Keyword

Cyberspace, intelligenza artificiale, intrusion detection systems

Introduzione

La sicurezza digitale è, oggi, tematica attuale e oggetto di recente, massima attenzione da parte di tutti i Governi, tanto da decidere di dedicare ad essa specifici piani strategici come il Piano Nazionale per la protezione cibernetica e la sicurezza informatica[1] stilato dall'Italia. Fino a qualche anno fa, però, le problematiche di sicurezza digitale erano relegate ai laboratori di Informatica laddove professori e studenti approfondivano gli aspetti di difesa dei sistemi informatici, sia software che hardware. Ivi si studiavano tecniche di attacco formando i cosiddetti white hat hacker[2]: gente molto responsabile delle potenzialità, anche negative, affidate nelle loro mani che avrebbero dovuto, sulla base della conoscenza acquisita, sperimentare sistemi di protezione e blindatura delle informazioni oppure sferrare attacchi simulati su interi sistemi informatici aziendali al fine di far prendere coscienza ai proprietari dei rischi che correva la loro infrastruttura.

Al contrario di ciò che si potrebbe pensare, il concetto di sicurezza informatica non è nato però con la nascita dell'informatica. Piuttosto è frutto dell'era dell'interconnessione, a partire dall'implementazione di internet ovvero del WWW – World Wide Web – la ragnatela mondiale di pagine web, inventata dall'informatico Tim Berners-Lee, come supporto al lavoro dei fisici del CERN nel 1991, per i quali Berners-Lee lavorava come consulente in ingegneria del software.

L'esigenza di sicurezza informatica

I computer, prima del 1991, eccetto rari casi, erano tutti dispositivi stand-alone: privi cioè di alcuna interconnessione tra essi, erano utili all'utente principalmente per la loro potenza di calcolo ma ben lontani dall'essere il prezioso strumento di comunicazione che conosciamo oggi. Dai primi anni '90, però, l'idea di mettere risorse a disposizione di chiunque desiderasse consultarle prese sempre più piede. La prima implicazione divenne la necessità di sperimentare e utilizzare nuove tecnologie che permettessero di raggiungere tutti i computer (ed in seguito tablet, smartphone, ecc.) connessi alla rete per condividere e consultare le informazioni in essi contenuti. È qui che sorsero importanti interrogativi e, conseguentemente, la necessità di risolvere problemi correlati agli interrogativi stessi. Quegli stessi problemi che chi si occupa di cyber defence oggi deve affrontare:

- come essere sicuri che la nostra connessione alla rete, sia che si tratti di un computer singolo, sia che si tratti di una rete aziendale o di un sistema informatico che gestisce il processo industriale di una struttura produttiva non sia forzato?
- esistono delle tecnologie che permettano di individuare gli intrusi che si sono infilati in una rete informatica?
- individuato un attacco, come ripristinare le risorse del sistema?

La questione si complica quando ci si trova in presenza di un attacco che coinvolge l'ICN (infrastruttura critica nazionale), quell'insieme di strutture di un Paese quali la rete idrica o energetica, obiettivi primari in scenari di cyber war[3].

In questo caso, per ricavare le corrette ed adeguate strategie di risposta, chi si occupa di cyber defence deve aggiungere, ai precedenti interrogativi, anche i seguenti:

- da dove proviene l'attacco?
- qual è il movente dell'aggressore?

Nel caso di un'intrusione in un computer privato infatti, per i motivi che spiegheremo di seguito, l'attacco può essere casuale e non finalizzato a nuocere in maniera diretta la macchina che è stata forzata. Diversamente, com'è facile immaginare, quando si parla di ICN dietro c'è sempre una chiara finalità e uno studio attento e approfondito del sistema obiettivo.

Siamo tutti soggetti digitali a rischio

Iniziamo per prima cosa a capire qual è il rischio reale a cui è sottoposto un normale computer privato, che sia una home station oppure un computer di ufficio aziendale. Il convincimento dell'utente medio è che nella vastità di computer connessi, probabilmente un hacker (ma sarebbe meglio definirlo cracker[4]) non punterà al suo… Ma il pericolo è molto più realistico di quanto si immagini!

Per capire la vulnerabilità dei comuni sistemi rispetto ad un attacco esterno bisogna riportare due numeri.

Il primo è il numero di computer connessi alla rete web che da ultimissimi dati si attesta a circa due miliardi di macchine. L'altro invece è il numero di porte di accesso che ogni singolo computer offre rispetto ai protocolli di connessione TCP[5] e UDP[6]: in totale 131.072[7]. Quindi ogni computer offre ai due miliardi di altri computer connessi nel mondo più di 131 mila porte di ingresso!

