Sicurezza informatica in ambienti sensibili immersione nel settore sanitario

WHITE PAPER



STORMSHIELD

Nulla ferma i criminali informatici. Di fronte all'importanza vitale dell'ambiente medico, non esitano ad approfittare delle fragilità dovute alla crisi sanitaria o delle falle derivanti dalla trasformazione digitale del settore. In Francia e all'estero, ospedali, farmacie, laboratori e altre strutture sanitarie si trovano ad affrontare continue ondate di attacchi cibernetici in un contesto di elevata vulnerabilità informatica.

Nel 2021, il numero di segnalazioni di incidenti nel settore della sanità è raddoppiato rispetto al 2020[1]. Come si spiega questo incremento senza precedenti? Le risposte sono tanto varie quanto le vulnerabilità delle strutture, e di recente si è aggiunto anche il profilo inedito di determinati bersagli. Infatti, questi incidenti vengono attualmente riscontrati dai fornitori di servizi nel settore sanitario.

Una delle principali preoccupazioni riguarda i dati sensibili in ambito medico. Sebbene la loro appetibilità per i criminali informatici non sia in dubbio, la gestione è oggetto di un ampio dibattito, in particolare nell'attuale contesto di strutturazione di un quadro normativo europeo.

L'obiettivo del presente white paper è quindi quello di consentire ai responsabili IT e all'intero ecosistema di collaboratori esterni e fornitori di servizi nel settore medico di immergersi nel contesto attuale del tema della sicurezza informatica nelle istituzioni sanitarie.

A tal fine, nelle pagine seguenti ci proponiamo di analizzare i problemi che affliggono il settore sanitario, di offrire un inventario operativo di possibili soluzioni e di avanzare alcune proiezioni sul futuro della sicurezza informatica nel settore.

04 — Relatori

01. Sicurezza informatica nel settore sanitario: perché tanta fragilità?

08 — *Infografica: panoramica globale degli attacchi informatici alle organizzazioni sanitarie*
10 — Forti vincoli materiali : un parco informatico unico nel suo genere
14 — Trasformazione digitale nella sanità: un'accelerazione tardiva da sostenere
16 — Il caso particolare dei dati sanitari
17 — *Intervista a Charles Blanc-Rolin : Qual è il legame tra accesso ai dati, salute e sicurezza ?*

02. Anatomia di una minaccia polimorfa con punti di ingresso multipli

22 — In che modo i criminali informatici si introducono nel sistema informatico delle strutture sanitarie?
26 — L'intero percorso assistenziale al centro del mirino
28 — Questo non è un attacco informatico

03. Quali rimedi adottare per rendere più sicuro il settore sanitario?

32 — Quali sono le misure per proteggere le infrastrutture sanitarie?
37 — *Focus: quali obblighi normativi vigono per le organizzazioni sanitarie?*
38 — Sensibilizzazione e impegno sostenuti dall'azione pubblica
40 — *Intervista incrociata: Il regolamento europeo sui dati sanitari è adeguato alle sfide?*

04. E in futuro?

46 — Un continuum di assistenza a livello europeo
48 — Medicina preventiva, gestione ospedaliera basata sui dati:le promesse (e le sfide) dei Big Data in campo medico
50 — Una collaborazione da consolidare
52 — *Intervista a Jacky Grisey : Il futuro della sicurezza informatica nel settore sanitario*

Relatori

CHARLES BLANC-ROLIN
RESPONSABILE DI PROGETTO PER LA SICUREZZA DIGITALE NEL SETTORE DELLA SANITÀ ELETTRONICA PAYS DE LA LOIRE

« In alcuni casi ho implementato soluzioni di bloccaggio fisico per le porte USB in collaborazione con il responsabile biomedico. In questo modo si evita, ad esempio, che qualcuno utilizzi l'ecografo per caricare il proprio smartphone... »
PAGINA 31

Qual è il legame tra accesso ai dati, salute e sicurezza ?
PAGINA 17

JACQUES LABIDURIE
RSSI CLINICA UNIVERSITARIA DI LIMOGES

« Gli industriali devono essere formati in materia di sicurezza informatica, visto che molti gestiscono ancora le tecnologie informatiche come 30 anni fa. Inoltre, le facoltà di medicina dovrebbero proporre anche dei corsi di sicurezza informatica, e non solo sulla protezione dei dati, come avviene attualmente. »
PAGINA 34

STORMSHIELD

JACK GRISEY
SECURITY OPERATIONS MANAGER DEDICATO AL SETTORE SALUTE ADVENS

« I principali attacchi informatici che si sono verificati negli ultimi anni hanno evidenziato le lacune in termini tecnici e organizzativi dei sistemi informatici delle organizzazioni sanitarie. Si è delineata una presa di coscienza, anche ai più alti livelli di governo. »
PAGINA 42

Il futuro della sanità nella sicurezza informatica
PAGINA 52



CORALIE ACHARD-TORTUL
DPO CLINICA UNIVERSITARIA DI LIMOGES

« Nelle nostre attività di sensibilizzazione la contestualizzazione è molto importante. L'incontro preliminare con il responsabile dell'unità permette, ad esempio, di capire come funziona la struttura e di acquisire esempi reali, come quello di lasciare la scheda in posizione durante le varie manipolazioni radio... »
PAGINA 35

JEAN-SYLVAIN CHAVANNE
RSSI CLINICA UNIVERSITARIA DI BREST

« Fatture false, richieste di rinnovo password fraudolente, reclami di pazienti immaginari... la qualità delle campagne di phishing che intercettiamo è in aumento. Alcuni si spingono addirittura a usurpare l'identità dell'Ospedale Universitario di Brest. »
PAGINA 23

Riflettori puntati sui dispositivi medici connessi
PAGINA 13

STÉPHANE PRÉVOST
PRODUCT MARKETING MANAGER STORMSHIELD

« L'installazione di una patch per una vulnerabilità critica su un componente esposto in Internet non garantisce la protezione da un precedente sfruttamento. È inoltre necessario analizzarne i log per verificare se è stato sfruttato e, in caso di dubbio, rinnovare tutti gli account. »
PAGINA 34

RAYNA STAMBOLIYSKA
ESPERTA DI DIPLOMAZIA DIGITALE, SPECIALISTA IN SICUREZZA INFORMATICA E MEMBRO INDIPENDENTE DEL GRUPPO DI LAVORO SULLE MINACCE EMERGENTI E FUTURE DELL'ENISA

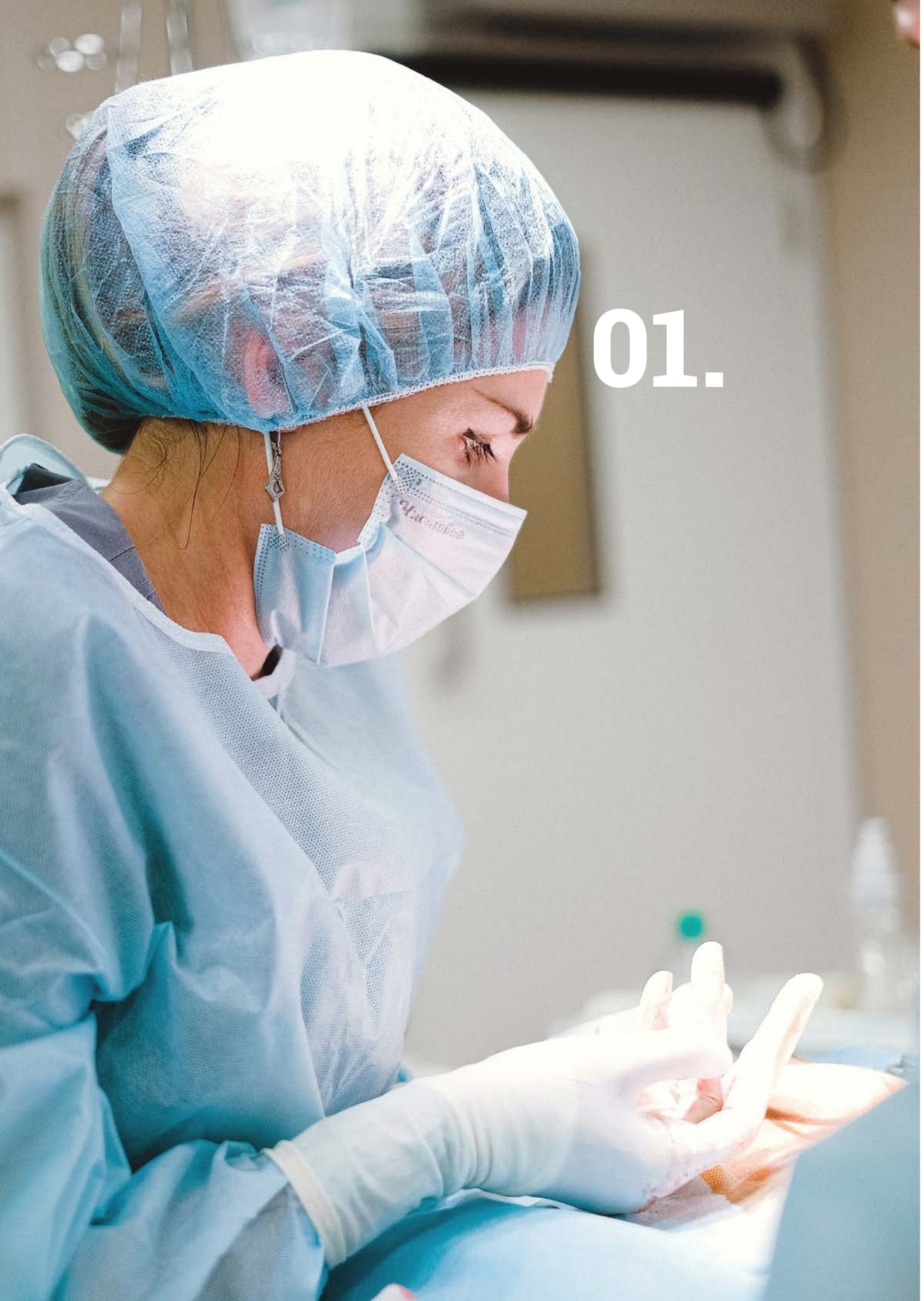
« I testi DSA e DMA, che affrontano il tema in modo trasversale e sistemico, sono in linea con i vari testi, tra cui il RGPD, la direttiva NIS e il Data Act. Essi mirano a proteggere l'innovazione, a tutelare i residenti europei e a stabilire l'autorità strategica dell'Unione europea. »
PAGINA 37

Il regolamento europeo sui dati sanitari è adeguato alle sfide?
PAGINA 41

DAMIAN KLIMAS
ASSOCIATO E OSSERVATORE DI DOTLAW DELLA RETE EHEALTH NETWORK

« L'adozione dell'EHDS accelererà l'implementazione di MyHealth@EU. Ciò significa che entro il 2025 le strutture sanitarie di tutti gli Stati membri e della Norvegia avranno un accesso facile e sicuro ai dati relativi alle allergie, alle prescrizioni e alla storia clinica di qualsiasi paziente, nella sua lingua, anche se vive in un altro Paese europeo. »
PAGINA 47

Il regolamento europeo sui dati sanitari è adeguato alle sfide?
PAGINA 41



01.

