Il Sistema Immunitario Aziendale

Date : 27 febbraio 2018

L’approccio statistico per sviluppare la Cyber Defence di nuova generazione

Darktrace segue un nuovo approccio per sfidare e neutralizzare i sofisticati attacchi provenienti sia dall’interno che dall’esterno di un’azienda impiegando avanzate tecniche di apprendimento automatico e algoritmi matematici.

Se guardiamo al medioevo, il concetto di città cinta da mura e posizionata sulla sommità di una collina era comune, per cui chi viveva dentro le mura era fidato, chi stava fuori non lo era. Questo modello era rassicurante ed ha funzionato bene finché il bisogno di espansione commerciale ha fatto si che individui ogni sorta hanno ad interagire fra di loro. La città moderna si fonda quindi sul turbinio dinamico di collaborazioni ed interazioni – che non richiedono presenza di mura.
Le città più moderne e floride nel mondo sono entità complesse che si sviluppano per chilometri.

La collaborazione e l’interazione fra le persone sono ovviamente fondamentali per il progresso e, abbiamo visto, anche nel campo della cyber security. Se vengono erette delle mura queste saranno spesso scavalcate e non solo da persone ostili ma anche dai dipendenti stessi che scelgono di eludere i controlli di sicurezza per espletare i loro compiti in modo efficiente. Nel valutare il rischio è fondamentale ricordare che i dipendenti non seguiranno sempre le linee guida impostate.

I dati non solo corrono il rischio di essere estratti illegalmente dall’azienda ma anche di essere alterati senza che nessuno se ne accorga. L’idea della perdita dei dati o del loro furto non è piacevole ma lo si resta sgomenti quando questo avviene. La sfida più difficile è capire quando l’integrità dei dati sia stata compromessa. Siamo tranquilli nel sapere che i nostri dati sono al sicuro, ma cosa succederebbe se in una banca il contenuto di 10.000 conti correnti venisse modificato e non sapessimo quali?

Un nuovo approccio attento a quelle attività ingannevoli che si manifestano in modo furtivo sarà il vincitore della battaglia contro gli attacchi informatici.
Questa tipo di battaglia è stata combattuta nel mondo biologico per milioni di anni. Il nostro DNA rappresenta l’informazione che è costantemente attaccata da svariati virus. Poiché non

possiamo vivere dentro una bolla di plastica per evitare questi attacchi virali siamo dotati di un sistema immunitario che sa come siamo fatti e quindi è in grado d'identificare ciò che per noi è anomalo ed estraneo. Gestire in questo modo ciò che non è prevedibile è cruciale per la nostra abilità, come esseri umani, a difenderci dalle minacce più gravi per la nostra salute mentre interagiamo e collaboriamo fra di noi. Darktrace aiuta le aziende a raggiungere questo equilibrio fornendogli un sistema immunitario capace di calcolare la probabilità delle minacce basandosi sui pezzi dell'evidenza. Basato su un collaudato approccio matematico e di apprendimento automatico esso consente alle aziende di restare vicino ai propri dipendenti ai fornitori ed ai clienti mentre le protegge da attacchi pericolosi e sofisticati. Questa tecnologia che auto apprende offre il primo pratico sistema per gestire la nuova realtà informatica quando non sempre siamo in grado di dire dove sia l'incendio da spegnere.

La minaccia è all'interno

Sebbene gli approcci tradizionali per la sicurezza distinguano fra interno ed esterno la realtà è che i confini siano virtualmente impossibili da definire all'interno delle infrastrutture aziendali moderne e che le minacce sono già presenti intorno alla rete.
Oggi i sistemi informativi aziendali e le reti sono globali, complessi e permeabili – e devono esserlo per consentirne il funzionamento e lo sviluppo nel mondo moderno. Comunque tutto ciò le rende vulnerabili agli attacchi.

Oggi tutte le aziende sono soggette ai rischi provenienti dall'interno, causati da gruppi di persone, i quali i propri dipendenti, i consulenti, i fornitori, i clienti oltre a gruppi ostili che hanno infiltrato l'azienda. I ripetuti attacchi di cui si ha notizia settimana dopo settimana, spesso sbattuti in prima pagina dai giornali, e che ledono la reputazione dell'azienda colpita sono la prova che i metodi tradizionali per gestire la sicurezza non funzionano.

Costruire un muro intorno ad un sistema che è già stato penetrato, e quindi intrinsecamente a rischio, non serve. Questo rallenta anche l'efficienza e la velocità con cui un'azienda moderna si pone sul mercato. Le aziende che applicano restrizioni sui loro dati corrono il rischio di veder danneggiate la competitività e la produttività e contemporaneamente sono estremamente vulnerabili sia alle minacce interne che ai sofisticati attacchi provenienti dall'esterno.