A questo punto bisogna ragionare sulle probabilità di diventare realisticamente oggetto di un attacco. Ovvero: che possibilità ha un comunissimo utente tra due miliardi di altri utenti, di diventare un bersaglio? Che appetibilità può avere per un ficcanaso digitale una piccola work station casalinga?

Il motivo più banale può essere quello di carpire codici segreti delle carte di credito e dati bancari da vendere poi a qualche carder[8]. Soprattutto se, ignaro del rischio che corre, il proprietario del computer forzato ha memorizzato sia il numero della carta che il pin, che i dati di accesso al proprio conto online. Operazione che darà i suoi frutti solo se i computer analizzati saranno davvero moltissimi.

Un altro movente per essere violato è quello di diventare, inconsapevolmente, uno Zombie[9] digitale e partecipare ad una botNet[10]! Un esercito di milioni di computer che, mentre svolgono regolarmente il loro compito (magari un po' più lentamente del solito), dopo essere stati infettati da un trojan[11], sono passati sotto il controllo di un botMaster[12] che li utilizza, tutti insieme, contemporaneamente, per sferrare attacchi a server di enti e società governative, multinazionali e aziende le cui informazioni sono molto appetibili per il mondo criminale.

Necessaria e sottovalutata

Da quanto detto prima si evince l'importanza di programmare interventi di sicurezza in maniera seria e professionale al fine di impedire gli accessi indesiderati e utilizzare solo le connessioni necessarie in condizioni di sicurezza. Purtroppo però, recenti ricerche hanno evidenziato come ancora non sia emersa una reale e concreta consapevolezza del rischio informatico. Da indagini di mercato risulta infatti che in Europa, soltanto il 20% dei leader aziendali ritenga che la cyber security sia un fattore di importanza rilevante, con conseguente scarso interesse nei confronti di investimenti in tale direzione, sia in termini di sistemi di protezione che di formazione del personale[13]. Ulteriori dati sottolineano inoltre che, a livello mondiale, soltanto il 44% dei computer è protetto da meccanismi di sicurezza. Tale percentuale per l'Italia è ancor più bassa: solo un terzo delle macchine è protetto!

Le tipologie di attacco

Entriamo quindi nel cuore del problema. Proteggere i requisiti di sicurezza di un sistema significa, in termini realistici, ridurre ad un valore accettabile la probabilità che vengano violati per mezzo di eventi indesiderati, individuandoli tempestivamente quando ed in quale parte del sistema questi accadano, limitandone i danni e ripristinando i requisiti violati nel minor tempo possibile.

È importante che queste misure siano adottate in maniera organica e sistematica, nell'ambito più generale di una politica di sicurezza e nel rispetto dei vincoli tecnici, logistici, amministrativi, politici ed economici imposti dalla struttura in cui il sistema opera.

La violazione di un sistema informatico viene classificata in letteratura in funzione del primum movens. Ma non solo. La prima classificazione avviene osservando se siamo di fronte ad un evento casuale o se si tratta di un vero e proprio attacco.

Definiamo l'evento indesiderato un accesso che non sia permesso dalla politica di sicurezza del sistema.

Stando alle statistiche, gli eventi indesiderati accidentali, quali il guasto di un dispositivo o l'errore umano come la cancellazione accidentale di un file, l'installazione di componenti incompatibili o infettate che corrompono il software di base restano la principale causa di perdita accidentale di dati.

Un insieme minore ma di assoluto rilievo è rappresentato dagli attacchi deliberati, per i quali è importante partire dal presupposto che chiunque tenti di penetrare nel sistema o di danneggiarlo applicherà, in sequenza o in parallelo, sfruttando eventuali effetti combinati, tutte le tecniche di cui dispone su tutte le componenti attaccabili.

Appare naturale caratterizzare un attacco in funzione della componente attaccata e della tecnica utilizzata dall'intruso. Un approccio sistematico parte dall'elencazione di tutte le parti del sistema. Sia fisiche, come calcolatori, router, cavi, che logiche quali file e processi. Lo step successivo è l'individuare di tutte le tecniche di attacco ad esse applicabili creando una matrice componente/tipologia di attacco.

Gli attacchi a livello fisico sono principalmente tesi a sottrarre o danneggiare risorse critiche mediante furto, attacco alla disponibilità ed alla riservatezza, danneggiamento.

Gli attacchi a livello logico (livello di interfaccia o client, livello applicazione o application server, livello di dati o data-server, livello mainframe) sono principalmente tesi a sottrarre informazioni e degradare l'operatività del sistema.

