Sicurezza stratificata: Il modello MindShield per proteggere infrastrutture critiche e servizi pubblici

Questo articolo fa parte di una serie dedicata al paradigma MindShield per la sicurezza integrata delle infrastrutture critiche. Nel presente contenuto analizzeremo la struttura del modello di sicurezza stratificata MindShield, esplorando i quattro livelli fondamentali che lo compongono: dalla base normativa alla cooperazione transnazionale. Esamineremo inoltre l'importanza dell'integrazione tra sicurezza fisica e logica e il coordinamento tra le diverse componenti per garantire una protezione efficace delle infrastrutture critiche e dei servizi pubblici essenziali.

Il modello di sicurezza stratificata MindShield per infrastrutture critiche

Uno degli aspetti su cui ci si è maggiormente soffermati nello spiegare l'approccio metodologico di questo progetto è stato proprio concetto di sicurezza stratificata. Avendo analizzato i componenti strumentali di *MindShield* possiamo ora dedicarci al disegno più ampio di questo progetto, ovvero alla composizione strutturale del modello.

In particolare, possiamo immaginare che alla base del modello vi sia riposto il compendio normativo, sia nazionale che sovranazionale, solido che consenta da un lato di rafforzare le misure di sicurezza delle infrastrutture critiche e dei servizi pubblici essenziali ma che permetta al contempo di salvaguardare i diritti, principi fondamentali e questioni

etiche. La componente legislativa, come abbiamo visto in diversi ambiti risulta in via di sviluppo, ma ad oggi una legislazione unitaria e risulta ancora carente.

Il secondo livello di *MindShield* è rappresentato dalla componente umana e dalla sicurezza fisica, elementi che insieme fanno parte di quell'approccio tradizionale e storico della security e che risultano a tutt'oggi imprescindibili per garantire la sicurezza delle infrastrutture critiche e dei servizi pubblici essenziali. Risulta difatti impensabile ipotizzare di affidare la sicurezza solo a tecnologie o innovazioni emergenti e sulle quali, peraltro, come si è avuto modo di accennare vi permangono svariati interrogativi e questioni da risolvere.

Il terzo livello della sicurezza è invece rappresentato dalla sicurezza logica e da tutte le tecnologie attualmente in via di sviluppo, il cui impiego consente di non solo di implementare e rendere più efficienti le procedure di controllo, di prevenire e mitigare i rischi e non da ultimo di rispondere prontamente nei casi in cui si dovessero verificare incidenti securitari.

Da ultimo possiamo ipotizzare, quale ulteriore, nonché complementare livello di sicurezza, la cooperazione transnazionale in materia di sicurezza, in relazione alle quali permangono ancora complesse sfide di coordinamento e creazione di un percorso unitario per la gestione di minacce e vulnerabilità locali, nazionali o globali.

Integrazione di tecnologie di sicurezza fisica e logica nel modello MindShield

Tra le componenti determinanti di *MindShield,* due di esse sono rappresentate dalle tecnologie fisiche e logiche, sulle quali ci si è soffermati in precedenza. Tuttavia, quando parliamo del modello sperimentale, oggetto del presente studio, dobbiamo comprendere in che modo queste ultime si corroborano

tra di esse e quali siano i benefici della loro applicazione sinergica.

Innanzitutto, come si è già avuto modo di chiarire, non è possibile ipotizzare allo stato dell'arte l'impiego di una sola di queste tecniche scissa dalle altre. Ciò è ancor più evidente posto che, le criticità, che le infrastrutture strategiche e i servizi pubblici essenziali si trovano ad affrontare, non riguardano singolarmente minacce fisiche o di tipo cibernetico e informatico. Oggigiorno, difatti, gli attacchi alla sicurezza risultano sempre più sofisticati e articolati nella propria esecuzione, complici anche le tecnologie in via di sviluppo che ne stanno supportando il perfezionamento. Risulta quindi indispensabile introdurre una serie di misure che possano rispondere ai pressanti bisogni di sicurezza.