Sicurezza informatica nel settore sanitario: perché tanta fragilità?

Perché ospedali, cliniche, farmacie e laboratori sono così vulnerabili ai rischi informatici? Dall'architettura dei sistemi informatici sanitari ai loro componenti, passando per i nuovi impieghi in campo medico, i motivi sono purtroppo tanto diversi quanto variegati.

Panoramica globale
degli attacchi informatici alle organizzazioni sanitarie



Centro medico presbiteriale di Hollywood
2016 — STATI UNITI

Ospedali Baton Rouge General, Jack Huston Memorial e Southwest Health[2]
2022 — STATI UNITI

Healthcare Service Executive
2021 — IRLANDA

l sistema sanitario della provincia di Terranova e Labrador[3]
2021— CANADA

Ospedale pediatrico di Boston
2014 — STATI UNITI

Ministero della salute
2021 — BRASILE

Organismi per la sanità
2020 — REGNO UNITO

National Health Service
2017 — REGNO UNITO

Ospedale universitario dell'Ile-de-France AP-HP
2020 — FRANCIA

Centre Hospitalier Sud Francilien de Corbeil Essonne
2022 — FRANCIA

Sistema francese di assicurazione
2022 — FRANCIA

Sistema sanitario[4]
2022 — DANIMARCA

Ospedale universitario di Düsseldorf (UKD)
2020— GERMANIA

Ospedale di Osaka
2022 — GIAPPONE

Catena di approvvigionamento del vaccino per il [5]
2020 — GERMANIA

Sito web di riferimento dedicato alla salute
2019 — INDIA

Centro ospedaliero di Issoudun
2019 — FRANCIA

Centri sanitari
2022— SPAGNA

Gruppo di istituti sanitari SingHealth
2018 — SINGAPORE

Grossista di una farmacia a Rouen
2020 — FRANCIA

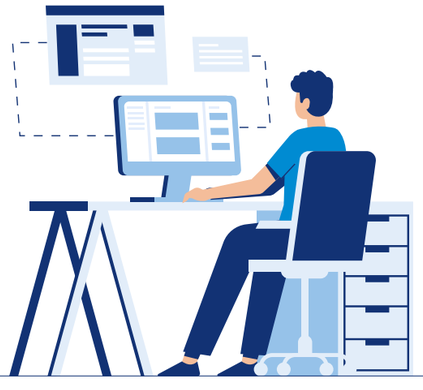
Gruppo ospedaliero Life Healthcare
2020 — SUDAFRICA

Ospedali Dharmais e Harapan Kita
2017 — INDONESIA

Compagnia di assicurazioni australiana
2022 — AUSTRALIA

1.1 Forti vincoli materiali: un parco informatico unico nel suo genere

La rete informatica rappresenta un elemento critico per il funzionamento dell'ospedale. Agisce come una vera e propria cinghia di trasmissione tra la rete operativa e il mondo esterno, ma deve fare i conti con un parco informatico particolare e con i problemi intrinseci del settore sanitario.



OBSOLESCENZA, CONVERGENZA DEL SISTEMA INFORMATICO, PERMEABILITÀ DELLA RETE: SONO TUTTI MALI CONDIVISI

Come in altri settori, in particolare quello industriale, anche sul fronte della sanità si registra l'obsolescenza del software. Pertanto, non è raro trovarsi di fronte a risorse informatiche di istituti sanitari la cui base software non si è evoluta per 20 anni. La lunga durata di vita, dovuta all'ammortamento delle apparecchiature mediche, fa sì che tali versioni di sistema non vengano mantenute e diventino obsolete, come Windows XP, minando la sicurezza di questi ambienti.

Si tratta di una vulnerabilità rafforzata dalla permeabilità delle reti, come nel caso della convergenza dei sistemi informatici nei gruppi ospedalieri francesi (GHT). Se interconnessi in modo non sicuro, aumentano il rischio di diffusione degli attacchi informatici.

Infine, anche la manutenzione da remoto, diffusa da tempo negli ospedali grazie agli interventi a distanza dei produttori di dispositivi medici, dei publisher o degli integratori di soluzioni applicative, presenta un rischio poiché l'accesso risulta più o meno sicuro.

GESTIONE SENSIBILE DEGLI EDIFICI OSPEDALIERI

Il concetto di sicurezza informatica richiama immediatamente alla mente il mondo dei sistemi informatici. Tuttavia, ora si rende necessario affrontare la questione in modo più ampio a causa della crescente interconnessione tra reti informatiche e reti operative.

Rientrano quindi nell'ambito di applicazione anche le infrastrutture tecniche (Gestione Tecnica Centralizzata [GTC], Gestione Tecnica degli Edifici [TGM]). Queste possono essere adottate per gestire la sicurezza antincendio, gli accessi, la videosorveglianza, il risparmio energetico e la qualità dell'aria interna in un edificio ospedaliero.

« Anche con il Sistema Generale di Riferimento per la Sicurezza (RGS)[6], è ancora difficile imporre requisiti minimi di sicurezza ai giganti dell'industria biomedica, ad esempio per i loro protocolli di manutenzione remota. In molti casi, aumentare la sicurezza a questo livello costituisce ancora un problema. »

CHARLES BLANC-ROLIN — RESPONSABILE DI PROGETTO PER LA SICUREZZA DIGITALE NEL SETTORE DELLA SANITÀ ELETTRONICA PAYS DE LA LOIRE

Questi diversi sistemi operativi, composti da automi di marchi e generazioni eterogenei, sono ancora troppo spesso collegati alla rete informatica in modo non sicuro e talvolta passano inosservati agli occhi dei responsabili della sicurezza dei sistemi informatici. Lo stesso dicasi per l'infrastruttura telefonica dell'organizzazione sanitaria, spesso trascurata. Tuttavia, se i telefoni IP di un ospedale venissero disabilitati da un attacco DDoS, le conseguenze sarebbero disastrose.

Questo problema è reso ancora più complesso dal fatto che la stessa struttura gestisce talvolta diversi edifici dislocati sul territorio.

FLASHER

UNO SCENARIO DI ATTACCO INFORMATICO

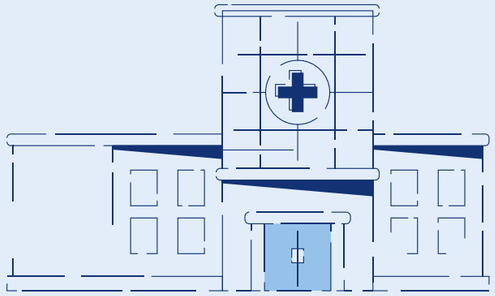
→ Un esempio concreto di attacco informatico alla sicurezza antincendio di un ospedale. —

DA NOTARE

LA QUALITÀ DELL'ARIA

è una questione di comfort nelle stanze dei pazienti ma è fondamentale in sala operatoria.

GESTIONE SENSIBILE DI EDIFICI OSPEDALIERI



- Collegamenti con altri servizi di emergenza
- Integrazione del sistema
- Convalida del sistema
- Sistemi commerciali e amministrativi
- Servizi ai pazienti
- Gestione dell'energia
- Riscaldamento, ventilazione e climatizzazione
- Protezione del perimetro
- Strutturazione e gestione dei cavi
- Comunicazioni voce e dati
- Convergenza IP
- Assistenza e manutenzione
- Televisione via antenna
- Video informativo per il pubblico/ cartelloni pubblicitari
- Servizi a bassissima tensione
- Impianto sonoro e annunci vocali
- Illuminazione
- Rilevazione e segnalazione incendi
- Controllo degli accessi
- Gestione di ascensori e scale mobili
- Gestione della localizzazione dei pazienti/delle risorse/ del flusso di lavoro clinico
- Sicurezza/CCTV e videosorveglianza digitale

PROTEZIONE DELLE APPARECCHIATURE BIOMEDICHE SOTTO I RIFLETTORI

Utilizzate per l'imaging medico o in biologia, gran parte delle apparecchiature biomediche sono collegate al sistema informatico (SI).

Ciò consente ad alcuni chirurghi, ad esempio, di essere assistiti in diretta da un collega dall'altra parte del mondo mediante una telecamera connessa in rete.

Oltre a migliorare le condizioni di cura dei pazienti, questo Internet degli oggetti medici (IoMT) favorisce la diagnosi e migliora la collaborazione tra gli operatori sanitari. Fornisce anche una risposta parziale al problema dei cosiddetti "deserti sanitari" nel caso della telemedicina, ma rappresenta un rischio per la sicurezza dell'ospedale.

Questi dispositivi, raramente presi di mira, sono spesso oggetto di danni collaterali negli attacchi informatici. Il loro punto debole consiste nell'essere collegati alla rete privi della necessaria protezione... E questo, mentre sono a diretto contatto con i pazienti.

Sviluppati da produttori industriali dotati di una cultura informatica limitata, spesso rappresentano un potenziale ricettacolo di infezioni.

ULTIME NOTIZIE

UNA PASSWORD CODIFICATA

→ Nell'ottobre 2022 è stata rivelata una vulnerabilità nelle apparecchiature mediche di laboratorio utilizzate per lo screening del cancro al collo dell'utero. La causa è da ricercarsi nelle informazioni di identificazione codificate nell'apparecchiatura.