I diversi tipi di attacchi:

- attacchi di intercettazione: possono richiedere un attacco preventivo a livello fisico per installare dispositivi pirata o di intrusione a livello logico. Le tecniche solitamente usate sono: sniffing[14], spoofing[15] o programmi che emulano servizi del sistema per capirne informazioni preziose
- attacchi basati sulla deduzione: sono condotti incrociando informazioni tratte dall'osservazione del sistema con informazioni ottenute attraverso altre vie, spesso con metodi di social engineering[16], come per esempio informazioni sulle persone che utilizzano il sistema e che potrebbero aiutare a dedurre password e codici
- attacchi di disturbo: sono quegli attacchi che hanno l'obiettivo di degradare l'operatività del sistema mediante virus[17], worm[18] o fenomeni di denial of service[19]. Si possono considerare come atti di sabotaggio, minacciando l'integrità e la disponibilità dei dati, più raramente la riservatezza

- attacchi di intrusione: si verificano quando il sistema non prevede strumenti evoluti per il riconoscimento dell'utente o quando vi sono degli ingressi non autorizzati attraverso le porte di connessione del computer.

Le contromisure

Per contromisure si intende l'insieme di azioni che concorrono, attivamente o passivamente, a:

- minimizzare la probabilità che gli eventi indesiderati accadano
- rilevare il fatto che siano accaduti
- individuare e minimizzare le conseguenze
- ripristinare il corretto funzionamento del sistema.

Una prima possibilità di classificare le contromisure consiste nell'osservarle in funzione degli eventi indesiderati che vanno a contrastare, affiancando a ciascun evento indesiderato le contromisure applicabili:

- contromisure preventive: finalizzate a minimizzare la probabilità che un evento indesiderato accada
- contromisure correttive: tese a riparare i danni causati da eventi indesiderati che, a dispetto delle contromisure preventive, siano ugualmente accaduti
- contromisure informatiche: basate sulla tecnologia informatica
- contromisure organizzative: riconducibili all'organizzazione che utilizza il sistema informatico ed alle norme e regole di comportamento stabilite dal personale
- contromisure operanti a livello fisico: proteggono i dispositivi (calcolatori, cavi, apparecchiature di rete, locali, impianti di alimentazione e condizionamento, ecc.) da attacchi di tipo fisico quali furto e danneggiamento
- contromisure operanti a livello logico (come ad esempio i software anti-virus): proteggono risorse logiche (basi di dati, registri di configurazione, moduli software, ecc.) da attacchi di tipo logico.

Una condizione essenziale affinché la tecnologia a protezione di un sistema informatico risulti efficace è che venga utilizzata nel modo corretto da personale pienamente consapevole della sua importanza.

Occorre, innanzi tutto, una forte dichiarazione d'intenti da parte dei vertici dell'organizzazione che gestisce il sistema. Devono essere quindi definiti con precisione i ruoli e le responsabilità nella gestione sicura del sistema e per ciascun ruolo: dall'amministratore al semplice utente, e quindi devono essere definite norme comportamentali e procedure precise da rispettare.

Affinché tutti gli aspetti procedurali vengano compresi e attuati correttamente è fondamentale istruire il personale a tutti i livelli con opportuni corsi di addestramento. I ruoli operativi che vengono generalmente definiti, nell'ambito della gestione sicura di un sistema informatico, appartengono a due tipologie, a seconda che controllino gli aspetti fisici o logici del sistema.

Relativamente alle contromisure basate sulla tecnologia informatica, un interessante criterio di classificazione è quello basato sul livello architetturale nel quale la contromisura agisce. Conviene

in tal senso distinguere fra contromisure a livello di applicazione, quindi specifiche del particolare sistema informatico considerato, e contromisure di base a carattere generale.

Le contromisure operanti a livello applicazione sono spesso caratterizzate da un'efficacia elevata, ma relativa ad un insieme tipicamente ristretto di eventi indesiderati che è quello specificamente previsto per l'applicazione che vanno a proteggere.

Le contromisure che operano a livello di DBMS[20], sistema operativo o rete hanno carattere più generale, rispetto al livello applicativo e indipendenti dalla particolare applicazione eseguita. Di conseguenza, sono spesso meno sofisticate di quelle a livello applicazione, ma dotate in compenso di un più ampio grado di copertura rispetto alla gamma degli eventi indesiderati che vanno a contrastare.

Le buone pratiche

Qualunque sia il campo applicativo di un'azienda, ente o organizzazione, come abbiamo detto, è di fondamentale importanza applicare dei protocolli precisi per ottenere gli obiettivi di sicurezza, ormai imprescindibili. È altamente consigliato applicare gli standard internazionali che guidano nell'affrontare le problematiche di cyber security con metodologie precise e pianificate.

