Il seminario: rapporto di sintesi

a cura di Gen. D.A. (r), Salvatore Gagliano

Il seminario pomeridiano della Conferenza, destinato alle aziende della cybersecurity, è stato aperto dal CEO di Fata informatica, Antonio Capobianco, che ha presentato la società che egli stesso fondò da giovane neolaureato in informatica nel 1994. L'azienda offre System Integration Software, attività di Development Training and Certification.

Sì è specificamente distinta per studi su *risk assessment and risk evaluation.*

In particolare, il *discussant* ha presentato uno strumento di calcolo del rischio informatico, basato sul metodo *Frequency*, il quale mette in relazione il vettore base, la maturità della minaccia e la frequenza dell'attacco; ciò determina il *frequency score* che unito al *temporal score* permette la individuazione del rischio.

Lo strumento integra, secondo un approccio ampiamente sistemico, il prodotto di punta di Fata Informatica, il *Sentinet3*, recentemente inserito dal *Gartner's Market Guide* tra i migliori prodotti nell'ambito dei *security analyzer.*

L'ingegner Capobianco ha invitato poi in chiusura a porre massima attenzione all'elemento umano e alla sua continua formazione, quale fondamentale strumento di solida sicurezza aziendale e sistemica. La *cyber situation awareness* del personale va continuamente stimolata, attraverso corsi interni di *security awareness*. Essi infatti assicurano il continuo coinvolgimento del personale, un basso impatto operativo, ampia accessibilità e semplicità anche attraverso tecniche di *gaming*.

Il dottor Marco Conflitti, *Head of Cybersecurity Central and Eastern Europe* di ATOS Italia, ha presentato il suo gruppo, leader globale nella *digital transformation* con oltre 110.000 dipendenti in 73 paesi e un fatturato annuo di 11 miliardi di euro.

In particolare, ATOS offre soluzioni end-to-end per Orchestrated Hybrid Cloud, Big Data, Business Applications e Digital Workplace.

Il *discussant* ha voluto preliminarmente rilevare che oggi le aziende hanno dinamicamente aggiornato il proprio *modus operandi* non più concentrandosi su di uno specifico prodotto bensì valutando globalmente rischi cui il *customer* è esposto, proponendo opportune soluzioni di sistema. Solamente in tal modo, supportando istituzioni, cittadini e imprese sarà possibile un armonico sviluppo digitale dell'Italia, contribuendo a progettare l' *information technology* del futuro.

Tuttavia la *compliance* ai quadri normativi di riferimento in termini di sicurezza è spesso percepita come atto dovuto, riducendo gli investimenti al minimo.

Inoltre si ricorre all'implementazione di misure di protezione che utilizzano piattaforme e soluzioni certamente valide, ma spesso poco contestualizzate rispetto all'ecosistema che si intende difendere, limitandosi al perimetro dell'ente/azienda e tralasciando la catena di *partner* e fornitori.

L'approccio alla *Cyber Security* che parte dalla valutazione dello stato corrente dei sistemi, ne individua i rischi e definisce le contromisure da adottare, stenta ancora ad affermarsi. Il dottor Conflitti ha concluso affermando che anche il processo di *procurement* va rivisto: dai criteri di selezione dei potenziali fornitori alla valutazione tecnico/economica delle offerte, dalla contrattualizzazione al monitoraggio della fornitura.

Aldo Di Mattia, *Principal System Engineer and Team Leader Centre/South Italy* di Fortinet, ha presentato l'azienda: un player internazionale con un sostanzioso *portfolio* clienti di oltre 400 mila unità, attiva nei settori Telco, PAC/Defense, PAL/Industry, Energy/Utilities.

Il *discussant* ha rilevato che, anche attraverso un'accresciuta consapevolezza del *management* delle realtà con le quali Fortinet si confronta, l'azienda propone ormai una protezione avanzata e continua rispetto a superfici d'attacco, sempre più ampie, integrate e automatizzate, oltre

alla potenza necessaria per soddisfare i requisiti prestazionali in continuo aumento, generati dalle reti *borderless* che costituiranno una naturale e inarrestabile evoluzione.

Certamente il panorama delle possibili minacce e dei rischi connessi è in costante evoluzione; una recentissima indagine ha rilevato che il 51% delle aziende "digitalizzate" è stata oggetto di attacchi che hanno comportato compromissioni di dati. La riduzione dei tempi di "scoperta" costituisce un importante elemento di efficace risposta.

L'architettura *Security Fabric* di Fortinet privilegia le attività preventive, con ampio utilizzo di processi di *AI* e di monitoraggio comportamentale attraverso *machine learning pattern* in ambienti rete, applicativi, *cloud* o *mobile*.

Le nuove barriere dell'evoluzione della *digital transformation* quali 5G, SDWAN (*Software-Defined Wide Area Network*), Multi-Cloud, OT, IoT e SDN saranno reali opportunità se l'ambiente operativo saprà garantirsi un adeguato livello di sicurezza.

Trend Micro, multinazionale con quartier generale a Tokyo con oltre 30 anni di attività, si propone, attraverso le nuove tecnologie di mettere in sicurezza molteplici ambiti, dal *cloud all industry 4.0*, al *mobile* e l'*IoT*.

Salvatore Marcis è il *Technical Director* per l'Italia e nel corso della sua presentazione ha rilevato come il futuro sia complesso, esposto, mal configurato, ma difendibile.

