IL NUOVO SOC EXPRIVIA: TRA TECNOLOGIA E TERRITORIO

02/09/21 - In questo periodo parlare di Cyber security è sempre più comune, anche se non sempre se ne parla con cognizione di causa.

Questa volta abbiamo pensato di parlarne con Domenico Raguseo, nella sua veste di direttore del nuovo *Security Operation Center* (SOC) di Molfetta.

Che cos'è un SOC? Perché avete aperto un SOC, e poi, perché in Puglia?

Un SOC è un centro per l'erogazione di servizi di sicurezza. In un SOC ci si occupa del monitoraggio degli eventi di sicurezza sette giorni su sette e H24, gestione delle infrastrutture, segmentazione e micro-segmentazione, gestione e governo identità, identità privilegiate ed accessi, e così via. I SOC moderni comprendono anche servizi proattivi, come programmi di training e awareness, penetration testing e vulnerabily assessment (VAPT) e il nostro Centro è provvisto anche di un "Computer Security Incident Response Team" (CSIRT). Infatti, anche se la miglior difesa è la prevenzione, in caso di attacco mettere a disposizione in tempi breve personale altamente specializzato fa la differenza tra una tragedia e un danno marginale.

In generale i SOC sono focalizzati sul perimetro IT, nel nostro caso invece ci occupiamo anche di IoT e sistemi industriali, SCADA e PLC questo perchè molti dei nostri clienti appartengono al mondo industriale e il futuro della cybersecurity è nell'IoT.

Non a caso, uno degli use case che utilizziamo maggiormente è relativo alla cyber security dei sistemi di videosorveglianza. Come ci insegna il caso Mirai, infatti, bisognerebbe controllare che i dispositivi IoT non vengano usati come basi per ulteriori attacchi o movimenti laterali.

Il nostro SOC è anche utilizzato come test bed, ovvero è impiegato per testare e mostrare ai clienti le tecnologie da noi prodotte e utilizzate, oltre a use case particolari (ad esempio MIRAI).

Exprivia crede fermamente nel valore della condivisione, per cui raccoglie, analizza e poi rende disponibili i dati pubblici relativi ad attacchi, incidenti e violazioni della privacy redigendo ogni tre mesi un Rapporto sulle minacce informatiche in Italia.

Noi abbiamo un particolare interesse per digitalizzazione e innovazione. Quanto può essere importante il Machine Learning (ML) nell'ambito della AI in relazione alla cyber threat intelligence?

Cercherò di semplificare la risposta. Tutti sappiamo che il termine hacker è usato per individuare una persona che grazie alle sue competenze è capace di migliorare la resilienza di un sistema digitale o di correggerne delle vulnerabilità attraverso specifiche attività. L'hacker cattivo, viceversa, è colui il quale cerca di sfruttare a suo vantaggio le vulnerabilità dei sistemi digitali.

Ora, se gli attaccanti usano il ML anche i buoni devono usare il ML. Le possibili applicazioni sono tante. Ad esempio il ML è usato per identificare pattern di attacco o prevenire un incidente. Gli attacchi possono essere portati avanti per mesi o anni ed è dunque importante essere in grado di identificare un Indicatore di Compromissione (IOC) grazie alla

EVENTI

SETTEMBRE 2021

Lu	Ma	Me	Gi	Ve	Sa	Do
30	31	1	2	3	4	5

Il nuovo SOC Exprivia: tra tecnologia e territorio

Il nuovo SOC Exprivia: tra tecnologia e territorio - Difesa OnlineIl nuovo SOC Exprivia: tra tecnologia e territorio
02/09/21
In questo periodo parlare di Cyber security è sempre più comune, anche se non sempre se ne parla con cognizione di causa.
Questa volta abbiamo pensato di parlarne con Domenico Raguseo, nella sua veste di direttore del nuovo Security Operation Center (SOC) di Molfetta.
Che cos'è un SOC? Perché avete aperto un SOC, e poi, perché in Puglia?
Un SOC è un centro per l'erogazione di servizi di sicurezza. In un SOC ci si occupa del monitoraggio degli eventi di sicurezza sette giorni su sette e H24, gestione delle infrastrutture, segmentazione e micro-segmentazione, gestione e governo identità, identità privilegiate ed accessi, e così via. I SOC moderni comprendono anche servizi proattivi, come programmi di training e awareness, penetration testing e vulnerabily assessment (VAPT) e il nostro Centro è provvisto anche di un "Computer Security Incident Response Team" (CSIRT). Infatti, anche se la miglior difesa è la prevenzione, in caso di attacco mettere a disposizione in tempi breve personale altamente specializzato fa la differenza tra una tragedia e un danno marginale.
In generale i SOC sono focalizzati sul perimetro IT, nel nostro caso invece ci occupiamo anche di IoT e sistemi industriali, SCADA e PLC questo perchè molti dei nostri clienti appartengono al mondo industriale e il futuro della cybersecurity è nell'IoT.
Non a caso, uno degli use case che utilizziamo maggiormente è relativo alla cyber security dei sistemi di videosorveglianza. Come ci insegna il caso Mirai, infatti, bisognerebbe controllare che i dispositivi IoT non vengano usati come basi per ulteriori attacchi o movimenti laterali.
Il nostro SOC è anche utilizzato come test bed, ovvero è impiegato per testare e mostrare ai clienti le tecnologie da noi prodotte e utilizzate, oltre a use case particolari (ad esempio MIRAI).
Exprivia crede fermamente nel valore della condivisione, per cui raccoglie, analizza e poi rende disponibili i dati pubblici relativi ad attacchi, incidenti e violazioni della privacy redigendo ogni tre mesi un Rapporto sulle minacce informatiche in Italia.
Noi abbiamo un particolare interesse per digitalizzazione e innovazione. Quanto può essere importante il Machine Learning (ML) nell'ambito della AI in relazione alla cyber threat intelligence?
Cercherò di semplificare la risposta. Tutti sappiamo che il termine hacker è usato per individuare una persona che grazie alle sue competenze è capace di migliorare la resilienza di un sistema digitale o di correggerne delle vulnerabilità attraverso specifiche attività. L'hacker cattivo, viceversa, è colui il quale cerca di sfruttare a suo vantaggio le vulnerabilità dei sistemi digitali.
Ora, se gli attaccanti usano il ML anche i buoni devono usare il ML. Le possibili applicazioni sono tante. Ad esempio il ML è usato per identificare pattern di attacco o