Uno degli standard più diffusi è l'ISO/IEC 27002. Pubblicato dall'International Organization for Standardization (ISO) e dall'International Electrotechnical Commission (IEC) prende come titolo *Information technology – Security techniques – Code of practice for information security management*. Riportiamo, citando la definizione dell'organismo che lo rilascia, gli obiettivi dello standard: «preservare la riservatezza [assicurando che l'informazione sia accessibile solo agli utenti autorizzati], l'integrità [salvaguardando l'accuratezza e la complessità dell'informazione e dei metodi di elaborazione] e la disponibilità [assicurando che gli utenti autorizzati abbiano accesso all'informazione ed alle attività connesse quando richiesto]».

Il documento definisce le politiche di sicurezza attraverso 10 aree di applicazione e controllo:

- Security Policy con direttive generali sulla gestione delle politiche di sicurezza
- Security Organization con direttive sul controllo della sicurezza nell'ambito dei soggetti dell'organizzazione che ne fa uso
- Asset Classification and Control con direttive in merito alle attività e agli strumenti interessati nel processo
- Personnel Security per ridurre i rischi di comportamenti che minino la sicurezza da parte del personale interno all'organizzazione
- Physical and Environmental Security con informazioni in merito alla protezione dei sistemi fisici e strumentali aziendali
- Communications and Operations Management per la gestione corretta ed in sicurezza delle flusso delle comunicazioni ed operativo
- Access control che si occupa invece della gestione degli accessi con la definizione dei ruoli e permessi
- System Development and Maintenance per il controllo del corretto sviluppo, funzionamento e manutenzione dei sistemi utilizzati

- Business Continuity Management che si occupa di prevenire e neutralizzare le interruzioni di attività rilevanti per l'attività economica dell'azienda
- Compliance per il controllo dell'adeguatezza del sistema alle norme civili, penali e dei requisiti di sicurezza.

Un intruso non bussa mai

L'adeguamento agli standard è un ottimo approccio alla sicurezza di tipo preventivo. L'adozione di buone pratiche rende senz'altro i sistemi più protetti ma, chiaramente, non ne garantisce l'infallibilità.

Quanto più il sistema informatico contiene informazioni 'critiche', tanto più sarà appetibile a cyber malintenzionati che tenteranno tutti i modi per forzarlo. Studiandolo con pazienza, sferrando attacchi conoscitivi, sfruttando le falle proprie dei vari sistemi operativi o dei software applicativi installati.

E se riuscissero ad entrare? Semplicemente, non ce ne accorgeremmo!

Anche se quando lavoriamo parliamo di finestre, di porte, di lavagne (i desktop), di cartelle, in realtà stiamo indicando con dei nomi di uso comune nella nostra vita quotidiana delle rappresentazioni digitali fatte di zero e uno e che rappresentano, a loro volta, delle tensioni elettriche. Quindi, una cartella non è altro che un oggetto digitale che chiamiamo così per convenzione e semplicità. Se qualcuno sta spiando all'interno della cartella non ce ne accorgiamo, anche se la consultiamo contemporaneamente. Così come le porte di accesso di cui abbiamo parlato in precedenza sono dei connettori logici da cui passano altrettanti segnali elettrici. Se qualcun altro entra attraverso una di queste porte all'interno del nostro computer non ce accorgiamo.

È per questo motivo quindi che risulta opportuno installare dei dispositivi le cui funzionalità siano quelle di monitorare se qualcuno si è introdotto nel sistema. Soprattutto quando ci sono dati critici da proteggere.

Da anni ormai si sperimentano diverse tipologie di sistemi informatici che hanno l'obiettivo di scovare gli intrusi che sono all'interno di computer e reti di organizzazioni. Questi sistemi prendono il nome di Intrusion Detection Systems.