La vera sfida per la cyber security non è quella di proteggere i sistemi informativi – è quella di mettere in conto la probabilità che si verifichi un attacco e capire cosa stia effettivamente accadendo all'interno di questi sistemi. È illusorio credere che la presenza di un lucchetto e di una chiave ci pongano al sicuro. In realtà sappiamo che i lucchetti si forzano e le chiavi si duplicano - e per cui non esiste una soluzione perfetta. La soluzione migliore è quella che consente alle aziende di continuare ad esporsi ad ogni tipo di rischio nell'interesse della globalizzazione, della connettività e della competitività.

Presupposti errati: Perché l'approccio tradizionale sta fallendo

Sono tre le ragioni per cui il tradizionale approccio IT alla sicurezza abbia fallito con la cyber security.

1. Non si può lasciare fuori la minaccia.

L’approccio tradizionale, per la sicurezza, presuppone che gli attaccanti si possano restare fuori dalla rete rinforzandone il perimetro. Le aziende hanno investito tempo e denaro per i controlli perimetrali e per riconfigurare le reti con l’obiettivo di preservare dalle infiltrazioni i loro sistemi informativi.

Sfortunatamente la maggior parte delle reti aziendali, in qualche maniera, è già compromessa. Chi ci minaccia è oggi capace di superare i controlli perimetrali e a questi aggiungiamo pure i rischi che pongono gli impiegati e gli addetti ai lavori che accedono alla rete. Occorre partire dal presupposto che si è costantemente esposti ai rischi di attacco e che molti di questi, certamente quelli più insidiosi, riusciranno a penetrare in un’azienda con relativa facilità.

2. Non si può definire ciò che è illecito

Creare delle regole ed usarle per monitorare le informazioni è alla base degli approcci tradizionali in campo IT. Questo modo di operare è stato esteso a tutti i processi di tipo automatico e quindi anche al campo della cyber security. Infatti esistono diverse soluzioni che tentano di definire ciò che pare ‘cattivo’ in modo da proteggerci se e quando questo elemento ‘cattivo’ si dovesse ripresentare esattamente nello stesso modo. Mentre questo approccio potrebbe proteggere da degli attaccanti poco sofisticati, ossia che riutilizzano lo stesso metodo di attacco più volte, i professionisti in questo campo sono tecnicamente dotati, cambiano continuamente le strategie di attacco ed impiegano strumenti appositamente sviluppati per portare a termine la loro missione.

Inoltre, affinché l’approccio basato su regole funzioni in maniera accurata sono richiesti continui aggiornamenti delle stesse e, inevitabilmente, si fa fatica a stare dietro alle continue evoluzioni delle metodologie di attacco. Questo è un approccio di tipo reattivo che è incapace di difenderci da attacchi nuovi e sempre diversi mentre sono in corso.

3. La minaccia non è puramente tecnica

Spesso ci si dimentica dell’essere umano che sta dietro ad ogni attacco informatico quando si parla di botnet, Trojan e RAT. Occorre ricordarsi che le minacce serie sono perpetrate da gente esperta che si muove in modo abile e silenzioso sulla rete. Il classico approccio detto ‘bianco e nero’ descritto in precedenza non è in grado di affrontare le complesse e delicate strategie messe in campo da questi attaccanti.

Chi agisce dall’interno o dall’esterno presenta normalmente delle peculiarità o lascia delle tracce prima di entrare in azione. Un consulente che si collega alla rete in orari strani della giornata, il raggruppamento di più file, la creazione di un nuovo account utente od il volume di email attraverso un server specifico – questi sono tutti segnali che da soli spesso non hanno senso ma una volta aggregati offrono una visione chiara di quello che sta accadendo.

Oltre alla natura umana di chi pianifica l’attacco dovremmo ricordarci delle vulnerabilità ‘naturali’ delle persone interne all’azienda che vengono spesso usate e sfruttate dagli

attaccanti. Gli attacchi che sfruttano tecniche di social-engineering sono in crescita e hanno lo scopo d'ingannare e spingere i dipendenti ad eseguire determinate azioni. Sebbene l'addestramento e la formazione degli stessi possa aiutare nel ridurre questi rischi è impossibile far si che tutti i dipendenti smettano di prendere decisioni sbagliate ogni volta.

