REGIONE CAMPANIA

Antonio Cardarelli
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE

CYBERSECURITY E SANITÀ: UN CAMBIO DI PARADIGMA

Salvatore Ascione

28 Novembre 2024

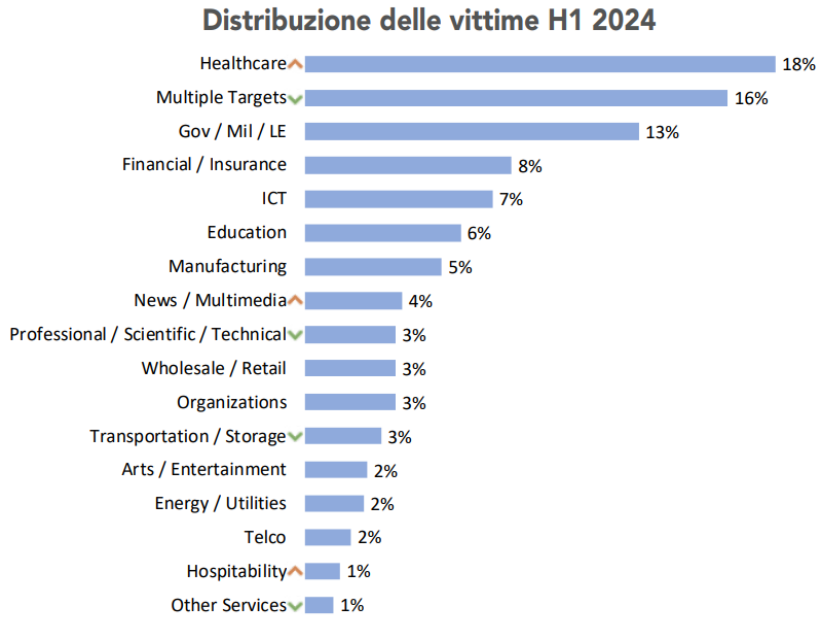
CONTESTO

- La cybersecurity nel settore sanitario è un tema di crescente importanza, considerata la vulnerabilità di infrastrutture critiche e la quantità di dati sensibili trattati. Gli attacchi informatici, come ransomware e phishing, hanno mostrato un aumento significativo negli ultimi due anni, mettendo a rischio servizi essenziali e la privacy dei pazienti. (Relazione annuale dell'Agenzia per la cybersicurezza nazionale (ACN))

- I dati sanitari valgono fino a 10 volte di più rispetto ai dati finanziari su mercati illeciti.

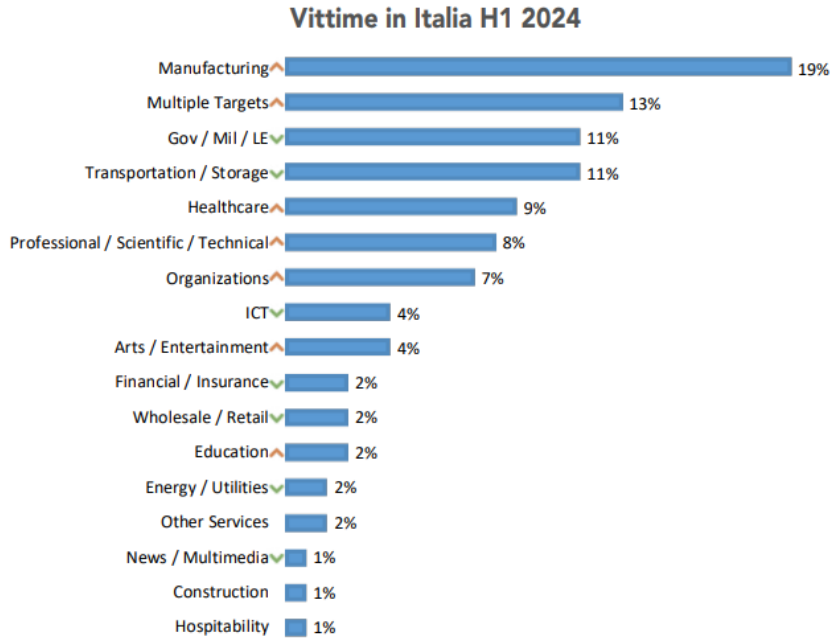
STATISTICHE

Lo scenario mondiale vede la sanità come il primo settore vittima di cyber-attacchi, con circa il 18% del totale.