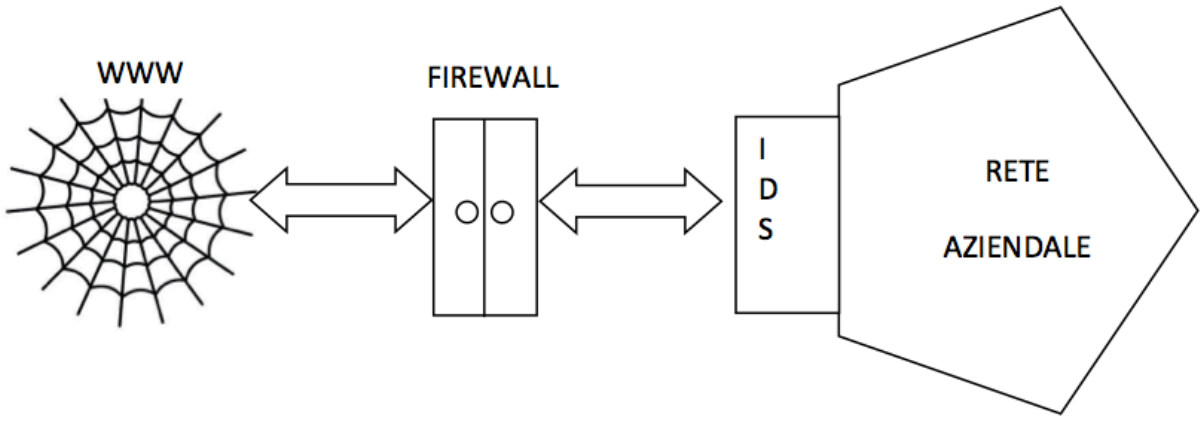
Intrusion Detection Systems

Con il nome di Intrusion Detection System (IDS) si definisce una tecnologia che svolge il suo compito nell'identificare, prevenire e, possibilmente, reagire a una entry non autorizzata e/o attività maliziosa. Ciò avviene monitorando un particolare insieme di attività, sia all'interno del sistema obiettivo, sia relativamente alla rete e al suo traffico per capire se c'è qualche comportamento anomalo che possa essere ricondotto ad un'intrusione.

L'obiettivo principale dell'IDS è classificare le attività di rete tra quelle intrusive e non intrusive in maniera efficiente, minimizzando, per quanto possibile, i falsi positivi ed utilizzando tecnologie che permettano al sistema stesso di apprendere dallo storico del suo funzionamento.

Un IDS protegge il sistema da attacchi, usi impropri e compromissioni. Tali sistemi sono in grado di monitorare l'attività di una rete, rivedere le configurazioni del sistema e del network alla ricerca di punti deboli, analizzare l'integrità dei dati.

Non sono, però, da confondere con i firewall: questi ultimi possono essere idealmente rappresentati come delle porte blindate che servono ad impedire l'ingresso non autorizzato, filtrando i pacchetti di informazione prima del loro ingresso. Gli IDS sono posti dopo, così come raffigurato nell'immagine che segue per monitorare non già il traffico esterno, ma quello interno alla rete aziendale.



Tipi di IDS

Le caratteristiche di progettazione di un IDS e le funzioni che esso è in grado di fornire, rappresentano la base per determinare l'implementazione di sicurezza più idonea. Esistono differenti tipi di IDS. Le diverse categorie identificano la capacità del sistema di intervenire per bloccare l'intrusione (Passive IDS versus Active IDS[21]), sia l'ambito in cui tali tecniche vengono applicate (Network-based IDS versus Host-based IDS[22]) ma anche le capacità che i sistemi utilizzano per scovare l'intruso (Misuse detection versus Anomaly detection).

Concentriamo il discorso sulle tecnologie di rilevamento Misuse e Anomaly detection.

I sistemi Misuse ID svolgono il loro compito di individuare comportamenti anomali mettendo a confronto i dati derivanti dall'analisi del traffico e un insieme di regole predefinite (di buon funzionamento) che ricercano comportamenti sospetti. In buona sostanza, il sistema riconosce gli attacchi che rientrano in determinate categorie già note e di cui ne riconosce la firma o il pattern[23]. Il limite di questi sistemi si evince dalla stessa descrizione: un comportamento sospetto viene riconosciuto allorquando sia già noto e studiato con classificazione dei pattern e/o firme.

I sistemi Anomaly detection sono basati, come dice il nome stesso, sulla ricerca di anomalie di funzionamento all'interno della rete ma anche dei sistemi operativi dei computer stessi. Essi sono dotati di una base di dati in cui sono memorizzate le informazioni che caratterizzano il normale o comunque accettabile funzionamento del sistema informatico, quali possono essere la percentuale di uso della CPU[24] il tempo di esecuzione delle applicazioni, le chiamate di sistema. Quando i dati elaborati contengono delle anomalie, l'IDS manda un allarme intrusione. Quali sono le

problematiche inerenti all'uso di questo tipo di IDS? I falsi allarmi. Per un funzionamento ottimale l'Anomaly IDS dovrebbe essere dotato di una robusta base di dati contenente le informazioni sul normale funzionamento di apprezzabile complessità oltre che di capacità di auto-apprendimento dalla casistica pregressa. Requisiti non banali.

L'efficacia dei sistemi di rilevamento intrusioni

Sin dalla loro introduzione, l'efficacia degli Intrusion Detection Systems è stata espressa in funzione di un dataset di valutazione per la misurazione, in maniera canonica, dei requisiti di performance, correttezza e usabilità. Tuttavia, l'opera dei ricercatori si è concentrata ben presto su altri tipi di test di valutazione quali l'accuratezza e l'efficacia dei sistemi, confrontando la percentuale di falsi allarmi in relazione agli attacchi effettivi rilevati. Negli anni, sono stati raccolti molti dati relativi alle prestazioni e validati diversi database operativi per la misurazione dell'efficacia, esprimendo metriche di rappresentazione della percentuale dei falsi positivi, dei rilevamenti effettuati, della precisione del sistema, delle prestazioni misurate secondo le curve ROC, tecnica statistica di misura dell'accuratezza di un test diagnostico lungo tutto il range dei valori possibili.