La sfida degli esperti della cyber ed IT Security è quella di sfruttare l'approccio probabilistico per notare le sfumature dei comportamenti umani. Questo vuol dire essere capaci di rilevare e d'interpretare quegli indicatori deboli che indicano azioni ed attività umane all'interno della rete in modo tale da rilevare l'emergere di comportamenti minacciosi portati avanti astutamente da chi si nasconde dietro ad un potenziale attacco.

La protezione dei dati non vuole dire limitarsi solo alla perdita dei dati

La natura del rischio è cambiata, è cosi ampia che include tutti i modi per procurare dei danni. La preoccupazione principale è per la perdita dei dati, vista la proliferazione di individui o gruppi di persone che vogliono impossessarsene per il loro valore finanziario (come i dati delle carte di credito), il loro valore economico (come i disegni industriali) o il valore politico (come i documenti di un governo).

È un fenomeno preoccupante, ma forse ancora più importante è che i sistemi informatici odierni consentano la modifica dei dati senza che nessuno se ne accorga. Sia che si agisca dall'interno o dall'esterno di una rete una volta dentro accedere ai dati e poterli alterare in tutto o in parte è di difficile individuazione. Con un piccolo sforzo doloso si possono causare problemi veramente seri. Immaginate lo scenario in cui anche il back-up sia corrotto.

La garanzia dell'integrità dei dati è fondamentale per le molte aziende che operano in un mercato libero. Per un'azienda sanitaria che gestisce i gruppi sanguigni dei propri pazienti o una banca che gestisce i saldi dei propri clienti la prospettiva che questi dati critici possano essere compromessi in qualche modo può portare ad un danno d'immagine tale da far cessare queste attività.

Quando pensiamo a come risolvere il problema degli attacchi informatici dobbiamo guardare oltre ai casi isolati di perdita dei dati o di attacchi a siti web e considerare invece le maggiori implicazioni che un attacco ad una grande organizzazione comporta con la perdita di credibilità della stessa. Edward Snowden ha dimostrato che anche le aziende meglio protette e quelle più attente alla sicurezza sono vulnerabili a fronte di attacchi portati avanti con astuzia da 'lupi solitari' che si muovono invisibili nei loro sistemi ed hanno le potenzialità di minarne completamente le capacità operative.

Minacce dall'interno

I pericoli che possono pervenire da persone interne all'azienda sono molto sottostimati, forse perché è un problema molto difficile da risolvere. Dobbiamo dare fiducia ai nostri dipendenti e partner commerciali consentendogli l'accessi ai dati che gli consentano di fare il loro lavoro, allo stesso tempo non possiamo contare sul fatto che tutti si comportino sempre allo stesso

modo. Alcuni possono essere vittime di attacchi di tipo phishing e involontariamente lasciare entrare qualcuno; altri possono avere del risentimento o degli altri motivi che li portano ad usare le credenziali di cui sono in possesso con intenti malevoli.

I pericoli provenienti dall'interno non sono imputabili solo ai nostri impiegati ma a chiunque abbia accesso alla rete, ai dati aziendali o agli uffici. Questo rende la gestione del tutto molto complessa. Le aziende moderne prosperano grazie all'interconnessione con altre realtà, i fornitori, i clienti, i consulenti, altre consociate e individui. Le aziende hanno espanso le loro reti e conseguentemente si sono aperte a rischi maggiori pur di poter essere efficienti e competitive sul mercato.

I motivi che spingono qualcuno ad agire dall'interno sono molteplici, sia involontariamente che deliberatamente, il guadagno, un'ideologia, il desiderio di essere legittimati, dedizione alla famiglia o agli amici o una disaffezione generale. Con una così vasta gamma di personalità e motivazioni che spingono ad agire è impossibile identificare in anticipo quegli utenti che possono rappresentare una minaccia.

Piuttosto che discutere su 'chi è stato' o cercare di indovinare 'chi lo farà' la vera sfida consiste nell'individuare questi attacchi e capire come si sviluppano in tempo reale analizzando e correlando deboli segnali di compromissione che ognuno di questi personaggi genera muovendosi dentro la rete. Incidenti di questo tipo non devono essere dello stesso livello di quelli causati da Edward Snowden o Bradley Manning per danneggiare la reputazione della vostra azienda o del vostro lavoro. Nonostante la sicurezza interna nella maggior parte delle aziende sia migliorata sappiamo che gli attacchi dall'interno sono sempre possibili pur impiegando strumenti di sicurezza dedicati e solidi regolamenti interni. Ovviamente poiché i confini di una rete diventano sempre più labili la distinzione tra chi è dentro e chi è fuori non ha più molto senso. In un modo o nell'altro gli attacchi odierni che hanno successo avvengono dietro ai firewall.
Dobbiamo imparare ad interpretare i comportamenti degli utenti, dei dispositivi e delle reti per identificare i veri avversari in un mondo in cui ognuno è o può diventare una minaccia interna.