20.000

« Gli istituti sanitari non sono sempre a conoscenza delle vulnerabilià e della obsolescenza, dei sistemi operativi su cui si basano questi dispositivi, ne del software e delle librerie integrate »

CHARLES BLANC-ROLIN — RESPONSABILE DI PROGETTO PER LA SICUREZZA DIGITALE NEL SETTORE DELLA SANITÀ ELETTRONICA PAYS DE LA LOIRE

UN SETTORE SOTTO PRESSIONE

La sicurezza informatica in ambito sanitario risente anche della generale mancanza di risorse nel settore. Negli ultimi anni i governo hanno messo a disposizione dei fondi. Inoltre, la sicurezza informatica in campo sanitario risente della mancanza di risorse e di esperti dedicati. —

« Ad oggi, concentriamo le nostre risorse umane nella sicurezza informatica sulla parte progettuale: non abbiamo risorse operative, nonostante ci sia una posizione di lavoro aperta a febbraio »

JACQUES LABIDURIE — RSSI CINICA UNIVERSITARIA DI LIMOGES

CIFRE SALIENTI

APPARECCHIATURE BIOMEDICHE

È il numero di apparecchiature biomediche distribuite nel Centro Ospedaliero Universitario (CHU) di Brest.

ULTIME NOTIZIE

UN ATTACCO DI TROPPO

A seguito dell'attacco al Centre Hospitalier Sud-Francilien[7] con sede a Corbeil-Essonnes alla fine di agosto 2022, il governo ha stanziato 20 milioni di euro per l'ANSSI al fine di potenziare il sostegno agli ospedali.

RIFLETTORI PUNTATI SUI DISPOSITIVI MEDICI CONNESSI

CON **JEAN-SYLVAIN CHAVANNE** — RSSI CLINICA UNIVERSITARIA DI BREST

→ Il marchio CE sui dispositivi medici. Questo segno di conformità, che viene apposto sui dispositivi medici, rappresenta una sfida importante per la sicurezza. In effetti, qualsiasi modifica strutturale metterebbe in discussione la marcatura, impedendo di eseguire gli aggiornamenti e le patch di sicurezza necessari su tali oggetti o dispositivi sanitari.

Questa situazione espone particolarmente i dispositivi medici a vulnerabilità di tipo Log4Shell e richiede l'uso di soluzioni di sicurezza perimetrale (partizionamento della rete, elementi di supervisione, ecc.).

Si tratta di un approccio che richiede competenze specifiche non necessariamente possedute dai team informatici. Si avverte quindi un'esigenza reale di formazione sulla sicurezza informatica e di collaborazione tra i dipartimenti IT, CISO e biomedico.

In caso contrario, persisteranno situazioni critiche, come nel caso delle apparecchiature di radioterapia ancora infettate dal worm Conficker nel 2022, a causa di una versione obsoleta di Windows. —

1.2 Trasformazione digitale nella sanità: un’accelerazione tardiva da sostenere

Negli ultimi anni abbiamo assistito all’innegabile ingresso della medicina elettronica nel settore sanitario, che ha generato una vera e propria rivoluzione digitale. I nuovi impieghi sono stati sperimentati nel delicato contesto della pandemia di Covid-19.



SVILUPPO DELLA TELEMEDICINA E DEL MONITORAGGIO REMOTO

Il crescente ricorso alla telemedicina e al monitoraggio remoto, in particolare nel contesto dell'ospedalizzazione a domicilio, amplia la potenziale superficie di attacco per le strutture sanitarie. Infatti, nel momento in cui un paziente riceve assistenza respiratoria a casa, il suo respiratore può diventare un nuovo punto di ingresso nel sistema informatico dell'ospedale.

ESTERNALIZZAZIONE DEI SERVIZI

Tra questi, il caso più emblematico è senza dubbio l'esternalizzazione della prenotazione di appuntamenti tramite piattaforme online, come Doctolib, che non manca di suscitare interrogativi e polemiche, in particolare per quanto riguarda la sicurezza dei dati scambiati.

« Il ricorso a servizi digitali in outsourcing, spesso meno sicuri, è molto diffuso e gli aggressori sono pronti a sfruttarlo. »

ANSSI — 2020[8]

LACUNE UMANE: LA SCARSA CONOSCENZA DEI RISCHI INFORMATICI

E poi c’è il fattore umano. Perché la trasformazione digitale nel settore sanitario si riflette sui dipendenti delle strutture assistenziali. Dipendenti che non condividono tutti gli stessi comportamenti di igiene digitale... Come riporta l'ANSSI nella sua guida all'igiene digitale: *« Ogni utente è un anello integrante della catena dei sistemi informatici. Per questo motivo, non appena entra a far parte del gruppo, è necessario informarlo sulle questioni di sicurezza, sulle regole da rispettare e sui comportamenti corretti da adottare in termini di sicurezza dei sistemi informatici, attraverso attività di sensibilizzazione e formazione. »*

26 gennaio 2022

Questa fragilità è aggravata dalla pratica del Bring Your Own Device (BYOD): alcuni medici, che si dividono tra studio privato e ospedale, utilizzano dispositivi non forniti dalla struttura ospedaliera e talvolta non conformi alle norme di sicurezza informatica. —

DATA CHIAVE

26 GENNAIO 2022 IN FRANCIA

Data in cui l'Autorità nazionale francese per la salute ha pubblicato le prime quattro linee guida per il monitoraggio medico a distanza per le seguenti patologie: diabete, insufficienza cardiaca cronica, insufficienza renale cronica e insufficienza respiratoria cronica.

Sono previsti ulteriori interventi volti ad ampliare questa base, con l'obiettivo di implementare il monitoraggio remoto in modo sostenibile e sicuro. —

1.3 Il caso particolare dei dati sanitari

Il settore sanitario è un obiettivo particolarmente ambito dai criminali informatici a causa della quantità di dati sanitari sensibili e vitali gestiti. Di cosa si tratta e quali sono i problemi che li riguardano?



QUAL È IL LEGAME TRA ACCESSO AI DATI, SALUTE E SICUREZZA ?

INTERVISTA

CHARLES BLANC-ROLIN
— RESPONSABILE DI PROGETTO PER LA SICUREZZA DIGITALE NEL SETTORE DELLA SANITÀ ELETTRONICA PAYS DE LA LOIRE

« I chirurghi preferiranno tornare alla medicina sul campo: ciò significa fare a meno dei dati piuttosto che affidarsi a dati potenzialmente errati o parziali. »



Come si definiscono i dati sulla salute?

C.BR — Il termine si riferisce a qualsiasi dato relativo alla salute del paziente, sia esso un referto operatorio, la citazione di un atto medico o un appuntamento con un professionista della salute.

In che modo l'accesso a questi dati sanitari è correlato alla sicurezza dei pazienti?

C.BR — La questione dei dati sensibili viene spesso affrontata in termini di **riservatezza**. La maggior parte delle persone teme la divulgazione dei codici delle carte di credito, ma non ha la minima idea delle conseguenze di un numero di previdenza sociale rubato. Tuttavia, soprattutto nel caso dei dati medici, le conseguenze possono essere gravi. L'**integrità** dei dati è una questione di sicurezza: se viene alterato un dosaggio o cancellata una segnalazione di allergia, la vita del paziente può essere a rischio. Anche la **disponibilità** è molto importante, ad esempio i chirurghi hanno bisogno di immagini per operare.

Perché la riservatezza dei dati è fondamentale nella sanità?

C.BR — Tornando all'esempio dei chirurghi, preferiranno tornare alla **medicina sul campo**: ciò significa fare a meno dei dati piuttosto che affidarsi a dati potenzialmente errati o parziali".

Quanto è diffusa l'inaccessibilità dei dati nel settore sanitario?

C.BR — Secondo il CERT-Santé, la metà degli incidenti segnalati nel 2021 ha riguardato « tutti o parte dei dati contenuti nelle applicazioni della struttura ». —

RIPARTIZIONE DEGLI INCIDENTI DI SICUREZZA IN BASE AL TIPO DI IMPATTO SUI DATI



Fonte: Osservatorio delle segnalazioni di incidenti di sicurezza nei sistemi informatici per il settore sanitario (2021)

SEMPRE PIÙ DATI DA PROTEGGERE

Un altro parametro da tenere in considerazione è la costante crescita del volume di dati generati dalle istituzioni sanitarie negli ultimi anni.

Ne è un esempio la crescente dematerializzazione nelle attività dei professionisti, con l'introduzione di servizi digitali di base come « Mon espace santé ». Disponibile dall'inizio del 2022, questo spazio consente al cittadino di consultare tutti i propri documenti sanitari (prescrizioni, risultati di esami, ecc.), di inserire informazioni personali sulla propria storia familiare e di scambiare dati con i professionisti della salute in modo sicuro.

La tecnologia digitale è diventata parte integrante dei processi aziendali degli operatori sanitari, come dimostra la proliferazione di strumenti diagnostici come Psychaclic[9] e l'obbligo in Francia, dal 1° marzo 2022, di rilasciare i certificati di morte per via elettronica.

Le banche dati diventano sempre più estese e la loro gestione e conformità sempre più complessa, tra obblighi di conservazione e diritto alla cancellazione[10] previsto dal GDPR...

UNA MINIERA (D'ORO) D'INFORMAZIONI

Sebbene i dati sanitari possano essere al centro di attacchi malevoli volti a destabilizzare le operazioni ospedaliere o a danneggiare un particolare individuo, i criminali informatici ne sono particolarmente interessati perché la loro vendita è molto redditizia. Esempio di giugno 2022: 1 miliardo di dati personali cinesi, comprese le informazioni mediche, sono stati messi in vendita per 10 Bitcoin (200.000 dollari)[11].

x30

CIFRE SALIENTI

VOLUME TOTALE DEI DATI SULLA SANITÀ ELETTRONICA

Nel 2016, l'Anap ha indicato che il volume totale dei dati sulla sanità elettronica raddoppiava ogni 73 giorni... Da allora sarebbe quindi aumentato di 30 volte.

