
# ContinuitÃ  operativa, vigilanza nelle infrastrutture e la nuova ondata di attacchi ai dati sanitari

## Descrizione



(Adnkronos) â?? Nel terzo episodio di â??State sicuri. Dentro la sicurezza che cambiaâ?•, Francesco Di Maio (Elt Group), Giulio Gravina (Anivipâ??Italpol) e Nunzia Ciardi (Acn) disegnano una sicurezza â??di sistemaâ?•: business continuity lungo lâ??intera filiera, presidio fisico dei nodi strategici e contrasto a minacce digitali potenziate dallâ??intelligenza artificiale. Dal jamming ai droni, fino ai ransomware sulla sanitÃ : persone, processi e tecnologia devono lavorare insieme. La bussola della puntata Ã¨ la continuitÃ  operativa. Francesco Di Maio, chief security, risk management & business continuity officer di Elt Group, ricorda che oggi i servizi critici non sono â??soltanto i servizi dellâ??azienda, ma sono servizi erogati a favore della comunitÃ â?•, e che la resilienza richiede un approccio â??sistematico, metodologicoâ?•, fino a porsi la domanda-chiave: â??quanto tempo possiamo rimanere fermi in assoluto per poi riprendere i servizi senza pregiudicare il nostro business, ma anche lâ??identitÃ  di una collettivitÃ â?•. Nella piÃ¹ recente strategia della Nato, osserva, il termine â??resilienzaâ?• Ã¨ citato 12 volte proprio per estendere lâ??attenzione ai soggetti civili. Lâ??esempio concreto arriva dallâ??attacco dellâ??8 dicembre 2023 a un provider cloud italiano: â??sette milioni di persone per giorni sono rimasti prive di servizi essenzialiâ?•. Per Di Maio la lezione Ã¨ chiara: servono pianificazione, legami stretti con le istituzioni e unâ??attenzione reale alla catena dei fornitori, perchÃ© â??interrompere queste forniture significa bloccarciâ?•, soprattutto in un Paese fatto di Pmi. â??La security non Ã¨ un costoâ?¦ Ã¨ un investimentoâ?•. Il fronte tecnologico si allarga alla guerra elettromagnetica: dal disturbo dei segnali gps (jamming) al contrasto dei droni. â??Per noi la migliore arma contro il carro armato era lo stesso carro armato. Oggi Ã¨ diventato il droneâ?•, afferma Di Maio. Ecco perchÃ© serve una cognizione â??a 360Â°â?• che affianchi alla componente convenzionale quella elettromagnetica, dominio in cui lâ??alleanza occidentale punta il proprio vantaggio tecnologico. Sul terreno, la vigilanza privata Ã¨ parte stabile dellâ??architettura del Paese. Giulio Gravina ricostruisce la svolta del Dm 269/2010: â??câ??Ã¨ stata una vera e propria rivoluzioneâ?•, con lâ??ingresso delle guardie giurate nelle infrastrutture critiche. â??Oggi le infrastrutture critiche italiane si servono quasi totalmente della vigilanza privataâ?•, spiega, ricordando che istituti e operatori operano con licenza del ministero dellâ??Interno e controlli periodici su profili etici e formativi. Il passo successivo Ã¨ la vera integrazione tra sicurezza fisica e sicurezza logica: nelle grandi aziende esistono giÃ  centri di monitoraggio digitale, ma â??anche la stessa telecameraâ?• puÃ² diventare vettore o vittima di un attacco.  Il quadro dei rischi cyber lo completa Nunzia Ciardi, vicedirettrice generale

dellâ??Acn: lâ??intelligenza artificiale Ã¨ â??unâ??alleata preziosaâ?• anche per gli aggressori, perchÃ© rende piÃ¹ efficienti molte fasi dellâ??attacco, dallâ??individuazione automatica delle vulnerabilitÃ  ai malware adattivi, fino ai deepfake â??indistinguibiliâ?•. Lâ??impatto piÃ¹ doloroso: la sanitÃ . â??Tra 2023 e 2024 circa 50 attacchi ad Aslâ?• hanno interrotto servizi essenziali; â??nellâ??area di Rho un solo attacco ha colpito un bacino di oltre 500.000 utentiâ?•, fermando radioterapie, pronto soccorso, trasfusioni e sale operatorie. Gli operatori dellâ??Acn â??vanno sul postoâ?• per accelerare il ripristino. Ma câ??Ã¨ anche un danno silente: il furto di cartelle cliniche, inclusi dati di minori, poi riversati nel dark web. Per questo â??la cybersicurezza non Ã¨ una sicurezza tecnicaâ?•: riguarda la vita quotidiana e richiede consapevolezza diffusa oltre alla tecnologia. Il messaggio dellâ??episodio Ã¨ netto: persone, processi e tecnologia devono muoversi insieme. La continuitÃ  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 unâ??utility al reparto ospedaliero. â??cronacawebinfo@adnkronos.com (Web Info)

**Categoria**

1. H24News



**Tag**

1. adnkronos
2. Ultimora

**Data di creazione**
Settembre 1, 2025
**Autore**
andreaperocchi_pdnrf3x8