icom
istituto per la competitività

DATI SANITARI
Cybersecurity, interoperabilità e privacy: quali nodi da sciogliere?

Mercoledì 20 Luglio 2022 ore 17:00 - 19:00
Roma, Sede I-Com, Palazzo Colonna, Piazza dei Santi Apostoli 66

Il trattamento dei dati personali in ambito sanitario

Nell'ecosistema delineato dal GDPR, per i dati sanitari è previsto un regime di **tutela rafforzata** (art.9) che determina un divieto generale di trattamento, fatta eccezione per alcune ipotesi.

Tra queste:

- Trattamento per **finalità di cura** (protetto dal segreto professionale)
- Trattamento per **interesse pubblico** (governo e ricerca)

Al di fuori delle ipotesi previste dall'art. 9, il trattamento deve possedere una base giuridica, che spesso viene individuata nel **consenso**

La centralità assoluta delle opportunità derivanti dell'utilizzo dei dati sanitari emerge anche dalla **Strategia europea per i dati**

Creazione dell'EHDS

L'obiettivo è quello di favorire la realizzazione di un **mercato unico per lo scambio e l'utilizzo dei dati sanitari**, delle cartelle cliniche elettroniche e dei sistemi di intelligenza artificiale
Allo stesso tempo, questa iniziativa pone le basi per **l'utilizzo secondario dei dati** per la ricerca, l'innovazione terapeutica e l'elaborazione di politiche e norme evidence-based.

Il Fascicolo Sanitario Elettronico: le nuove Linee guida

Le **Linee Guida per l'Attuazione del Fascicolo Sanitario Elettronico**, che sintetizzano ed emendano tutte le precedenti raccomandazioni, sono state pubblicate l'11 luglio 2022.

Il documento si sviluppa a partire da diverse constatazioni:

- Il FSE è stato **sviluppato in maniera disomogenea** nei vari contesti regionali
- **Il nucleo minimo di informazioni non è stato implementato** in tutte le regioni
- Contiene **dati non strutturati** che ne limitano fortemente l'utilizzo

Inoltre viene evidenziato come elementi fondamentali, tra cui il patient summary, risultino ad oggi poco alimentati sia per mancanza di competenze che di risorse

Le direttrici d'azione individuate dalle Linee guida

1. Garantire servizi di sanità digitale omogenei ed uniformi
2. Uniformare i contenuti in termini di codifiche adottate
3. Rafforzare l'architettura per migliorare l'interoperabilità
4. Potenziare la governance delle regole di attuazione

Il ruolo dell'interoperabilità

I livelli di interoperabilità

Interoperabilità di base: dati trasferiti da un sistema all'altro senza essere interpretati o trasformati

Interoperabilità strutturale: dati standardizzati così che possano essere scambiati ed interpretati da più sistemi

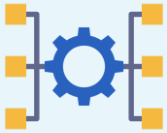
Interoperabilità organizzativa: scambio continuo di dati tra varie organizzazioni con obiettivi e normative diversi

Interoperabilità semantica: scambio tra sistemi di dati con strutture completamente diverse indipendentemente dal formato o dall'origine

Benefici ottenibili

- Migliore **coordinamento delle cure**
- Erogazione di **prestazioni qualitativamente superiori**
- **Migliore qualità del lavoro** per il personale amministrativo e clinico
- **Qualità della vita superiore** per i pazienti
- Facilitazione della **gestione finanziaria** e della **programmazione**

Il modello di interoperabilità per il FSE: nodi da sciogliere



L'INI (**Infrastruttura Nazionale per l'Interoperabilità**) svolge la funzione di mediatore nella comunicazione tra i diversi FSE Regionali, con vari scopi: **indicizzare i documenti** relativi a **eventi avvenuti fuori Regione**; intermediare le **richieste di ricerca e consultazione** di documenti tra diverse Regioni e **abilitare il trasferimento dei fascicoli** tra i domini regionali.