Ciò non toglie che, a livello settoriale esistano certamente alcune iniziative per l'integrazione fisica e logica della sicurezza, tra queste si può ad esempio citare quella che ha visto protagonisti IBM e il consorzio sicurezza CNS Tech e che ha dato vita al CPSIEM, una piattaforma per il "Cyber-Physical Security Information Event Management"[1] che riunisce il controllo dei sistemi SIEM di IBM e PSIM di CNS. Questi processi di integrazione rappresentano dei modelli virtuosi che non possono essere esclusi da un modello per la gestione ottimizzata della sicurezza come quello di *MindShield.*

In particolare, per realizzare un tessuto securitario più solido nelle infrastrutture critiche e nei servizi pubblici essenziali, sarebbe necessario garantire la formazione in tema di cybersicurezza e di sicurezza fisica a tutti gli operatori del settore. L'impego di personale specializzato, in grado affrontare sfide complesse di sicurezza sta divenendo ormai un'esigenza sempre più concreta e impellente sia in ambito pubblico che privato. Peraltro, appare sempre più evidente la necessità di creare squadre multidisciplinari di esperti, che siano in grado di individuare e affrontare simultaneamente

eventi critici di tipo fisico o logico.

Un esempio "*lampante*" di tale esigenza è stato individuato dal CESPIS (Centro Studi Prevenzione Investigazione e Sicurezza), il quale ha esemplificato molto chiaramente uno scenario tipo: "*un device IP della videosorveglianza installato sulla rete dati va offline:*

- *il settore IT dirà che il problema risiede nel dispositivo, e dunque il settore della sicurezza fisica avviserà i responsabili della manutenzione;*
- *un tecnico controlla la videocamera "non funzionante", e scopre che la componente hardware è online (operativa), ma offline (inoperativa) solo nella parte software;*
- *il problema torna nuovamente al servizio IT, che nel frattempo scopre un malfunzionamento residente su un loro switch di rete che blocca il flusso dati.*

Ovviamente nessuno ha colpe dirette, se non quella indiretta, questo sì, della mancata integrazione di due settori vitali e strategici per ogni organizzazione che si dichiari tale!

Ed è proprio la mancanza di una vision finalizzata al raggiungimento dell'obiettivo a creare queste "illogiche" condizioni, che richiedono poi inutili sprechi di risorse (umane ed economiche) per giungere alla completa risoluzione dei problemi.

Del resto, tutto ciò si amplifica perché nel perimetro IT gli operatori, generalmente, non sono degli esperti di sistemi hardware dedicati alla sicurezza fisica; non ne conoscono il funzionamento e le funzionalità, dal momento che non ne sono mai stati responsabili, tanto della progettazione quanto della gestione di tali dispositivi.

Ma le motivazioni sono anche altre: nel dominio IT è sempre stato predominante lo sviluppo dei software, mentre in quello fisico è prevalsa sempre la funzionalità hardware; situazioni che hanno generato nel tempo questa paradossale "distonia"

linguistica, trasformatasi col tempo in una preoccupante barriera funzionale."[2]

Un esempio piuttosto lineare, che non può certamente dare conto della complessità dei problemi di sicurezza, ma che tuttavia consente di afferrare la rilevanza della integrazione fisico-logica degli elementi costitutivi di una rete di sicurezza efficace ed efficiente.

Coordinamento e collaborazione tra le componenti di *MindShield*

Sin qui si è dato atto dell'importanza dei diversi elementi costitutivi di *MindShield* così come del loro impiego simultaneo, tuttavia, è imprescindibile comprendere che, la somma dei singoli componenti non può offrire un risultato soddisfacente in assenza di un efficace coordinamento tra ciascuno di essi. Per tale ragione il modello proposto prevede la creazione di un piano sinergico per la sicurezza integrata.

In particolare, ciascuno dei componenti di *MindShield* dovrebbe potersi rapportare agli altri sia mediante la ricerca scientifica multidisciplinare sul tema che attraverso la creazione di piani di prevenzione e risposta agli incidenti di sicurezza. Peraltro, una siffatta collaborazione tra i vari livelli di *MindShield* potrebbe consentire di fornire risposte adeguate anche laddove uno dei componenti venisse compromesso, per una qualsiasi ragione.