CIFRE SALIENTI

Tra 50 e 250 €

CARTELLA CLINICA

Questo è il prezzo di rivendita di una singola cartella clinica[12]

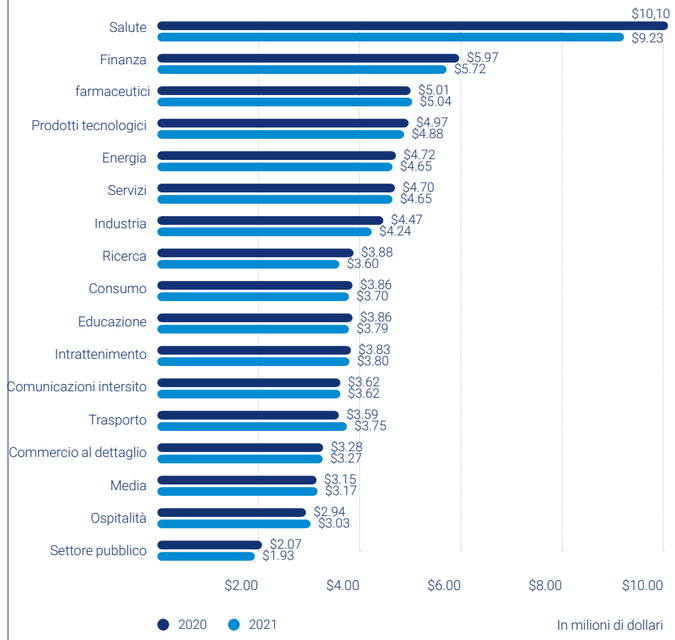
I dati sulla salute sono quindi una risorsa preziosa che interessa anche altri attori, come i GAFAM. Nel giugno 2022, il sito web investigativo The Markup[13] ha rivelato che le strutture sanitarie americane trasmettevano a Facebook informazioni sensibili (nome del medico, termini di ricerca o patologia) sui loro pazienti attraverso l'uso del "Meta Pixel".

PERDITE ONEROSE

Questo tipo di casi viene trattato sempre più spesso dai media e sta gradualmente sensibilizzando l'opinione pubblica. Anche la reputazione delle aziende vittime è messa a dura prova, come nel caso di Shields, un gruppo statunitense di diagnostica per immagini e chirurgia ambulatoriale che ha subito un furto di dati a danno di quasi 2 milioni di persone.

Ma il prezzo da pagare è altrettanto netto e significativo. Secondo un rapporto di IBM[14], il costo medio di una violazione dei dati per una struttura sanitaria è di oltre 10 milioni di dollari. —

COSTO MEDIO DI UNA VIOLAZIONE DEI DATI PER MERCATO VERTICALE, DOMINATO DALLA SANITÀ



1,5 M€

CIFRE SALIENTI

AMMENDE

1,5 milioni di euro Questo è l'importo dell'ammenda inflitta a Dedalus Biologie per falle nella sicurezza che "hanno portato alla fuga di dati medici di quasi 500.000 persone" (CNIL).

PER APPROFONDIRE

CINQUE WEBINAR DEDICATI

→ Seguite la nostra serie di 5 webinar[15] per saperne di più sull'ipersensibilità degli ospedali agli attacchi informatici.



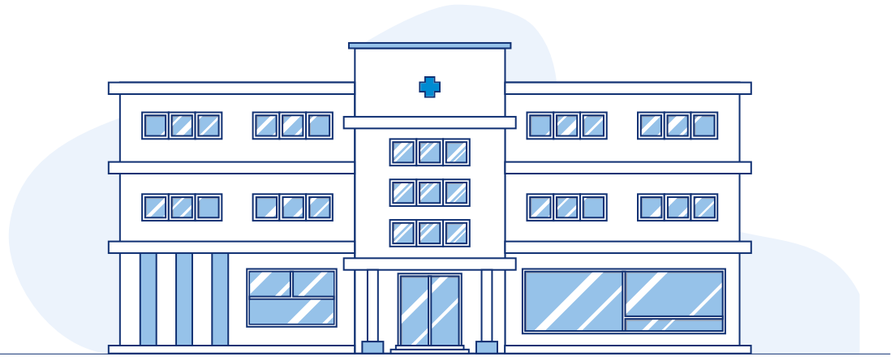
02.

Anatomia di una minaccia polimorfa con punti di ingresso multipli

Quali sono i vettori utilizzati per introdurre le minacce informatiche nelle strutture sanitarie? Quali sono i diversi tipi di attacco subiti? Si tratta sempre di episodi mirati? I criminali informatici non mancano d'ingegno quando si tratta di attaccare il settore medico, ma a volte l'incidente di sicurezza è dovuto a un malfunzionamento e non a un attacco informatico. Le conseguenze però sono altrettanto disastrose.

2.1 In che modo i cybercriminali si introducono nel sistema informatico delle strutture sanitarie?

Purtroppo, i punti d'ingresso nelle strutture sanitarie per le minacce informatiche sono numerosi e si possono raggruppare in quattro vettori.



1. ELEMENTO UMANO

Gli attacchi informatici si servono, o prendono di mira, uno o più individu (medici, infermieri, agenti, amministratori e persino gli stessi pazienti).
Nel 2020, un grossista di Rouen, fornitore delle farmacie della regione, ha effettuato un ordine di 6,6 milioni di euro per gel e mascherine a una società che alla fine si è rivelata un fantasma. Un drammatico esempio di "truffa del presidente"[16] nel teso contesto della pandemia di Covid-19.

2. SOFTWARE

Gli attacchi informatici a livello di software sono quelli che sfruttano una debolezza, una falla o un'obsolescenza del software installato su apparecchiature informatiche o dispositivi medici computerizzati.
Nel 2020, una controversia ha portato alla luce una serie di falle di sicurezza in una soluzione del gruppo Dedalus, specializzato in software sanitari. Uno di questi consentiva l'accesso ai ticket aperti dai clienti di ospedali e laboratori dell'azienda, che potevano contenere identificativi e password di amministrazione remota.

3. RETE

Come suggerisce il nome, un attacco informatico di rete indica qualsiasi attacco informatico che passa attraverso la rete dell'ospedale.
I servizi di Assistance Publique - Hôpitaux de Paris (AP-HP) sono stati presi di mira nel 2020 da un attacco DDoS (Network Denial of Service) a due dei suoi siti Internet. La conseguenza è stata l'interruzione dell'accesso alla posta elettronica e alle applicazioni per i dipendenti.

4. DISPOSITIVI FISICI

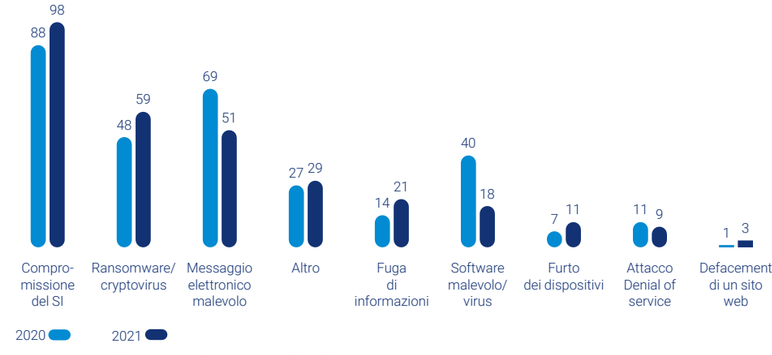
Gli attacchi informatici fisici mirano specificamente alla dimensione materiale delle apparecchiature mediche, informatiche o operative.
Nel 2019, alcuni ricercatori israeliani hanno simulato un attacco *man-in-the-middle* introducendo un Raspberry Pi in un ospedale. In questo modo sono riusciti a intercettare i dati di imaging medico trasmessi tramite il protocollo DICOM e a dimostrare che potevano essere alterati.

Indipendentemente dal vettore di attacco scelto dal criminale informatico, la « carica virale » più comune nel settore sanitario è oggi il ransomware. Ma le strutture sanitarie sono anche particolarmente esposte agli attacchi di tipo distributed denial of service e al furto di dati. —

