



Continuit  operativa, vigilanza nelle infrastrutture e la nuova ondata di attacchi ai dati sanitari

Descrizione

(Adnkronos)    Nel terzo episodio di    State sicuri. Dentro la sicurezza che cambia  , Francesco Di Maio (Elt Group), Giulio Gravina (Anivip  Italtel) e Nunzia Ciardi (Acn) disegnano una sicurezza    di sistema  : business continuity lungo lâ  intera filiera, presidio fisico dei nodi strategici e contrasto a minacce digitali potenziate dall  intelligenza artificiale. Dal jamming ai droni, fino ai ransomware sulla sanit  : persone, processi e tecnologia devono lavorare insieme. La bussola della puntata    la continuit  operativa. Francesco Di Maio, chief security, risk management & business continuity officer di Elt Group, ricorda che oggi i servizi critici non sono    soltanto i servizi dell  azienda, ma sono servizi erogati a favore della comunit    , e che la resilienza richiede un approccio    sistemico, metodologico  , fino a porsi la domanda-chiave:    quanto tempo possiamo rimanere fermi in assoluto per poi riprendere i servizi senza pregiudicare il nostro business, ma anche lâ  identit  di una collettivit    . Nella pi   recente strategia della Nato, osserva, il termine    resilienza      citato 12 volte proprio per estendere lâ  attenzione ai soggetti civili. L  esempio concreto arriva dall  attacco dell  8 dicembre 2023 a un provider cloud italiano:    sette milioni di persone per giorni sono rimasti prive di servizi essenziali  . Per Di Maio la lezione    chiara: servono pianificazione, legami stretti con le istituzioni e un  attenzione reale alla catena dei fornitori, perch   interrompere queste forniture significa bloccarci  , soprattutto in un Paese fatto di Pmi.    La security non    un costo  ,    un investimento  . Il fronte tecnologico si allarga alla guerra elettromagnetica: dal disturbo dei segnali gps (jamming) al contrasto dei droni.    Per noi la migliore arma contro il carro armato era lo stesso carro armato. Oggi    diventato il drone  , afferma Di Maio. Ecco perch   serve una cognizione    a 360    che affianchi alla componente convenzionale quella elettromagnetica, dominio in cui lâ  alleanza occidentale punta il proprio vantaggio tecnologico. Sul terreno, la vigilanza privata    parte stabile dell  architettura del Paese. Giulio Gravina ricostruisce la svolta del Dm 269/2010:    c     stata una vera e propria rivoluzione  , con lâ  ingresso delle guardie giurate nelle infrastrutture critiche.    Oggi le infrastrutture critiche italiane si servono quasi totalmente della vigilanza privata  , spiega, ricordando che istituti e operatori operano con licenza del ministero dell  Interno e controlli periodici su profili etici e formativi. Il passo successivo    la vera integrazione tra sicurezza fisica e sicurezza logica: nelle grandi aziende esistono gi   centri di monitoraggio digitale, ma    anche la stessa telecamera   pu   diventare vettore o vittima di un attacco. Il quadro dei rischi cyber lo completa Nunzia Ciardi, vicedirettrice generale

dell'Acn: l'intelligenza artificiale è un'alleata preziosa• anche per gli aggressori, perché rende più efficienti molte fasi dell'attacco, dall'individuazione automatica delle vulnerabilità ai malware adattivi, fino ai deepfake indistinguibili. L'impatto più doloroso: la sanità. Tra 2023 e 2024 circa 50 attacchi ad Asl• hanno interrotto servizi essenziali; nell'area di Rho un solo attacco ha colpito un bacino di oltre 500.000 utenti•, fermando radioterapie, pronto soccorso, trasfusioni e sale operatorie. Gli operatori dell'Acn vanno sul posto• per accelerare il ripristino. Ma c'è anche un danno silente: il furto di cartelle cliniche, inclusi dati di minori, poi riversati nel dark web. Per questo la cybersicurezza non è una sicurezza tecnica•: riguarda la vita quotidiana e richiede consapevolezza diffusa oltre alla tecnologia. Il messaggio dell'episodio è netto: persone, processi e tecnologia devono muoversi insieme. La continuità del servizio pubblico dipende dalla programmazione delle imprese; il presidio fisico di siti e reti va connesso al monitoraggio digitale; la risposta dello Stato si rafforza con standard condivisi e filiere preparate, dai grandi gruppi alle Pmi, dalla sala operativa di un'utility al reparto ospedaliero. cronacawebinfo@adnkronos.com (Web Info)

Categoria

1. H24News

Tag

1. adnkronos
2. Ultimora

Data di creazione

Settembre 1, 2025

Autore

andreaperocchi_pdnrf3x8

default watermark