Trend ha scelto un approccio certamente sistemico per far fronte con flessibilità alla sempre più rapida evoluzione delle minacce; ha sviluppato caratteri di *design* multilivello, in modo da permettere ai sistemi di scambiare con continuità informazioni allo scopo di monitorare e individuare comportamenti sospetti, rivelatori di attività *cyber*; ha sviluppato prioritariamente l'automazione dei processi con l'obiettivo di rendere i *task* di sicurezza i più rapidi possibili per un'efficace difesa d'ambiente; infine potenziare le attività di controllo ed interoperabilità che consentano eventuali integrazioni verso sistemi terzi.

Federico Santi, responsabile dei servizi di *cybersecurity* di DXC Italia ha poi aperto il suo intervento, illustrando brevemente le caratteristiche prestazionali di DXC, azienda multinazionale sorta dalla fusione di HP Servizi e CSC per dare vita ad uno dei principali *IT service provider* a livello mondiale.

DXC è organizzata per aree di mercato e linee di offerta, tra le quali, oltre ai servizi *Cloud*, *Application* e *Analytics*, certamente quelli di *cybersecurity*, che ruotano attorno a nove *Global Security Center* con *Innovation Center* regionali; essi offrono supporto alle principali organizzazioni pubbliche e private, tra le quali sono presenti gran parte delle infrastrutture critiche nazionali.

Il *discussant* ha inteso porre poi l'accento su temi al momento di grande attualità e che devono essere congiuntamente affrontati.

In particolare:

- la valutazione dei rischi di *compliance* e *cyber* in generale è ormai un tema trasversale che interessa *CEO*, *risk managers*, *Audit*, *Legal* e non esclusivamente *CIO* e *CISO*; è pertanto indispensabile trasversalmente sviluppare metodi e strumenti di analisi capaci di identificare i rischi all'interno dei processi, organizzazioni e infrastrutture; per questo soprattutto gli IT *provider* devono rinnovarsi e, citando testualmente, "uscire dalla *comfort zone*";
- uno dei filoni della direttiva NIS forse più controverso è quello dell'*info-sharing*; infatti processi e organizzazioni ancora stentano ad avviare questo percorso virtuoso e l'ostacolo appare essere di natura sostanzialmente culturale: resistenza a superare l'idea che "siamo più sicuri con un approccio *security by obscurity*". È necessario al riguardo "riequilibrare il passo della comunità difensiva con quello della comunità offensiva",

investendo sulla selezione e *awareness* del *top management* per riorientare le rispettive organizzazioni;

- è indispensabile accelerare il passaggio dalle misure di sicurezza statiche (*civil law like*) a quelle dinamiche (*common law like* id. GDPR) al *continuous monitoring & reengineering*, attraverso un incremento qualitativo di *risk analysis*, alla sicurezza progettuale (SIEM, SOC, CERT) anche attraverso strumenti evoluti di *Big Data Analytics*, di *Artificial Intelligence* e analisi comportamentale.

Lorenzo Russo, *Director* di *Deloitte Cyber Risk Services,* ha inteso porre l'accento sull'espansione del profilo di rischio delle organizzazioni che hanno intrapreso il percorso di trasformazione digitale e dei relativi strumenti aggiornati di gestione del rischio.

Una recente indagine (*Deloitte's 2019 Future of Cyber Survey*) mostra che per quasi il 50 per cento delle organizzazioni in sviluppo digitale, la *cybersecurity* è stabilmente nell'agenda trimestrale del Consiglio d'Amministrazione.

Il *discussant* ha opportunamente sottolineato il ruolo chiave che il CISO (*Chief Information Security Officer*) assume nel processo di trasformazione digitale, che intenda efficacemente proteggere le infrastrutture critiche. In particolare, le differenti strutture organizzative permettono al CISO di focalizzarsi su ruoli tipicamente di indirizzo e controllo o anche di carattere tecnico. Egli assolve il compito di *reporting,* che peraltro non ha ancora un univoco riferimento sia all'interno che all'esterno dell'organizzazione.

In ambito organizzativo poi il *cyber risk*, determinato da un'analisi dinamica dello stesso, va opportunamente integrato con lo ERM (*Enterprise Risk Management*). Essa avviene attraverso un approccio basato sugli scenari di rischio, costituiti dalla combinazione di Minaccia, Asset interessato ed effetto determinato.

La metodologia di analisi quantitativa di *Cyber Risk Management* può essere applicata per l'identificazione del *Top Cyber Risk* di un'organizzazione e/o a supporto dell'identificazione degli investimenti di sicurezza.

Gli interventi dei qualificati rappresentanti di affermati *vendors*, brevemente riassunti, al di là delle rispettive soluzioni illustrate, hanno concordemente evidenziato la necessità:

- di porre massima attenzione all'elemento umano e alla sua continua formazione, quale fondamentale strumento di solida sicurezza aziendale e sistemica;
- che la valutazione dei rischi di *compliance* e *cyber* in generale è tema trasversale all'organizzazione che deve interessare CEO, *risk managers*, *Audit*, *Legal advisor* e non può più essere limitato a CIO e CISO;
- che le aziende procedano dinamicamente a modificare il proprio "modus operandi", non più proponendo uno specifico prodotto bensì valutando dinamicamente i rischi cui il *customer* è esposto, offrendo complessive soluzioni di sistema;
- che anche il processo di *procurement* sia rivisitato, ponendo maggiore attenzione ai criteri di selezione dei potenziali fornitori, alla valutazione tecnico/economica delle offerte, alla contrattualizzazione e al monitoraggio della fornitura;
- che il flusso di *info-sharing* tra gli operatori di sistemi complessi di sicurezza sia incrementato, costantemente aggiornato e congiuntamente attivate efficaci misure di prevenzione e investigazione.