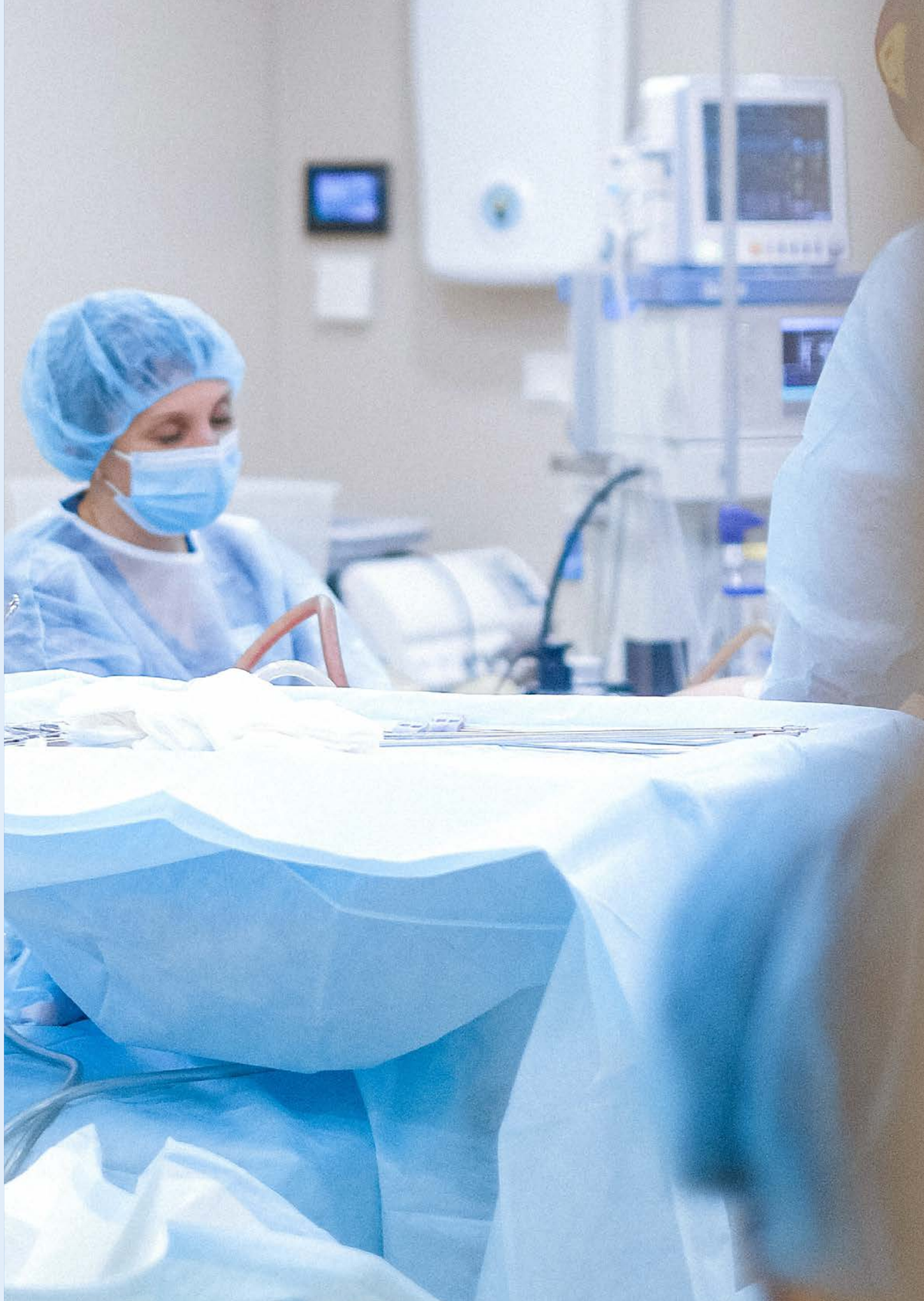
« Fatture false, richieste di rinnovo password fraudolente, reclami di pazienti immaginari... la qualità delle campagne di phishing che intercettiamo è in aumento. Alcuni si spingono addirittura a usurpare l'identità dell'Ospedale Universitario di Brest. Ma l'aumento più evidente riguarda i broker di accesso iniziale (IAB). Questi cybercriminali sono specializzati nella ricerca di ID utenti da rivendere. »

JEAN-SYLVAIN CHAVANNE — RSSI CLINICA UNIVERSITARIA DI BREST

NUMERO DI INCIDENTI PER TIPO DI ORIGINE



Fonte: report IBM Security, Cost of Data Breach (2022)



2.2 L'intero percorso assistenziale al centro del mirino

Ospedali e cliniche sono l'obiettivo principale degli attacchi informatici nel settore sanitario. Ma non sono i soli. Anche i laboratori, i fornitori e persino i pazienti sono nel mirino dei criminali informatici.



Nel 2022 sono già stati colpiti diversi ospedali americani (Baton Rouge General in Louisiana, Jack Huston Memorial a Phoenix e Southwest Health Center in Wisconsin), oltre che in Francia (Vitry-le-François, Saint-Dizier, Charleville-Mézières, Corbeil-Essonnes) e Spagna (Barcellona).

Sono stati presi di mira anche i laboratori, in particolare per i dati medico-amministrativi inseriti nei software di biologia medica come Mega Bus[18].

In tempi più recenti, i criminali informatici hanno ulteriormente ampliato la loro gamma di obiettivi. Da un lato, si rivolgono ai vari fornitori per ottenere l'apertura delle porte virtuali dei sistemi informatici ospedalieri; dall'altro, non esitano ad attaccare i pazienti stessi, che vengono ricattati in seguito al furto dei dati sanitari e/o personali. —

QUANDO I CYBERCRIMINALI PRENDONO DI MIRA I PAZIENTI

→ Nel 2020, i pazienti di una ventina di centri di psicoterapia finlandesi, gestiti dalla società Vastaamo, hanno avuto la spiacevole sorpresa di ricevere una richiesta di riscatto di 500 euro da pagare in Bitcoin, pena la divulgazione dei dati raccolti durante le loro sedute. Un caso di doppia estorsione[19] che ha generato migliaia di denunce alle autorità. —

QUANDO I CRIMINALI INFORMATICI PRENDONO DI MIRA LA CATENA LOGISTICA

→ Nel 2020, i fornitori specializzati nella catena del freddo per i vaccini Covid-19 sono stati presi di mira da campagne di phishing. L'obiettivo era quello di reperire informazioni sensibili sulle modalità di trasporto e distribuzione. Una campagna che ha le caratteristiche di un attacco a livello statale, secondo i ricercatori di sicurezza informatica di IBM. —

2.3 Questo non è un attacco informatico

Sebbene si debbano adottare tutte le misure necessarie per proteggersi dagli attacchi informatici, non bisogna dimenticare che anche gli incidenti non malevoli possono comportare gravi conseguenze per il sistema sanitario.



In un ambiente ospedaliero vulnerabile e fragile, un incidente informatico può effettivamente trasformarsi in un incidente di sicurezza. Un esempio è quello del giugno 2022 presso l'ospedale universitario di Nantes, dove un grave guasto, causato dall'antivirus installato, ha colpito tutte le postazioni di lavoro con Windows 7, comprese le apparecchiature biomediche, rendendole inutilizzabili. —

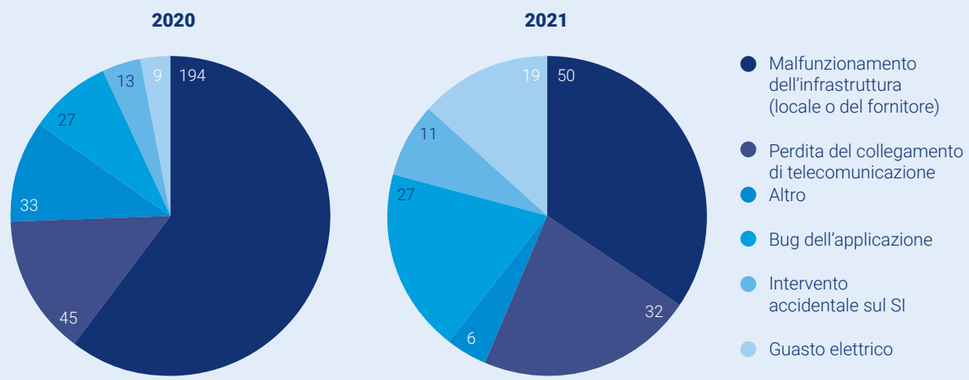
48%

CIFRE SALIENTI

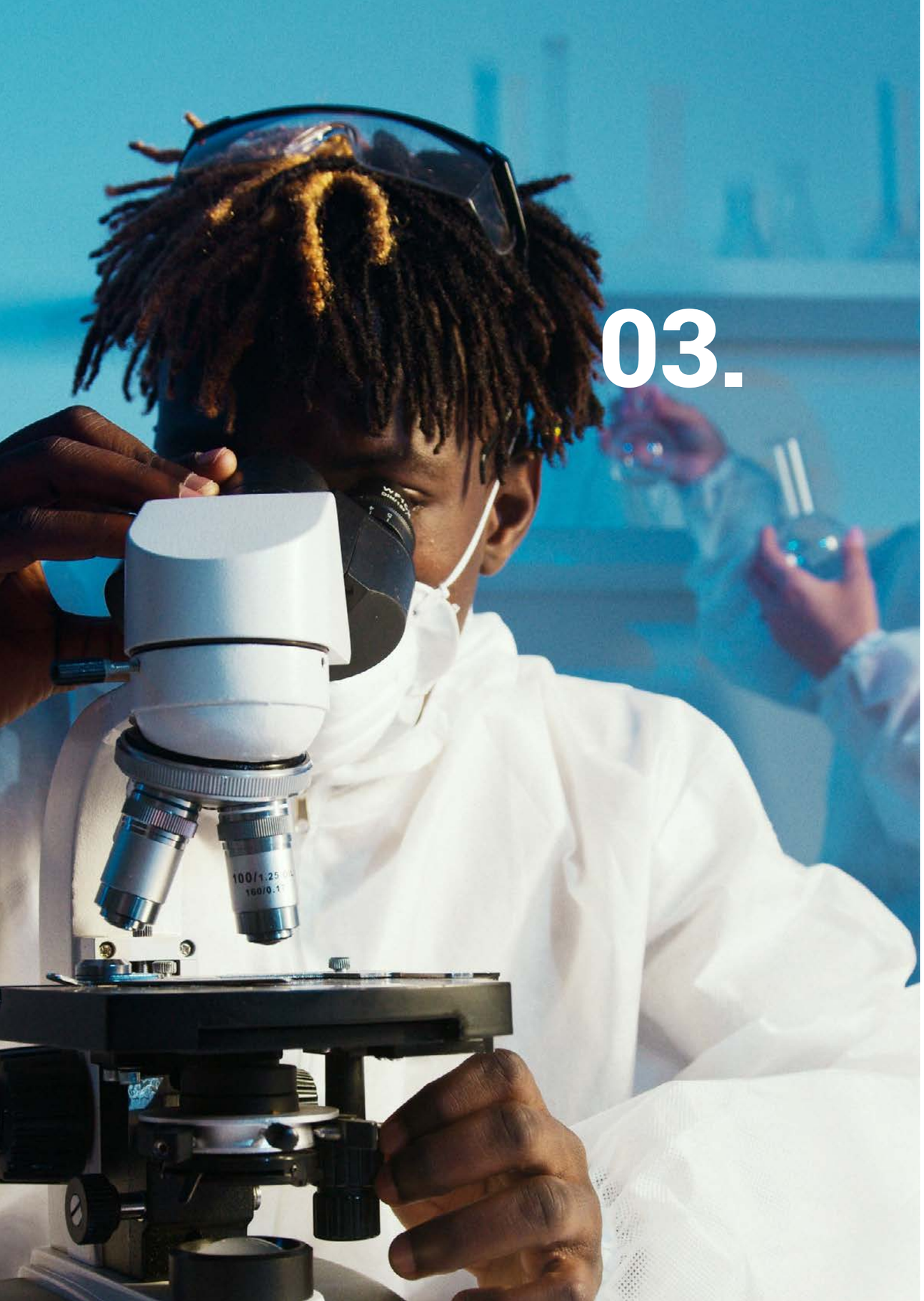
NON MALEVOLE

Il 48 % delle segnalazioni pervenute alll'Observatoire CERT-Santé[20] non sono di origine malevola

RIPARTIZIONE DEGLI INCIDENTI DI ORIGINE NON MALEVOLA



Fonte: Osservatorio delle segnalazioni di incidenti di sicurezza nei sistemi informatici per il settore sanitario (2021)



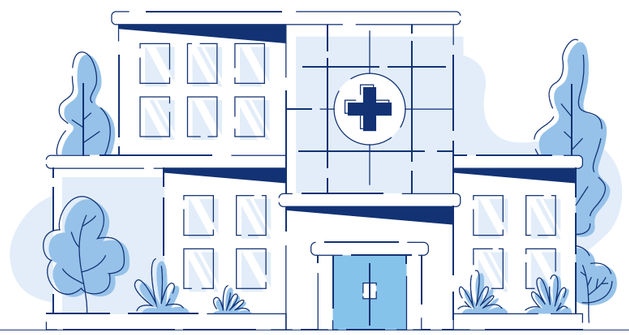
03.