Introduciamo il Sistema Immunitario Aziendale

Darktrace è stata la prima ad usare un approccio completamente nuovo per affrontare le minacce informatiche, noto come Sistema Immunitario Aziendale (o The Enterprise Immune System), partendo dal presupposto che le aziende siano costantemente minacciate dall'interno. Questa categoria emergente rappresenta una tecnologia all'avanguardia in grado di 'conoscere' l'azienda in modo adattativo, in tempo reale e quindi in grado di capire quando un comportamento anomalo inizia a palesarsi.

Così come il DNA dei virus, che muta ed evolve costantemente nel corpo umano per sopravvivere, gli attaccanti informatici cambiano e adattano il loro comportamento per evitare di essere scoperti. Fortunatamente per noi il sistema immunitario è altrettanto intelligente come il DNA dei virus – impara e capisce in modo continuo ciò che costituisce una minaccia. Non è un sistema perfetto – a volte prendiamo un raffreddore – ma generalmente ci protegge molto bene da malattie gravi. Questo consente agli esseri umani di interagire fra di loro esponendosi

quotidianamente a molteplici rischi. Gli esseri umani crescono interagendo socialmente e collaborando fra di loro e vivere in una provetta sterile non ha senso e, a maggior ragione, non ce l'ha nemmeno per un'azienda moderna.

L'innovativo approccio di Darktrace si fonda su una complessa base matematica che calcola la probabilità che si verifichi un evento alla luce di ciò che si è rilevato in precedenza. Questo metodo probabilistico per evidenziare anomalie è pragmatico ed accurato ai fini di una protezione da vettori d'attacco sconosciuti che operano all'interno di reti informatiche complesse.
Il Sistema Immunitario Aziendale desume in modo iterativo modelli di vita di ogni rete, dispositivo ed utente, correlando poi queste informazioni in modo tale da avere una visione globale dello stato 'normale' della rete aziendale e poter quindi individuare quelle deviazioni dalla 'normalità' che rivelano una minaccia in corso.

Questo nuovo approccio non richiede una conoscenza a priori delle minacce esistenti dato che va a ricercare quei comportamenti che probabilisticamente sono considerati anomali e quindi meritevoli di approfondita indagine. Un Sistema Immunitario Aziendale offre per la prima volta alle aziende la possibilità di trovarsi un passo avanti alle minacce consentendogli di correggere le attività sospette individuate prima che facciano danni più significativi. Consente inoltre agli analisti di sicurezza di concentrarsi solamente sugli incidenti veramente significativi che possano mettere a repentaglio la sicurezza della rete senza perdere tempo ad inseguire molteplici falsi allarmi.

La capacità del Sistema Immunitario Aziendale di auto apprendere e adattarsi a condizioni che cambiano in tempo reale costituisce un passo importante per le aziende di tutto il mondo e gli consente di conciliare la necessità di avere i dipendenti, i clienti ed i fornitori interconnessi e al contempo garantirsi la protezione da minacce concrete e pericolose per le proprie attività nel modo più efficiente possibile.

La Matematica ed il Machine Learning fatti bene

Il cuore del rivoluzionario approccio di Darktrace si basa su importanti passi avanti fatti dalla matematica probabilistica all'Università di Cambridge. La teoria Baiesiana è nota per la sua capacità di dare un senso a grandi quantità di dati e un nuovo ramo della matematica, chiamato Recursive Bayesian Estimation (RBE), è il perno fondante dell'innovativa tecnologia Darktrace.

Descrivendo matematicamente la 'normalità' di un comportamento effettuato analizzando diverse tipologie di dati, la RBE riesce ad identificare i comportamenti che cambiano durante un attacco quando i tradizionali metodi basati su signature falliscono. Utilizzando la RBE i modelli matematici di Darktrace si modificano costantemente e in tempo reale sulla base di nuove informazioni che vengono analizzate calcolandone continuamente i livelli di pericolo.

Darktrace utilizza anche il metodo Sequential Monte Carlo per calcolare la distribuzione della probabilità dello stato di una rete. La distribuzione viene costruita analizzando un insieme complesso di valori o 'caratteristiche' dei dati generati da dispositivi, dalla rete e dal traffico stesso. Questi valori vengono raccolti in modo iterativo ed elaborati in tempo reale sulla

piattaforma. Un modo accettabile di rappresentare le informazioni relazionali fra le entità di sistemi dinamici in genere, quali una rete aziendale, una cellula vivente, una comunità sociale o anche internet stessa è quello di usare una rete stocastica, che varia nel tempo in modo casuale e con certe caratteristiche.