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

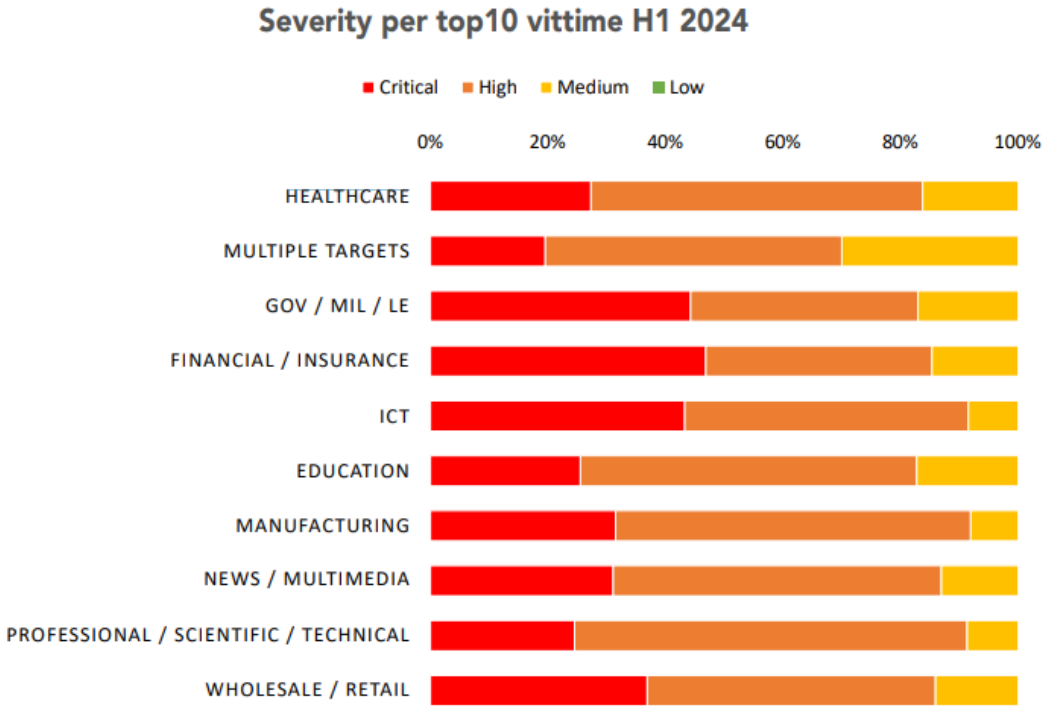
In Italia, l'healthcare è il quinto settore più colpito da attacchi informatici, con circa il 9% del totale



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

TIPOLOGIE DI ATTACCHI PIU' DIFFUSE

- **Ransomware**: blocco dei dati e richiesta di riscatto.
- **Phishing**: sottrazione di credenziali attraverso email ingannevoli.
- **Malware**: software dannosi che compromettono i sistemi.



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

IMPATTO e COSTI PER UNA AZIENDA SANITARIA

- Interruzione dei servizi sanitari essenziali, ritardi per espletare prestazioni sanitarie e, di conseguenza, disagi ai pazienti (**Direzione Sanitaria**)
- Compromissione della privacy dei pazienti ed attivazione procedure di tutela (**Ufficio Legale, Ufficio Comunicazione e Trasparenza, DPO**)
- Costi economici per la risoluzione e ripristino dei sistemi (remediation) e la gestione delle crisi (procedure alternative) (**Ufficio Sistemi Informativi**)
- Danno alla reputazione Aziendale (**DIREZIONE GENERALE**)

CONVIENE IL CAMBIO DI PARADIGMA IN SANITA'

COME ATTUARE IL CAMBIO DI PARADIGMA

- Crittografia dei dati sensibili. (Le funzioni di hash crittografiche)
- Micro-Segmentazione delle reti informatiche aziendali (Innovative MFA-based segmentation solution)
- Controllo rigoroso degli accessi e autenticazione a più fattori. (Multi Factor Authentication -MFA)
- Analisi periodica dei rischi e aggiornamento dei sistemi. (Sistemi di rilevamento delle intrusioni)
- Formazione continua del personale sulle pratiche di sicurezza informatica.

MODELLO ZERO TRUST

SOLO COSI' LA SANITA' E' GIA' PRONTA PER IL NIS 2

- Implementazione di misure che riducono in maniera significativa il rischio di data violation e attacchi ransomware
- Cambio di paradigma che rappresenta una sfida considerevole anche in termini di budget

RIFERIMENTI

- https://www.acn.gov.it/portale/relazione-annuale-2023
- https://www.cybersecurity360.it/legal/telemedicina-e-nis-2-la-sicurezza-dei-pazienti-al-centro-un-approccio-metodico-e-avanzato/
- https://clusit.it/rapporto-clusit/
- https://www.nis-2-directive.com/