L'efficacia espressa in relazione a prototipi di laboratorio può però risultare difficile da riportare nel mondo reale.

Il dominio in cui si progetta l'applicazione di un IDS è senz'altro quello di un'architettura di rete complessa, ove vi siano connessi un alto numero di dispositivi e ove la mole di dati elaborata sia di ragguardevole entità. Quel che ne consegue, in tali contesti di reale utilizzo, è che il processo applicativo per il rilevamento dell'intruso diventa lento e che non consente di lanciare un allarme in tempo reale ma si registra piuttosto un ritardo che può pregiudicare l'azione di ripristino della condizione di sicurezza.

Allo stato attuale gli IDS più efficaci sono quelli basati su un insieme di sistemi esperti[25]. Essi utilizzano diverse basi di dati in cui sono memorizzate le informazioni che aiutano a decidere il sistema se si è sotto attacco o meno. La scelta del sistema esperto più adeguato viene gestito da un supervisore classificatore, che funziona anche da sensore, che prende le decisioni. Ciò significa che piuttosto che fare lo screening di tutti i dati su cui si basa la classificazione, il sistema è in grado di decidere la base di dati più giusta, migliorando il processo rispetto ai requisiti di valutazione.

In passato sono state applicate varie tecniche di classificazione, mutuate da varie discipline quali statistica, intelligenza artificiale, cibernetica, reti neurali.

Recentemente, gli avanzamenti nel campo dell'intelligenza artificiale hanno permesso di applicare nuove tecniche ai sistemi oggetto del nostro articolo, con successo, raggiungendo diversi obiettivi solo lontanamente sfiorati in passato. In particolare, le tecniche dell'intelligenza artificiale hanno potenziato i sistemi grazie alla:

- flessibilità rispetto alle architetture hardware e software
- adattabilità rispetto alle regole specifiche delle tecniche convenzionali
- capacità di riconoscere pattern e rilevamento di nuovi pattern non noti
- aumentate capacità di calcolo

- capacità di apprendimento automatico.

L'ultima caratteristica è probabilmente la più interessante ed è quella che si avvantaggia degli studi sull'apprendimento tramite esempi.

È possibile per una macchina apprendere?

Diverse sono le definizioni di apprendimento. L'apprendimento potrebbe essere definito come la possibilità degli esseri umani – che anche i calcolatori dovrebbero avere - di accrescere la propria conoscenza ed abilità, componente fondamentale dell'intelligenza. Potrebbe un essere umano essere definito intelligente se compisse continuamente gli stessi errori senza migliorare le proprie prestazioni attraverso lo studio e l'esercizio? Senz'altro no. Secondo la definizione precedente, però, è anche vero che, malgrado sia detto comunemente macchina intelligente, un computer, se non sa migliorare la propria capacità risolutiva nei confronti dei problemi, intelligente non lo è proprio.

Lo sforzo dell'intelligenza artificiale è stato, fin dall'inizio, di arrivare ad elaborare un modello di apprendimento valido per le macchine. Modello applicabile anche sulle persone, al fine di rendere un processo, quello di apprendimento, appunto, da lungo, faticoso e caotico (come tutte le intelligenze umane ben riconoscono) ad una sequenza di strategie che estraggano regolarità e principi di ordine superiore da un insieme di dati disomogenei e, spesso, contraddittori.

Ma c'è di più della semplice astrazione di regole. Rovesciando la medaglia, una macchina dotata di un processo cognitivo strutturato, definito sistema esperto, una volta formulato un valido modello di apprendimento, avrà come obiettivo l'emulazione o anche il superamento delle capacità dei migliori esperti umani nella risoluzione di problemi in domini ristretti a carattere specialistico. Lasciando all'operatore umano, solo, la discrezionalità e il momento di validazione dell'intervento proposto dalla macchina.

Un sistema esperto possiede come base di conoscenza le informazioni che gli sono state fornite quando è stato programmato. Ma è stato programmato anche per subire delle modifiche nel corso del tempo, durante il suo funzionamento. Con l'apprendimento, un sistema arricchisce, autonomamente, la propria base di conoscenza con delle nuove espressioni formulate secondo un linguaggio formale – logica, reti semantiche, sistemi di produzioni – in modo da poterle utilizzare in un'occasione successiva. D'altro canto, secondo le prime definizioni di sistema esperto, nell'ottica di apprendimento inteso come miglioramento, i cambiamenti che avvengono nel sistema gli permettono di funzionare meglio nell'ambiente nel quale esso deve operare in termini di efficacia (il sistema impara a fare più cose di quante ne sapeva fare in precedenza) e efficienza (il sistema impara a fare meglio le cose che già sapeva fare).