La norma prevede che i documenti contenuti nell'FSE seguano gli standard **HL7 CDA** (Clinical Document Architecture) release 2 e i **sistemi di codifica** nazionali e internazionali (es. ICD-9-CM per la classificazione delle patologie)

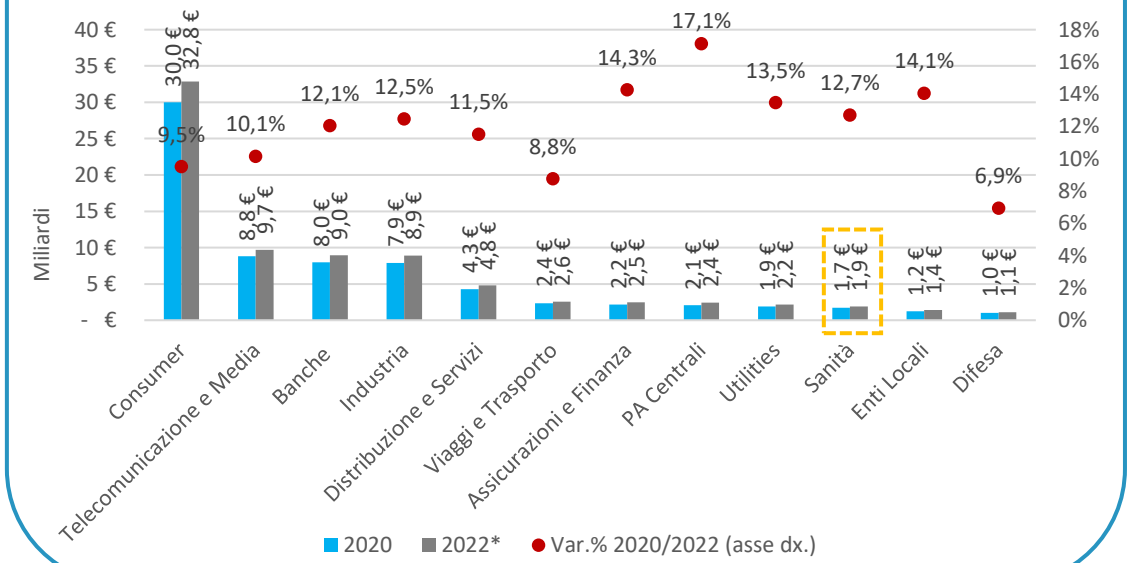
Secondo le Linee Guida, l'interoperabilità degli FSE regionali risulta senza dubbio **limitata dai seguenti fattori**:

- **Assenza di un'Anagrafe Nazionale Assistiti** alla quale sia possibile allineare le Anagrafi Regionali utilizzate per l'apertura dei fascicoli
- **Esperienza di uso disomogenea** nella restituzione grafica e nella presentazione dei documenti all'utente
- Applicazione di modalità di **firma digitale differenti**
- **Metadatazione non omogenea** dei documenti antecedenti la creazione dell'Infrastruttura Nazionale Interoperabilità
- **Processi di trasferimento** dei fascicoli tra Regioni **non automatizzabili**
- Possibilità di avere fascicoli aperti su **posizioni anagrafiche non esistenti** per INI (perché basati sul sistema Tessera Sanitaria)
- **Impossibilità di recuperare e visualizzare documenti prodotti in strutture di altre Regioni**

