Var Group Digital Security: Detection e remediation per mitigare eventi malevoli

di Diego Marson - Chief Security Officer, Var Group Digital Security

Ci può parlare di Yarix e di Var Group?
Yarix è la società a capo della divisione **Digital Security** di **Var Group** ed è una delle aziende italiane più riconosciute, innovative e autorevoli nel comparto della sicurezza informatica: da oltre 20 anni fornisce servizi e soluzioni di cyber security, business continuity e disaster recovery a industrie, enti governativi e militari, aziende del comparto sanitario e università.
Fondata nel 2001, Yarix è oggi tra i più importanti player sul territorio nazionale. Dispone di un Cognitive Security Operation Center tra i più evoluti in Italia e si avvale di team specializzati in defensive e offensive security, cyber threat Intelligence, incident response.
Il 2014 ha visto l'avvio di una strategia di crescita finalizzata alla creazione di un polo di eccellenza per la gestione globale della sicurezza delle imprese. Attraverso un processo di acquisizioni che ha portato all'integrazione di realtà col maggiore potenziale e le competenze più evolute in Italia, Var Group e Yarix offrono alle aziende italiane – che affrontano le sfide dell'innovazione tecnologica e della trasformazione digitale – un nuovo livello di protezione.

Var Group S.p.A.,con un fatturato di 572 milioni di euro al 30 aprile 2022, oltre 3400 collaboratori, presente in Italia con una copertura capillare, e in 9 paesi all'estero (Francia, Germania, Spagna, Romania, Austria, Svizzera, Cina, Messico, Tunisia), è uno dei principali partner per la trasformazione digitale delle imprese.
L'offerta Var Group trae la propria forza dalla profonda conoscenza dei processi aziendali e dall'approccio consulenziale. È frutto del lavoro di Business Unit focalizzate nello sviluppo di progetti di: Customer & Business Experience, Digital Process Engineering, Digital Industries, Digital Cloud, Smart Services, Data Science, Digital Technologies e Digital Security.

Fondata nel 2012 e parte di **Var Group Digital Security** dal 2022, **NGS** è una società di consulenza specializzata in sicurezza informatica ed edge security. Offre soluzioni specifiche per la protezione di aziende enterprise nazionali ed internazionali, operanti nei settori manifatturiero e marittimo, differenziandosi per la capacità di mettere in relazione elevate competenze e tecnologie, sfruttando al meglio le potenzialità dei prodotti per integrarli in progetti ad altissima customizzazione.

Qual è l'attuale scenario della cybersecurity, dal vostro punto di osservazione?
Con il panorama delle minacce informatiche in continua evoluzione ed espansione diventa essenziale capire come queste possano impattare qualsiasi tipologia di organizzazione.
Negli ultimi sei mesi abbiamo assistito a un'impennata nella frequenza e nella complessità degli attacchi, nonché all'utilizzo di nuove tattiche da parte dei Threat Actor;

parallelamente si è ridotto sempre più il tempo che intercorre tra la pubblicazione di una vulnerabilità e il suo attivo sfruttamento da parte di questi gruppi criminali.
Il processo di security in ambienti OT, per quanto presenti delle peculiarità uniche rispetto agli ambienti IT nei quali siamo più soliti vedere calato un processo di questo tipo, presenta diversi aspetti sovrapponibili a quelli trattati in un classico ambiente IT.
Riteniamo che la tematica della corretta definizione dell'infrastruttura di rete, complessa perché include i temi del dimensionamento, delle opportune ridondanze, le corrette segmentazioni e la definizione di policy strutturate per le comunicazioni, non debba essere appannaggio degli ambienti IT classici, ma che la definizione di tutti questi aspetti necessiti di essere gestita in modo organico come un unico insieme.
Allo stesso modo, il processo di security in ambiente OT non può prescindere dagli aspetti storicamente più legati alla cybersecurity quali, ad esempio, la consapevolezza delle minacce esistenti, nate fuori dal proprio perimetro e sfruttate attivamente dai gruppi TA; la conoscenza di eventuali sistemi vulnerabili nella propria infrastruttura e i metodi di mitigazione che si possono intraprendere; la possibilità di identificare possibili azioni malevole impattanti sui sistemi industriali e le modalità per gestirli 24/7 in modo automatico o, dove non realizzabile, mediante opportune segnalazioni in tempo reale ai responsabili di linea.
Questo perché, senza una visibilità completa e in tempo reale delle reti, dei dispositivi e dello stato dei processi di un sistema di controllo industriale (ICS), proteggere le reti di controllo dagli attacchi informatici ed evitare interruzioni operative è una sfida impari.

La possibilità offerta da un sistema come **Nozomi Networks** di integrarsi con sistemi come i Next-Generation Firewall (NGFW) di Palo Alto Networks consente di rispondere in modo efficace a queste minacce.
Grazie alle API messe a disposizione da Palo Alto Networks e la Nozomi Networks Open, è possibile far lavorare di concerto le due soluzioni per estendere le azioni di rilevamento, prevenzione e correzione delle minacce in modo molto più rapido rispetto a quanto possibile in precedenza.

Quale sarà il vostro contributo al convegno del 28 settembre *IoT/OT & Asset Governance: Sicurezza, Continuità Operativa, Monitoraggio e Compliance*?
Nel nostro intervento ci soffermeremo proprio sull'ultimo aspetto prima citato, ovvero la **detection** e le **remediation** a fronte di un evento da parte di un attore malevolo.
Per farlo, ci serviremo di un ambiente di simulazione, preparato per ricalcare due differenti impianti produttivi: un impianto di imbottigliamento ed una raffineria petrolifera, al fine di evidenziare il comportamento degli stessi a fronte di azioni malevole.
Nel primo scenario illustreremo degli ambienti nei quali non sono presenti sistemi di riconoscimento - e risposta - ad eventi malevoli, dando evidenza di come queste azioni portino alla compromissione dell'operatività e possano compromettere, a causa di aspetti di security non correttamente trattati, la safety sia dell'impianto che degli operatori.
La tecnologia presente nella simulazione è costituita dalla parte Threat and Anomaly Detection di Nozomi Network e da Firewall Palo Alto.

VARGROUP