L'apprendimento tramite esempi di una macchina

In realtà le normali macchine computazionali hanno seguito un processo di apprendimento: tutte le istruzioni che eseguono sono state registrate nel sistema ed esso, rispondendo agli stimoli dell'operatore, utilizza tale conoscenza per eseguire dei compiti. Anche i sistemi per l'identificazione degli intrusi di cui abbiamo parlato si comportano così. Essi vengono programmati con una base di conoscenza: sanno se condurre la caccia nel network aziendale o in un sistema operativo, se sono di tipo reattivo sanno come riportare le cose al loro posto al verificarsi di un dato

fatto, sanno cercare una firma e riconoscere un comportamento anomalo confrontandolo con la loro conoscenza di comportamenti normali. Il salto in avanti è la programmazione di sistemi che al verificarsi di un fatto nuovo, siano in grado di applicare delle regole di inferenza[26] per astrarne una nuova da applicare in futuro. È questo l'apprendimento tramite esempi.

Conclusioni

Pur essendo una tematica molto interessante e avvincente, l'approfondimento di come funzioni nello specifico una macchina programmata per apprendere da sé esula dagli obiettivi del nostro paper. La materia, basata su formalismi matematici e quindi adatta ad essere approfondita per chi possiede le basi giuste per affrontare gli argomenti, può peraltro essere applicata, come abbiamo detto, anche quando ad apprendere sono gli esseri umani, che grazie agli strumenti forniti imparano ad acquisire informazioni più velocemente, a leggere con disinvoltura documenti tecnici, a memorizzare dati efficacemente, soprattutto quando i dati sono molti e il tempo è poco. E questo la rende ancor più affascinante. Senz'altro, quel che possiamo sottolineare con forza, a conclusione dell'articolo, è la necessità di dotarsi, nelle strutture e aziende di qualsivoglia dimensione di adeguate tecniche di protezione che non devono essere disgiunte da corretti e consapevoli comportamenti da parte degli operatori umani. Inoltre, allorquando ci si trovi in presenza di dati critici e quando sia importante accorgersi di presenze indesiderate, bisogna, imprescindibilmente, affidarsi alle più recenti e sofisticate tecnologie dal momento che, di fatto, l'inganno può essere dietro l'angolo.

Note

[1] Adottato dal Presidente del Consiglio dei ministri nel dicembre 2013, il Piano nazionale per la protezione cibernetica e la sicurezza informatica <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf> (ultimo accesso 10 febbraio 2015) individua gli indirizzi operativi, gli obiettivi da conseguire e le linee d'azione da porre in essere per dare concreta attuazione al Quadro strategico nazionale per la sicurezza dello spazio cibernetico <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf> (ultimo accesso 10 febbraio 2015), in linea con quanto previsto dal decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013 recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale <http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/riferimenti-giuridici/normativa-di-riferimento/dpcm-24-gennaio-2013.html> (ultimo accesso 10 febbraio 2015). Con questo ulteriore documento l'Italia si dota di una strategia organica, alla cui attuazione sono chiamati a concorrere non solo gli attori, pubblici e privati, richiamati nel Quadro strategico nazionale ma anche tutti coloro che, su base quotidiana, fanno uso delle moderne tecnologie informatiche, a partire dal singolo cittadino.

[2] White hat hacker: hacker che mette a disposizione le sue competenze in materia di cyber-security a beneficio di aziende e società al fine di testare, implementare e prevenire attacchi informatici sui sistemi in esame, mantenendone l'assoluto riserbo. Si differenzia dal black hat hacker in quanto quest'ultimo mette a disposizione le sue competenze al mondo del crimine informatico o le applica egli stesso, per ottenerne un profitto.

[3] Il termine cyber war, o meglio cyber-warfare, indica le diverse metodologie elettroniche, informatiche e di telecomunicazioni per preparare e condurre operazioni militari tesi all'alterazione e/o distruzione dei sistemi di comunicazione o dell'Infrastruttura critica di un Paese.

[4] Cracker: persona che rompe o elude i sistemi di sicurezza di un sistema informatico al fine di trarne profitto. Il cracker è solitamente un esperto di informatica (spesso autodidatta) capace di forzare un sistema mediante l'applicazione sistematica di tecniche sofisticate di attacco. Può agire per proprio tornaconto o al soldo di altri individui che trarranno profitto dalla sua azione. Si differenzia dal *lamer* per la preparazione molto specialistica.

[5] In informatica, allorquando si voglia trasferire l'informazione da un sistema ad un altro è necessario individuare delle regole precise e ben definite per permettere ai sistemi di capirsi tra loro. Questo vale sia all'interno dei componenti della macchina che tra macchine diverse. L'insieme delle regole di comunicazione vengono definite protocolli. Il protocollo TCP (Transmission Control Protocol) si occupa di garantire il corretto trasferimento attraverso la rete di comunicazione.