La trasformazione digitale della sanità e il rischio cyber

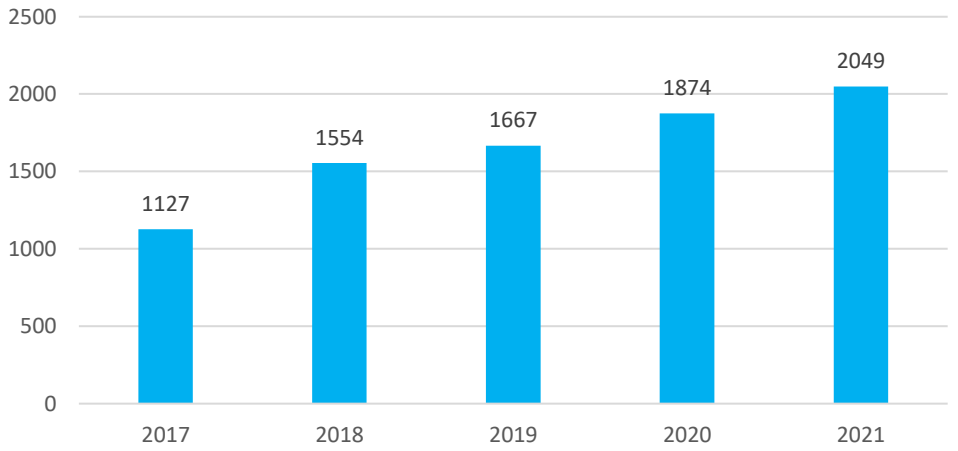
Il processo di **trasformazione digitale del settore sanitario** è stato evidentemente accelerato dall'emergenza pandemica, portandolo a quota €1,7 miliardi nel 2020 in termini di spesa digitale. Una fetta minoritaria in un mercato digitale italiano giunto a quota €71,5 miliardi, ma che mostra **trend in crescita in particolare nel biennio 2021-2022 (+12,7%).**

Il mercato digitale in Italia per settore economico



Il ricorso a soluzioni digitali, oltre alle innumerevoli esternalità positive**, ha portato anche alla nascita di nuovi rischi**, come quelli derivanti dal crescente fenomeno del **cyber-crime**. Nel periodo 2017-2021, il numero di azioni attacchi gravi è cresciuto ad un **CAGR del 12,7%,** che le ha portate quasi a raddoppiare (+82%)

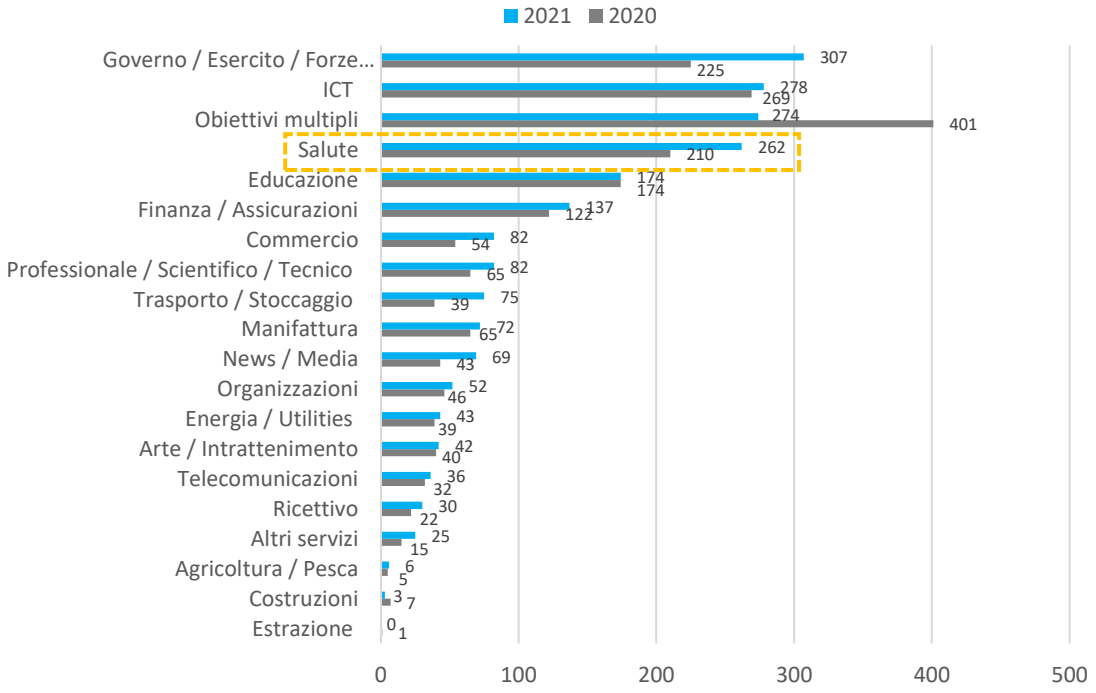
Attacchi informatici gravi a livello globale