prevenire un incidente. Gli attacchi possono essere portati avanti per mesi o anni ed è dunque importante essere in grado di identificare un Indicatore di Compromissione (IOC) grazie alla analisi in tempi brevi di enormi quantitativi di dati.

Un campo di impiego è quello della Anomaly Detection. Gli attaccanti usano spesso metodologie differenti, per cui riconoscere gli IOC è sempre più complicato. È più semplice individuare, grazie al ML un comportamento "normale" e cogliere, di conseguenza, i comportamenti anomali.

Capire quale traffico è normale e quale no è uno degli impieghi più comuni del Machine Learning.

Nella Operational Technology (OT) e nell'Internet of Things (IoT) è molto comune ricorrere alla tecnologia dell'Anomaly Detection basata sull' analisi comportamentale (UBA - User Behaviour Analitics).

Anche nel Vulnerability Assessment e Penetration Testing è possibile usare l'Artificial Intelligence: per esempio ci sono dei tool che insegnano ad utilizzare tecniche di SQL Injection, usate per attaccare applicazioni che gestiscono dati attraverso database relazionali sfruttando il linguaggio SQL.

Inoltre esistono strumenti di ML che sono in grado di individuare le vulnerabilità più probabili da sfruttare a seconda del software.

Non dobbiamo però dimenticarci della cyber security dei sistemi di Intelligenza Artificiale: in questo caso si parla di Adversarial Artificial Intelligence. Infatti, se i sistemi di AI sono alimentati da dati errati non possiamo essere sicuri che la AI si comporti come noi vogliamo.

Ci puoi spiegare l'impiego delle reti di videocamere o di altri oggetti per fare determinati tipi di attacchi, tipo Mirai?

Parliamo un attimo di IoT e poi arriviamo a Mirai. Il mercato affronta il tema di IoT pensando al dispositivo che viene compromesso. Se ho una rete di telecamere, ad esempio, penso che il servizio reso possa essere compromesso. In verità questo è solo un aspetto del problema.

Esistono dispositivi di tutti i tipi in rete, dalle videocamere agli orologi, dalle lavatrici, ai frigoriferi compreso lo smart clothing (abbigliamento intelligente). Questo significa che tantissimi oggetti sono impiegati potenzialmente per condurre attacchi non diretti al servizio reso dagli oggetti stessi. Esistono inoltre strumenti che aiutano a reperire le informazioni sugli oggetti in rete senza eccessivi costi e ciò agevola gli attaccanti.

Un esempio sono le telecamere di videosorveglianza. L'attacco Mirai usa le telecamere compromesse (che nel frattempo continuano a funzionare correttamente) ma è diretto ad altri servizi non collegati al funzionamento delle videocamere. Le bot installate sulle videocamere sono usate per fare altro, senza che ci si accorga del danno reale. Il problema dell'IoT è che vi sono migliaia di oggetti con bassissima sicurezza che, per esempio nel caso di Mirai, possono essere usati per fare un attacco di Distributed Denial Of Service (DDOS) verso obiettivi diversi.

È sicuramente vero che esistono pericoli e rischi cyber legati al nostro modello di società, ma è anche vero che spesso questi sono usati come scusante.

Mi capita spesso di parlare di cyber security con persone di tutti i tipi.

A volte capita che si commettano degli errori, altre volte ci si trova davanti qualcuno più bravo. A volte la differenza tra le due situazioni è molto lieve e quindi è meglio aspettare e capire.