[6] UDP (User Datagram Protocol) è un altro protocollo delle telecomunicazioni, di minore qualità rispetto a TCP, utile quando si abbiano forti vincoli sulla velocità e l'economia di risorse della rete.

[7] Il numero di porte è rappresentato da cifre a 16 bit. Ciascun protocollo può quindi esprimere un numero di porte pari a 2^{16} - 1= 65.535.

[8] Carder: un criminale il cui obiettivo è ottenere dati sensibili di carte di credito per poi clonarle e rubarne i soldi contenuti. Solitamente, ma non sempre, le operazioni di prelievo sono somme di piccole entità in maniera tale che il malcapitato non si accorga del furto e questo possa essere ripetuto più volte.

[9] Zombie: computer forzato dall'attività di un cracker che ha segretamente preso il controllo del computer della vittima per condurre attività illegali. Lo zombie può lavorare per anni, senza che il proprietario riesca ad accorgersene. Una delle attività più frequenti dello zombie è quello di inviare massicce quantità di spam o di sferrare l'attacco a pagine Web di particolare interesse.

[10] BotNet: una rete di computer che effettuano la stessa attività contemporaneamente, il cui nome deriva dalla combinazione delle parole robot e network. I computer che fanno parte di una botNet vengono cooptati attraverso il download guidato di codice maligno, utilizzando vulnerabilità dei differenti browser, oppure attraverso l'intrusione di un trojan, magari scaricato come attachment di un'email. La prima botNet di cui si abbia traccia risale al 2001 ed è servita per mettere insieme un'imponente operazione di spamming.

[11] Trojan: un programma, apparentemente utile, che invece nasconde delle funzionalità maliziose che infettano il computer.

[12] BotMaster: colui che crea e controlla una botNet e dietro cui si nasconde al fine di compiere crimini informatici senza che le attività di polizia possano collegare l'attività criminale alla persona che la realizza.

[13] Fonte ACS Registrar 2014, <http://www.acsregistrars.it/sicurezza-informatica-usa-piu-protetti-di-europa/> (ultimo accesso 10 febbraio 2015).

[14] Sniffing: l'intercettazione passiva, mediante appositi programmi definiti sniffer, di dati interessanti attraverso l'analisi casuale dei pacchetti che transitano per la rete.

[15] Spoofing: la falsificazione dell'identità attraverso la rete.

[16] Social engineering: la manipolazione psicologica delle persone al fine di carpirne informazioni confidenziali o, direttamente, accesso ai sistemi informatici. Utilizza delle precise e controllate tecniche di persuasione, derivanti dallo studio di come un essere umano prende le decisioni.

[17] Virus: un programma software che può infettare un computer nascondendosi sotto altri file. È dotato di capacità di auto replicarsi fino a rallentare considerevolmente il sistema per sovraccarico delle risorse come le memorie e il processore. Può anche arrecare danni di tipo hardware derivanti da surriscaldamento.

[18] Worm: un programma software di tipo malware che può infettare un computer. Al contrario del virus, non si nasconde dietro altri programmi ma viene solitamente scaricato come attachment di e-mail o attraverso il file -sharing.

[19] Denial of service: una tipologia di attacco che prevede l'accesso al sistema obiettivo al fine di esaurirne le risorse e quindi di bloccarlo temporaneamente.

[20] DBMS (Data Base Management System), sistema per l'organizzazione e la gestione di basi di dati in maniera strutturata.

[21] Gli IDS passivi non hanno la capacità di intervenire rispetto all'anomalia che è stata riscontrata, al contrario di quelli attivi che decidono la strategia più opportuna, derivante dai risultati dell'analisi che hanno condotto.

[22] I Network-IDS effettuano la ricerca all'interno di una rete di computer connessi tra di loro e quindi analizzano il traffico di rete. Gli Host-IDS svolgono la loro azione analizzando il comportamento delle componenti di un computer isolato.

[23] Pattern: schema ricorrente di funzionamento di un software o di un componente hardware.

[24] CPU (Control Process Unit), detto anche processore, è il cuore pulsante di un computer che effettua tutti i calcoli e le elaborazioni.

[25] Software dotato di una base di conoscenza specializzata fornitagli all'atto della programmazione capace di effettuare diagnosi in ambito di interesse specifico, seguendo un modello di ragionamento. Vengono utilizzati al posto dell'operatore umano, o di un team di operatori umani, il cui solo il compito è quello di validare i risultati.

[26] Modello logico per cui, data una serie di assunzioni che fungono da premessa, arrivano a formulare una conclusione.