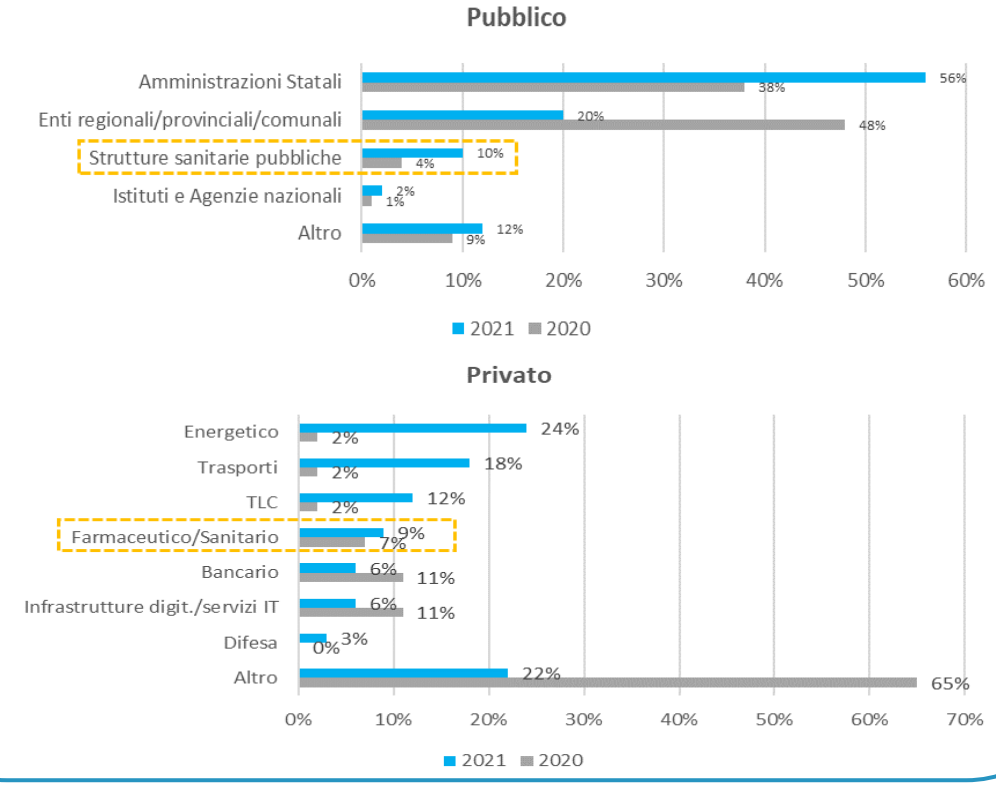
Fonte: NetConsulting cube (ottobre 2021) e Clusit (marzo 2022)

La cybersecurity in sanità

Il comparto sanitario figura al quarto posto, essendo stato vittima di ben **262 attacchi** gravi a livello **globale**, uno dei settori che hanno visto il **maggiore aumento** di attacchi tra il **2020** e il **2021** in **valori assoluti (+52 YoY)**



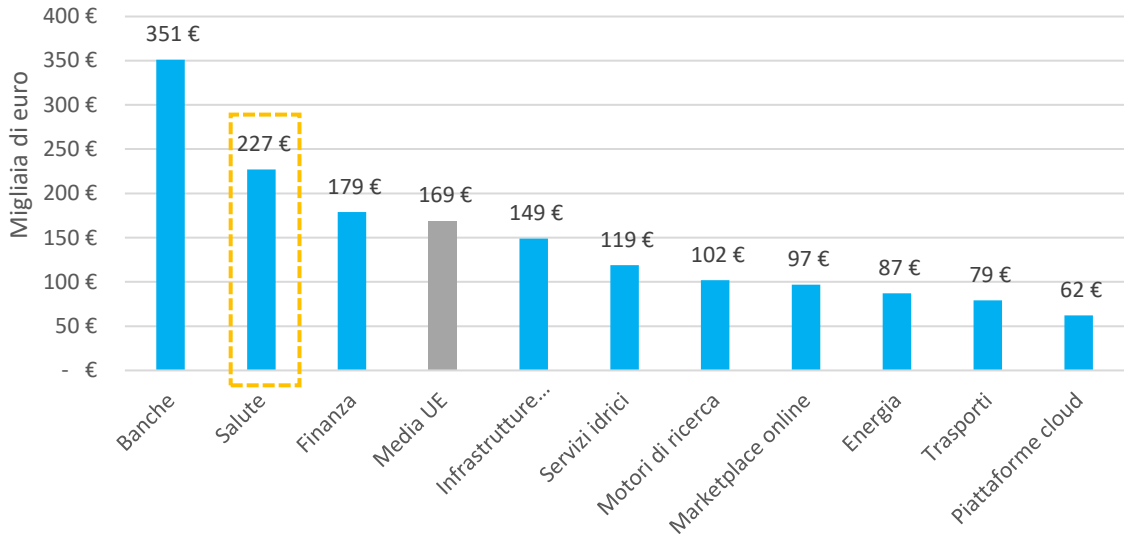
Anche a livello nazionale il settore risulta un target ambìto, in particolare a livello **pubblico** (oggetto del **10%** degli **attacchi complessivi**), sebbene anche nel **privato** gli attacchi risultino in crescita (9% degli attacchi)