Quando si parla di sicurezza dell'IoT invece, occorre affrontare due macro aree.
La prima è la governance dell'IoT. Spesso il problema di sicurezza dipende dalla cattiva divisione delle responsabilità all'interno dell'organizzazione. Assumersi la responsabilità della sicurezza delle telecamere, per esempio, è un costo; dunque qualcuno deve non solo prendersi la responsabilità ma anche assumersi l'onere del costo. Non si fa sicurezza a costo zero.
Il secondo punto riguarda il mercato. Se si vendono al consumatore generico dispositivi come frigoriferi connessi a Internet, non si può pretendere che l'utente capisca qualcosa di cyber. L'azienda produttrice dovrebbe farsi carico della sicurezza e della certificazione di questi prodotti. Ciò, molto probabilmente, aumenterà i costi del prodotto ma credo non se ne possa fare più a meno.
Un altro tema al quale teniamo tantissimo è legato alla ricerca e alla formazione. Quali sono le relazioni tra il vostro SOC e le Università, scuole e centri di ricerca?
Il nostro SOC è stato aperto nell'head quarterdi Exprivia, a Molfetta, ma il nostro personale è distribuito in tutto il mondo. Avere la possibilità di collaborare con le Università, sia per le attività di ricerca. sia nella selezione dei talenti , è una delle nostre priorità.
L'industria ha sempre il triste problema di essere sotto la minaccia del ritorno di investimento, per cui considerando che gli attaccanti investono in ricerca e sviluppo, anche noi dobbiamo farlo.
Con le Università partecipiamo anche a diversi progetti, tra questi ECHO, un progetto dell'Unione Europea che punta ad accrescere la capacità di cyber resilience dei Paesi aderenti. Tutto ciò ci aiuta a ridurre il gap tra attaccanti e difensori.
Exprivia ha anche avviato una Academy che ci consente da un lato di ricollocare personale con nuove competenze utili per restare sul mercato del lavoro, e dall'altro a formare nuovo personale.
Con l'introduzione dell'Intelligenza Artificiale i tempi per l'attacco e la individuazione di una strategia di difesa si fanno sempre più brevi. Come è possibile impiegare l'AI per difendersi?
L'AI viene utilizzata principalmente per identificare un attacco e suggerire le mosse migliori per rispondere. L'AI può aiutare ma oggi tutto dipende anche dalla tecnologia impiegata nei sistemi, dalle persone e dalla loro preparazione e da tanti altri elementi.
In generale però dobbiamo parlare di incidente e non di attacco.
Quando vi è un incidente, dopo una prima analisi si riesce già a capire se è in corso un attacco e l'AI può aiutare sia nell'analisi che nell'elaborazione di contromisure adeguate nei tempi più rapidi.
Bisogna ricordarsi però che, in generale, non esiste un tipo di difesa valido sempre e per ogni tipo di attacco, per cui non si deve commettere l'errore di pensare che l'AI sia la soluzione a tutti i tipi di attacco. Fortunatamente però, esistono strumenti che impiegano l' Intelligenza Artificiale con modalità differenti.
In generale la cyber security è molto complessa e dipende da tanti fattori; l'Intelligenza Artificiale può aiutare, ma anche dimostrarsi inutile o pericolosa. Molto dipende ancora dalla capacità delle persone.
Quali sono le nuove soluzioni in ambito cyber security?
Oggi si parla tanto di micro-segmentazione, una tecnologia molto utile grazie alla quale due utenti possono colloquiare solo su specifici canali, su particolari servizi o su particolari argomenti, non su tutto.

Anche passare al Cloud è uno dei temi ancora molto discussi, ma spesso poco compresi; il Cloud può certamente aiutare nel migliorare la sicurezza, ma l'importante è che venga usato correttamente.

Domenico, hai fatto una bella panoramica sul SOC e sulle tecnologie impiegabili, ma abbiamo ancora una curiosità, per cui, per chiudere torniamo alla prima domanda: perchè in Puglia?

Exprivia, società fondata dal suo attuale presidente Domenico Favuzzi, quotata in borsa e con circa 2400 dipendenti, ha la sua sede principale in Puglia.

Dunque la cosa più ragionevole ci è sembrata quella di aprire il SOC in questa regione anche per contribuire allo sviluppo del territorio. È chiaro che noi forniamo servizi ovunque, in Italia e all'estero; moltissimo personale è pugliese, ma i professionisti che lavorano con noi provengono da diverse regioni, lavorando anche da remoto e non presso clienti italiani ed esteri.

Alessandro Rugolo, Maurizio D'Amato, Simone Domini

Per approfondire:

- Exprivia - Future. Perfect. Simple

- Exprivia Threat Intelligence Report 2Q 2021

- Cyber security: cos'è un SOC? - Difesa Online

- ECHO Network

- What is SCADA System ? - Basics of SCADA - InstrumentationTools

- What is PLC ? Programmable Logic Controller - Unitronics (unitronicsplc.com)