Così, ad esempio, l'istituzione di unità di crisi transnazionali e permanenti potrebbero fornire supporto immediato in tutte quelle situazioni nelle quali uno dei componenti (come la sicurezza fisica) risultasse carente o compromesso, fornendo così un concreto ausilio in una condizione di emergenza e vulnerabilità di un territorio. Parimenti nei casi di interruzione o danneggiamento degli strumenti digitali potrebbe intervenire la componente umana e analogica, come è capitato ad esempio nei casi di corruzione

dei sistemi informatici degli ospedali, nei quali la componente umana è prontamente intervenuta attraverso l'introduzione in via eccezionale di procedure alternative e analogiche di accettazione e triage dei pazienti[3].

Proprio in ragione della necessaria connessione e cooperazione di tutti gli elementi di MindShield si può comprendere la scelta di un modello di sicurezza stratificata, nel quale i singoli elementi siano tra essi complementari e svolgano una funzione di consolidamento o risanamento del tessuto della sicurezza infrastrutturale e dei servizi pubblici essenziali.

Il modello MindShield di sicurezza stratificata rappresenta un approccio innovativo e integrato per la protezione delle infrastrutture critiche e dei servizi pubblici essenziali. Attraverso l'analisi dei quattro livelli strutturali e dell'importanza dell'integrazione fisico-logica, emerge chiaramente la necessità di un coordinamento sinergico tra tutte le componenti per garantire una sicurezza efficace e resiliente.

Per approfondire il tema vi invitiamo a consultare il white paper completo della Dottoressa **Livia Cimpoia** dal titolo **"MindShield" – un nuovo paradigma di sicurezza integrata per infrastrutture critiche"** per approfondire tutti gli aspetti del modello di sicurezza stratificata.

Nel prossimo articolo della serie esploreremo il ruolo cruciale della cooperazione internazionale nel modello MindShield, analizzando le sfide e le opportunità della collaborazione transnazionale per la gestione delle minacce globali alle infrastrutture critiche e ai servizi pubblici essenziali.

Note

[1] Si vedano in tal senso CNS Tech (2021). Sicurezza logica e fisica nei Data Center. Online:

https://www.consorziosicurezza.com/sicurezza-logica-e-sicurezza-fisica-nei-data-center/# [richiamato: 27.12.2023]. e Frattini, F., U. Giordano e V. Conti (2019). Facing Cyber-Physical Security Threats by PSIM-SIEM Integration. In, *2019 15th European Dependable Computing Conference (EDCC).* [Place of publication not identified]: IEEE (83–8).

[2] CESPIS (2023). L'importanza dell'integrazione tra sicurezza fisica e logica. [richiamato: 27.12.2023].

[3] Cfr., Agenzia ANSA (2022). A Milano attacco hacker agli ospedali Fatebenefratelli e Sacco. [richiamato: 27.12.2023].; e Agenzia ANSA (2023). Attacco hacker agli ospedali di Modena, riunita l'unità di crisi. Online: [richiamato: 27.12.2023].

Profilo Autore

Laureata in Giurisprudenza all'Università degli Studi di Milano, si è specializzata con il massimo dei voti in Scienze Forensi presso l'Università La Sapienza di Roma, con focus su sicurezza globale, infrastrutture critiche e crimini contro categorie vulnerabili.
Ha acquisito esperienza nella pubblica amministrazione attraverso il Servizio Civile Nazionale e lavorando per diverse amministrazioni pubbliche, occupandosi di contabilità pubblica, servizi sociali e servizio pubblico nei Ministeri degli Interni e della Giustizia.
Attualmente è funzionaria presso il Ministero della Giustizia, in servizio al Tribunale di Milano – XII Sezione Civile, dove si occupa di diritto dell'immigrazione, protezione internazionale e diritto di soggiorno.
Ha partecipato a formazioni di eccellenza organizzate dalla Scuola Nazionale della Magistratura, dal Ministero della Giustizia e dall'Agenzia Europea per l'Asilo (EUAA), acquisendo competenze nella valutazione delle domande di Protezione Internazionale e nella produzione di Report COI.
In conclusione del tirocinio forense, mentre si prepara a conseguire il titolo di avvocato, sta perseguendo una seconda

laurea magistrale in psicologia del lavoro e delle organizzazioni.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/sicurezza-stratificata/