Fonte: Clusit (marzo 2022) e Presidenza del Consiglio dei Ministri (Relazione sulla politica dell'informazione per la sicurezza, 2021)

L’aspetto economico

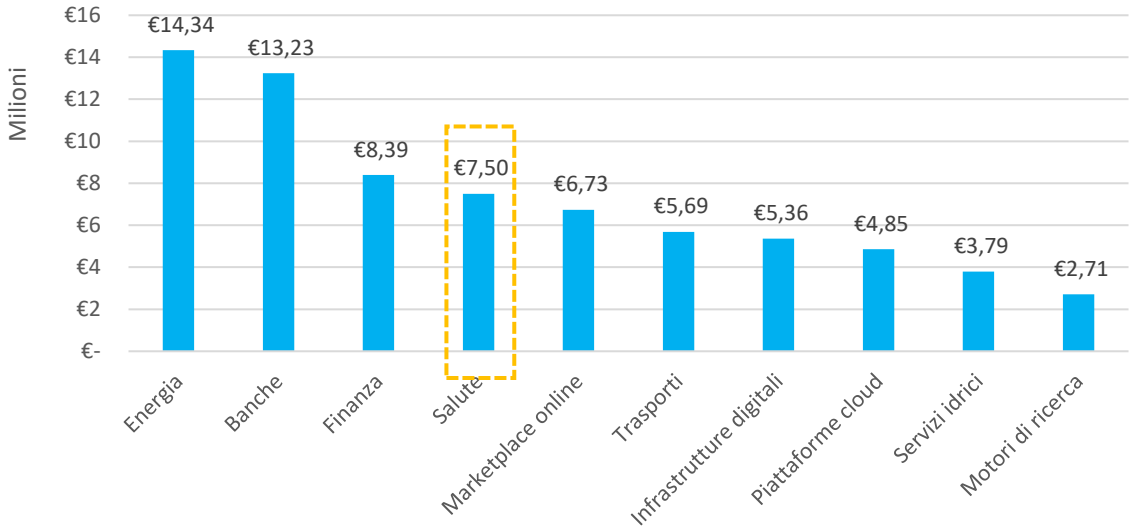
Costo medio di un grave incidente di sicurezza informatica in UE per settore



Il comparto sanitario, con un danno medio di circa €227 mila, occupa il **secondo posto tra le tipologie di organizzazioni che subiscono i danni più rilevanti** in caso di incidente di sicurezza informatica

La sanità risulta uno dei comparti più bersagliati dai cybercriminali, presenta però **investimenti in cybersecurity sensibilmente inferiori a quelli di altri settori** strategici quali comparto energetico, bancario e finanziario

Spesa media in sicurezza informatica degli OSE/DSP per settore



Fonte: Enisa

I nostri contatti

Piazza dei Santi Apostoli 66
00187 Roma
tel. +39 06 4740746

Rond Point Schuman, 6
1040 Bruxelles
Tel. + 32 (0) 22347882
info@i-com.it

www.i-com.it
www.i-comEU.eu