Quali rimedi adottare per rendere più sicuro il settore sanitario?

Come proteggersi dagli attacchi informatici? Che cosa dice la legislazione attuale al riguardo? Che tipo di assistenza possono fornire le autorità pubbliche in merito? Questo processo può risultare complesso, ma è fondamentale per garantire una protezione adeguata.

3.1 Quali sono le misure per proteggere le infrastrutture sanitarie?

Le infrastrutture delle organizzazioni sanitarie sono di natura vitale. Le prestazioni e la disponibilità delle reti informatiche nei nostri sistemi sanitari sono estremamente importanti, poiché la vita dei pazienti dipende spesso dalle informazioni che vengono scambiate.



FASE 1: AUDIT E ANALISI DEI RISCHI

La prima fase di qualsiasi approccio alla protezione informatica deve riguardare la conoscenza dei propri sistemi. Qui, l'obiettivo è identificare gli asset più sensibili per ridurre la superficie di attacco definendo una politica di sicurezza.

« Questa mappatura permette di riconoscere e classificare le componenti dei sistemi informatici e operativi delle strutture sanitarie secondo vari criteri come l'obsolescenza o la criticità. »

STÉPHANE PREVOST — PRODUCT MARKETING MANAGER, STORMSHIELD

FASE 2: IMPLEMENTAZIONE DI SOLUZIONI DI PROTEZIONE ADEGUATE

Queste soluzioni, offerte da apparecchiature come quelle proposte da Stormshield, coprono perimetri diversi.

Protezione delle reti

Tra le caratteristiche necessarie per proteggere le reti informatiche degli ospedali figurano:

- La segmentazione della rete,
- Il controllo degli accessi, la gestione della telemanutenzione e altri accessi remoti,
- La protezione delle comunicazioni,
- L'autenticazione a doppio fattore,
- Politiche di filtro per utente,
- Protezione dei protocolli di comunicazione delle apparecchiature biomediche (prevenzione delle intrusioni) - IPS OT).

Protezione delle postazioni di lavoro

Per poter garantire una maggiore protezione dei propri terminali, le strutture sanitarie devono mettere in atto:

- L'autenticazione a doppio fattore,
- La prevenzione delle intrusioni nelle postazioni di lavoro (HIPS) mediante analisi comportamentale,
- La gestione di dispositivi esterni (fino all'implementazione di stazioni bianche).

« In alcuni casi ho implementato soluzioni di bloccaggio fisico per le porte USB in collaborazione con il responsabile biomedico. In questo modo si evita, ad esempio, che qualcuno utilizzi l'ecografo per caricare il proprio smartphone, rischiando di compromettere il dispositivo. »

CHARLES BLANC-ROLIN — RESPONSABILE DI PROGETTO PER LA SICUREZZA DIGITALE NEL SETTORE DELLA SANITÀ ELETTRONICA PAYS DE LA LOIRE

PSEUDONIMIZZAZIONE O REVERSIBILITÀ DELL'ANONIMATO

CON **JEAN-SYLVAIN CHAVANNE** — RSSI CLINICA UNIVERSITARIA DI BREST

→ ***« Una delle particolarità del settore sanitario è che alcuni dati sensibili non possono essere resi completamente anonimi: ad esempio, una struttura assistenziale potrebbe avere la necessità di rintracciare un paziente che si è sottoposto a un determinato trattamento. Per questo motivo, i dati dei pazienti sono divisi in due database per consentire una nuova identificazione, qualora fosse necessario. » —***

Anche l'utilizzo di password robuste sono una pratica necessaria per evitare di diventare il bersaglio di azioni malevoli provenienti da internet.

Infine, migliorare il monitoraggio delle patch è essenziale per aumentare il livello di sicurezza delle postazioni di lavoro all'interno delle strutture sanitarie. A tal fine, occorre controllare i componenti esposti e aggiornarli quando viene resa disponibile una patch, trattando le vulnerabilità critiche come una priorità. Durante l'attacco informatico all'ospedale di Düsseldorf, la tragedia poteva essere evitata: una patch per la vulnerabilità sfruttata era stata resa disponibile sette mesi prima.

Protezione dei dati

Se la prima azione a questo livello è quella di vietare l'invio di qualsiasi file di pazienti via e-mail in chiaro, sono necessarie altre misure. Occorre garantire:

- Una cartella clinica crittografata con diverse chiavi di accesso,
- Crittografia end-to-end delle informazioni, in particolare quando vengono estratte dal SI per essere trasmesse a un altro ospedale (come parte di un percorso di cura coordinato, ad esempio),
- Un processo di anonimizzazione e pseudonimizzazione per un'elaborazione efficiente dei dati.



FASE 3: AUDITING E MIGLIORAMENTO CONTINUO

Il passo successivo consiste nel monitorare la conformità e verificare eventuali scostamenti dalla politica di sicurezza. A tal riguardo, occorre in particolare:

- analizzare regolarmente i log delle proprie apparecchiature perimetrali,
- eseguire audit di sicurezza o test di penetrazione,
- riavviare una fase di pianificazione per implementare azioni correttive.

«L'interesse dimostrato dalle organizzazioni sanitarie nei confronti dei SOC gestiti conferma l'interesse nella condivisione delle risorse a fronte delle difficoltà di reclutamento per queste figure (mancanza di profili, di fondi, ecc.). »

JACKY GRISEY — SECURITY OPERATIONS MANAGER DEDICATO AL SETTORE SALUTE, ADVENS

« L'installazione di una patch per una vulnerabilità critica su un componente esposto in Internet non garantisce la protezione da un precedente sfruttamento. È necessario analizzarne i log per verificare che non sia stato sfruttato su un altro componente e, in caso di dubbio, rinnovare tutti gli account. »

STÉPHANE PRÉVOST — PRODUCT MARKETING MANAGER STORMSHIELD

IMPEGNARSI IN ATTIVITÀ DI SENSIBILIZZAZIONE E FORMAZIONE

Se si intende migliorare il livello di protezione nelle strutture sanitarie, occorre implementare una campagna di sensibilizzazione. Tale campagna dovrebbe essere inizialmente rivolta agli operatori del settore, come nel caso del Centre-Val de Loire[22] attraverso lo sviluppo di **piattaforme di sensibilizzazione e formazione** per le strutture sanitarie e medico-sociali. Ma queste azioni di comunicazione e sensibilizzazione dovrebbero essere rivolte anche ai pazienti e ai produttori di dispositivi medici, con un tono adatto a ciascun destinatario.

« Gli ambienti industriali devono essere formati in materia di sicurezza informatica, visto che molti gestiscono ancora le tecnologie informatiche come 30 anni fa. Inoltre, le facoltà di medicina dovrebbero proporre anche dei corsi di sicurezza informatica, e non solo sulla protezione dei dati, come avviene attualmente. »

JACQUES LABIDURIE — RSSI CINICA UNIVERSITARIA DI LIMOGES

Alcuni soggetti non esitano a spingersi oltre per responsabilizzare gli utenti. Il centro ospedaliero di Calais registra attualmente le sessioni sui suoi server[23], considerati critici. Questa nuova politica viene applicata anche ai suoi fornitori, coinvolgendone circa il 40%.

Tuttavia, in questo settore, già sottoposto a forti pressioni, è indispensabile **che la sicurezza informatica sia coerente con le pratiche aziendali:** ad esempio, non è opportuno chiedere ripetutamente di inserire una password di 12 caratteri in una situazione di emergenza. —

COME RENDERE PIÙ SICURI I DISPOSITIVI MEDICI SENZA COMPROMETTERE IL LORO MARCHIO CE?

→ La principale soluzione di protezione delle reti consiste nel suddividerle e isolarle dal resto del sistema informatico tramite micro-segmentazione. Pertanto, in caso di necessità di uno scambio di flussi, occorre impostare un filtraggio molto accurato e, se possibile, prevedere il rilevamento di anomalie su questi stessi flussi, ad esempio tramite una sonda IDS. —

« Nelle nostre attività di sensibilizzazione, la contestualizzazione è molto importante. L'incontro preliminare con il responsabile dell'unità permette, ad esempio, di capire come funziona la struttura e di acquisire esempi reali, come quello di lasciare la scheda in posizione durante le varie manipolazioni radio. I reparti amministrativi, di acquisto, di ricerca clinica, hanno tutti un vocabolario specifico che va padroneggiato per essere efficace. »

CORALIE ACHARD-TORTUL — DPO CLINICA UNIVERSITARIA DI LIMOGES

PROTEZIONE INFORMATICA DELLE STRUTTURE SANITARIE CON STORMSHIELD

SICUREZZA INFORMATICA E SALUTE

→ Stormshield contribuisce allo sviluppo di una sicurezza informatica affidabile a livello europeo. Tutte le linee di prodotti agiscono costantemente secondo determinati criteri di qualificazione e certificazione della sicurezza con le autorità europee competenti.