Nei problemi multi dimensionali, quali l'osservazione del traffico di pacchetti e l'attività dei dispositivi di una WAN o LAN aziendale, dove sia l'input che l'output possono contenere decine di migliaia e a volte anche milioni di valori interconnessi, la capacità di apprendere di una struttura funzionale distribuita e coerente è ostacolata dalla mancanza di una architettura normalizzata.

In questo contesto Darktrace è pioniera del più avanzato sistema di calcolo su larga scala per definire una funzione strutturale, in ambito networking, estendendo il modello di regressione lineare regolare L1 (metodo LASSO) alla famiglia di modelli di regressione 'strutturati'. Questo consente di scoprire le reali associazioni tra il malware trovato, eventi in input e l'output che possono essere efficacemente risolti impiegando modelli ottimizzati.

Per la tecnologia Sistema Immunitario Aziendale sono richieste metodologie ingegnose atte a valutare ed analizzare modelli i cui elementi variano in presenza di modifiche strutturali che si presentano in tempi e luoghi non prevedibili. Esempi di questi modelli s'incontrano frequentemente nei problemi in ambito sociale e biologico dove i dati sono strutturati e progressivi e i presupposti sulle variabili indipendenti ed identicamente distribuite di campioni generati con un modello invariante non sono più validi.

Ad esempio se in un dato istante le osservazioni (come un'istantanea dello stato sociale di tutti gli attori) vengono distribuite sulla base di un modello (come una rete) specifico per quell'istante, queste non possono essere usate direttamente per effettuare delle stime su modelli che si riferiscono a momenti diversi.

Darktrace è stata la prima ad usare i metodi bayesiani per il monitoraggio dei modelli che cambiano strutture e parametri, aggregando questi dati, il momento in cui avvengono ed eventuali altre incognite. Questo approccio metodologico è essenziale per analizzare le anomalie comportamentali, altrimenti invisibili, di un dispositivo e che ne indicano il compromesso.

Questo nuovo approccio matematico consente a Darktrace di desumere e verificare legami casuali fra variabili, osservazioni e insiemi di caratteristiche. La causalità di Granger, ossia la causalità basata sulla predizione, i principi bayesiani applicati alle reti e i nuovi studi sulla relazione causa ed effetto fra variabili in istanti diversi, detto Convergent Cross Mapping, consentono di elaborare con un alto grado di confidenza i legami casuali senza il bisogno di ripetute e continue osservazioni.

I fondamenti matematici di Darktrace consentono di determinare la normalità di un comportamento utilizzando i metodi descritti in precedenza quali il metodo del pivot applicato alla RBE, il metodo Monte Carlo Sequenziale. La combinazione di questi metodi consente d'individuare una probabile sequenza di compromissione.

Conclusione

In un’epoca di constanti minacce interne è necessario un nuovo approccio che non distingua semplicemente tra ‘interno’ ed ‘esterno’ ma che sia anche capace di capire cosa stia accadendo all’interno di un’azienda per gestire l’evento inatteso.

Le aziende oggi non vanno considerate come delle città fortificate – gli scambi e la collaborazione fra confini geografici e virtuali sono vitali per la loro sopravvivenza. Il nuovo modello di sicurezza deve consentire ed incoraggiare l’apertura degli scambi con la consapevolezza che il pericolo è già presente e che la battaglia contro di esso è continua.

Il Sistema Immunitario Aziendale consente alle aziende di riconoscere il pericolo in modo olistico e di difendersi con l’uso di tecniche di apprendimento automatico e progressi in ambito matematico. Il sistema apprende su base continua e questo lo rende in grado di gestire l’imprevedibilità di attacchi sofisticati adattandosi sia ai cambiamenti interni all’azienda che al panorama delle minacce.

Le aziende che hanno investito nel Sistema Immunitario Aziendale inserendolo nella loro infrastruttura di rete stanno beneficiando di una tecnologia all’avanguardia nel campo dell’apprendimento automatico e della matematica per proteggersi dalle minacce insidiose e persistenti che provengono dall’interno delle loro reti consentendogli di mantenere la flessibilità e l’interconnettività oggi necessarie. Il Sistema Immunitario Aziendale è il cuore di questo nuovo approccio che si adatta alla complessità dei nostri sistemi e delle minacce in essi presenti. La possibilità di prendere un raffreddore rientra nel calcolo delle probabilità ma è un prezzo che vale la pena pagare.