STORMSHIELD NETWORK SECURITY PER LA PROTEZIONE DELLA RETE

Poiché in questo determinato settore la disponibilità dei servizi è fondamentale, la gamma di firewall Stormshield Network Security (SNS) ne garantisce la continuità e la fruibilità attraverso la segmentazione della rete, la funzionalità di bypass e la prevenzione delle intrusioni. Per proteggere i dati dei pazienti durante gli scambi, questi firewall proteggono l'accesso remoto tramite reti private virtuali (VPN).

STORMSHIELD DATA SECURITY PER LA PROTEZIONE DEI DATI

La protezione dei dati sanitari sta diventando una questione sempre più centrale e vitale per le strutture assistenziali. Grazie alla crittografia end-to-end, Stormshield Data Security (SDS) preserva l'integrità e la riservatezza delle informazioni sensibili, soprattutto quando i dati vengono estrapolati dal sistema informatico.

STORMSHIELD ENDPOINT SECURITY PER LA PROTEZIONE DEI SERVER E DELLE POSTAZIONI DI LAVORO

Per supportare le trasformazioni del settore sanitario e i nuovi utilizzi professionali, la soluzione Stormshield Endpoint Security (SES) offre una protezione autonoma ai terminali, in grado di modificare dinamicamente i livelli di sicurezza in base all'ambiente in cui si trovano.

STORMSHIELD LOG SUPERVISOR PER LA VISIBILITÀ DEGLI EVENTI DI RETE

Con lo strumento Stormshield Log Supervisor (SLS) è possibile visualizzare a colpo d'occhio lo stato della rete IT e accedere ai registri degli eventi. Una soluzione ideale per ottimizzare le vostre attività d ricerca e di risposta agli incidenti.

QUALI OBBLIGHI NORMATIVI VIGONO PER LE ORGANIZZAZIONI SANITARIE?



NEGLI STATI UNITI

→ Si applica lo standard americano HIPAA (Health Insurance Portability and Accountability Act) e la sua componente sui dati sanitari personali chiamata ePHI (electronic Protected Health Information).

A LIVELLO EUROPEO

→ La direttiva NIS 2 elenca una serie di obblighi per gli operatori di servizi essenziali (OSE), che comprendono la maggior parte delle organizzazioni sanitarie con un servizio di emergenza medica. Tra questi, rientra l'obbligo di segnalare gli incidenti di sicurezza. Come tutte le organizzazioni che operano nell'Unione Europea, anche queste devono rispettare il GDPR.

IN FRANCIA

→ Queste strutture sensibili, talvolta classificate come operatori di importanza vitale (OIV), sono anche soggette al Codice di Sanità Pubblica, all'istruzione interministeriale n. 901 e al PGSSI-S, di cui dal mese di aprile è disponibile il primo documento esecutivo, lo standard di identificazione elettronica[24]. Quest'ultimo impone alle istituzioni e ai publisher dei vincoli in termini di identificazione dei pazienti e dei professionisti, al fine di rafforzare la sicurezza dell'accesso. Inoltre, le strutture sanitarie possono fare riferimento alla guida alle buone pratiche pubblicata dall'ANSSI.

3.2 Una presa di coscienza e impegno sostenuti dall'azione pubblica

Tuttavia, la vulnerabilità delle strutture sanitarie non è una novità ed è fonte di preoccupazione per i professionisti da oltre un decennio. Al riguardo, esistono già iniziative, sia a livello europeo che nazionale.



A LIVELLO EUROPEO

Di fronte all'emergere di una vera e propria economia dei dati, l'Unione europea si sta strutturando con tutta una serie di testi in fase di studio o già in vigore:

- Regolamento generale sulla protezione dei dati (GDPR) di carattere personale.
- Regolamento sul quadro globale per l'utilizzo dei dati a livello UE (Data Governance Act [DGA]).
- Regolamento sui servizi digitali (Digital Services Act [DSA]).
- Regolamento sui mercati digitali (Digital Markets Act [DMA]).

Il progetto di regolamento sullo Spazio europeo dei dati sanitari (EHDS)[25] è il primo testo verticale del corpus, ossia il primo testo che propone un quadro di condivisione dei dati per un particolare settore. Pubblicato all'inizio di maggio 2022, è stato descritto come « *un nuovo inizio per la politica sanitaria digitale dell'UE* » [26] da Margarítis Schinás, vicepresidente della Commissione europea. —

DATA CHIAVE

Luglio 2016

Già nel luglio 2016, l'Europa ha affrontato la questione informatica attraverso la Direttiva NIS e l'identificazione degli Operatori di Servizi Essenziali (OSE) nel settore sanitario (insieme ad altri settori come energia, trasporti, acqua, banche e infrastrutture digitali). L'obiettivo: proteggere i loro sistemi informatici critici.

« Questi interventi (DSA e DMA), che affrontano il tema in modo trasversale e sistemico, sono in linea con i vari testi, tra cui il GDPR, la direttiva NIS e il Data Act. Essi mirano a favorire l'innovazione, a tutelare i residenti europei e a stabilire l'autorità strategica dell'Unione europea. »

RAYNA STAMBOLIYSKA — ESPERTA DI DIPLOMAZIA DIGITALE, SPECIALISTA IN SICUREZZA INFORMATICA E MEMBRO INDIPENDENTE DEL GRUPPO DI LAVORO SULLE MINACCE EMERGENTI E FUTURE DELL'ENISA

INTERVISTA INCROCIATA

QUESTO REGOLAMENTO EUROPEO SUI DATI SANITARI È ADEGUATO ALLE SFIDE?

Questo documento risponde alle sfide che ci troviamo ad affrontare oggi. Tra 5-10 anni dovrà essere aggiornato per rispondere alle nuove minacce emerse con le tecnologie di decentralizzazione, il Web 3.0 e così via, ma in questa fase **è da considerarsi una valida integrazione al GDPR e alla direttiva NIS.**

Si tratta quindi di una tappa importante nella nostra storia comune, sebbene sembri che sia stata la pandemia COVID-19 a dare il via a questa rinascita. È in questo contesto che la rete eHealth Network, che riunisce i rappresentanti degli Stati membri nel campo della salute digitale e alla quale partecipo come osservatore, ha fornito un primo esempio di cooperazione europea: una serie di strumenti comuni per lo sviluppo di applicazioni mobili di monitoraggio dei contatti.

La pandemia ha evidenziato la necessità di regolamentare ulteriormente il settore per garantire una reale protezione dei dati sanitari. I decisori europei lo hanno ben compreso e questo regolamento ne è la prova. **Con esso si propone uno schema volto a garantire la condivisione delle informazioni, a rafforzare gli obblighi di segnalazione degli incidenti e di interoperabilità.**
Ne dovrebbero derivare anche diversi standard di certificazione (per le cartelle cliniche elettroniche, le app di assistenza sanitaria, ecc.).

Questo documento, incrociato con altre normative, è tra i più avanzati: si può addirittura parlare di un testo unico per quanto riguarda i capitoli sull'uso primario e secondario dei dati. Quest'ultimo apre la strada ad un utilizzo nella ricerca per orientare le politiche di salute pubblica e migliorare il follow-up dei pazienti. —



DAMIAN KLIMAS — ASSOCIATO E OSSERVATORE DI DOTLAW DELLA RETE EHEALTH NETWORK

Sì abbastanza

Dal punto di vista settoriale, il testo si basa sul quadro orizzontale stabilito dalla direttiva NIS2 per quanto riguarda le questioni di sicurezza. Tuttavia, l'articolo 50 fornisce elementi specifici sulla sicurezza degli accessi.

L'obiettivo di questo testo è quello di proporre un quadro di condivisione dei dati che avrà un forte impatto sulle modalità di utilizzo degli stessi in Europa. Gli obiettivi sono significativi: armonizzare il concetto di utilizzo secondario dei dati sanitari tra i diversi Stati e implementare una solida infrastruttura tecnologica per consentire l'utilizzo di tali dati.



RAYNA STAMBOLIYSKA — ESPERTA DI DIPLOMAZIA DIGITALE, SPECIALISTA IN SICUREZZA INFORMATICA E MEMBRO INDIPENDENTE DEL GRUPPO DI LAVORO SULLE MINACCE EMERGENTI E FUTURE DELL'ENISA

In questa fase, il documento solleva questioni relative al controllo dei dati nel contesto di tale condivisione. **Dal canto nostro, possiamo lamentare la creazione di un diritto di accesso incoerente con quello già definito dal GDPR**, che potrebbe portare a situazioni di incertezza giuridica. Anche il tema del controllo individuale è affrontato in modo insufficiente: l'organo di governo dell'EHDS non include, ad esempio, un rappresentante dei pazienti.

Infine, **allo stato attuale, la questione dell'implementazione di tale spazio non è molto chiara:** si potrebbe supporre di dover creare un'unica enorme banca dati, mentre in realtà il testo prevede l'interconnessione di diverse banche dati decentralizzate.

Questa architettura solleva tutta una serie di questioni (governance, percorsi utente, formati dei dati, procedure di ricorso, ecc.) le cui risposte non possono e non devono essere principalmente tecnologiche. —

ASPETTI DA CONSIDERARE

→ Il regolamento prevede tuttavia alcuni requisiti tecnici di sicurezza su questioni pratiche di accesso e tracciabilità (articolo 50 del CF).

No affatto

132

CIFRE SALIENTI

Sono 132 le strutture coinvolte nel percorso di sicurezza informatica del piano France Relance.

CHARLOTTE DRAPEAU — RESPONSABILE DELL'UFFICIO SALUTE E SOCIETÀ, ANSSI, 2022[29]

A LIVELLO NAZIONALE

Nell'aprile 2019, il governo francese ha presentato una tabella di marcia per« *accelerare il passaggio al digitale nella sanità* »[27] nel contesto di un piano più ampio, denominato *Ma Santé 2022*. A tale iniziativa ha fatto seguito la pubblicazione di una dottrina tecnica. Quest'ultima, sottoposta a revisione annuale, definisce un quadro di riferimento e propone un percorso per tutti gli operatori della sanità elettronica in Francia.

La componente digitale del piano sanitario Ségur si inserisce in questo quadro di riferimento e mira ad accelerare il processo di trasformazione. Attraverso di esso, il Ministero della Solidarietà e della Salute ha sbloccato investimenti per 2 miliardi di euro. Tra gli obiettivi vi sono il supporto alla transizione digitale delle strutture sanitarie e medico-sociali, la modernizzazione dei sistemi informatici esistenti e il consolidamento dell'interoperabilità, della convergenza e della sicurezza. Il budget include 350 milioni di euro specificamente dedicati alla sicurezza informatica di queste strutture.

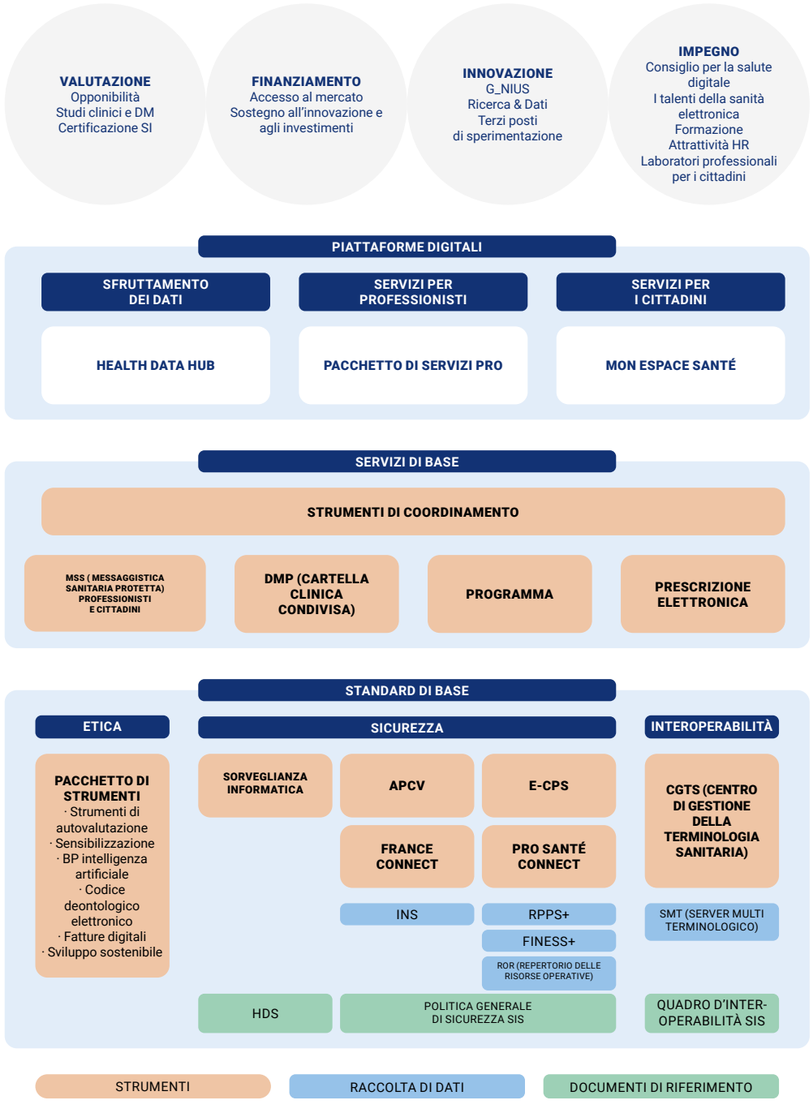
Da parte sua, l'ANSSI ha ricevuto una sovvenzione di 136 milioni di euro nell'ambito del piano di rilancio della Francia per il potenziamento della sicurezza informatica nazionale. Di questa somma, 25 milioni di euro saranno destinati alla sicurezza informatica delle strutture sanitarie attraverso lo svolgimento di audit nell'ambito di programmi di sicurezza informatica. —

« I principali attacchi informatici che si sono verificati negli ultimi anni hanno evidenziato le lacune in termini tecnici e organizzativi dei sistemi informatici delle organizzazioni sanitarie. Si è delineata una presa di coscienza, anche ai più alti livelli di governo. »

JACKY GRISEY — SECURITY OPERATIONS MANAGER DEDICATO AL SETTORE SALUTE, ADVENS

LE COMPONENTI DEL QUADRO DI RIFERIMENTO FORNITO DALLO STATO FRANCESE

Lo schema riassume le componenti del quadro di riferimento per la sanità elettronica in Francia, e va letto dal basso verso l'alto: prima gli standard di base, poi i servizi di base e infine le piattaforme digitali.



Fonte: Dottrina della salute digitale, Ministero della Solidarietà e della Salute (2021)



04.

E in futuro?

Come sarà il mondo della sanità nei prossimi anni? Che impatto avrà sulla sicurezza informatica? Uno studio di previsione che sottolinea la portata del compito.

4.1 Un continuum di assistenza a livello europeo

La condivisione dei dati sanitari tra operatori, ricercatori e industria dovrebbe favorire una migliore assistenza ai cittadini. Questa è la promessa dell' European Health Data Space (EHDS), presentato dalla Commissione europea come futuro spazio europeo dei dati sanitari. A condizione che interoperabilità sia sinonimo di sicurezza.





Se il regolamento sull'EHDS sarà adottato senza modifiche sostanziali, il programma MyHealth@EU diventerà obbligatorio nell'Unione europea e consentirà a ogni residente di beneficiare della continuità delle cure in ogni Stato membro. Il servizio è già attivo in Francia attraverso il portale Sesali.fr dal luglio 2021[30].

Nei prossimi anni, quindi, l'interoperabilità e la sicurezza dei dati dovranno continuare a essere al centro delle politiche sanitarie europee. —

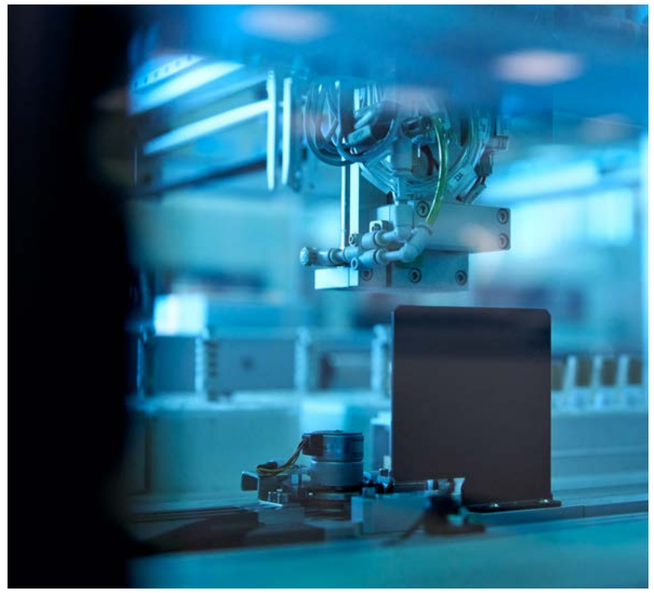
« L'adozione dell'EHDS accelererà l'implementazione di MyHealth@EU. Ciò significa che entro il 2025 le strutture sanitarie di tutti gli Stati membri e della Norvegia avranno un accesso facile e sicuro ai dati relativi alle allergie, alle prescrizioni e alla storia clinica di qualsiasi paziente, nella sua lingua, anche se vive in un altro stato europeo. »

DAMIAN KLIMAS — ASSOCIATO E OSSERVATORE DI DOTLAW DELLA RETE EHEALTH NETWORK

4.2 Medicina preventiva, gestione ospedaliera basata sui dati: le promesse (e le sfide) dei Big Data in campo medico

Mentre la raccolta di dati medici è un compito relativamente facile, elaborarli e analizzarli è più complesso. Dietro il concetto di Big Data medico, le promesse di una medicina personalizzata e predittiva sono soggette a requisiti di sicurezza informatica.





Tali dimensioni saranno tanto più strategiche considerando le promettenti prospettive di sfruttamento di grandi quantità di dati. Molte aziende utilizzano il machine learning per fornire strumenti diagnostici agli operatori sanitari. Tra queste, la start-up lituana Ligence[31] fornisce un software di analisi degli ecocardiogrammi per i cardiologi. Si tratta di soluzioni che integrano la questione della sicurezza informatica nella loro progettazione.

« Se vogliamo individuare le patologie in futuro piuttosto che curarle, dobbiamo assolutamente affrontare le questioni relative alla governance dei dati sanitari e quindi alle misure di sicurezza associate. Ecco perché la missione del CISO in una struttura sanitaria è quella di creare le condizioni adatte ad accogliere un sistema informatico ospedaliero affidabile sia per i professionisti che per i pazienti. »

JEAN-SYLVAIN CHAVANNE — RSSI CLINICA UNIVERSITARIA DI BREST

Per quanto riguarda la gestione data-driven delle strutture sanitarie, alcuni operatori, come FHF[32], ritengono che il PMSI (Programme de Médicalisation des Systèmes d'Information), in quanto primo database medico nazionale, fornisca informazioni sufficientemente strutturate per alimentare un algoritmo di process mining. Un'operazione che, in ultima analisi, consentirebbe di confrontare i dati sul campo del PMSI con un percorso ideale del paziente e di ottimizzare l'assistenza passo dopo passo. —

« Il margine di miglioramento che precede una gestione data-driven è ancora molto ampio, in quanto molte strutture sanitarie stanno ancora facendo il punto della situazione per elaborare una tabella di marcia. »

CHARLES BLANC-ROLIN — RESPONSABILE DI PROGETTO PER LA SICUREZZA DIGITALE NEL SETTORE DELLA SANITÀ ELETTRONICA PAYS DE LA LOIRE

PER APPROFONDIRE

DATA MANAGER
→ Avere dati è positivo, condividerli è meglio. Se da un lato la condivisione dei dati consente ai ricercatori di tutto il mondo di mettere in comune le proprie risorse, dall'altro occorre rispettare norme estremamente severe volte a proteggere e mettere al sicuro i dati dei pazienti. È questa la base per la creazione di una vera e propria professione di data manager in ambito sanitario.

4.3 Una collaborazione da consolidare

Con l'integrazione della biomedicina e dei sistemi operativi di gestione tecnica degli edifici, la copertura SSI (sicurezza dei sistemi informatici) degli impianti sta diventando sempre più ampia e diventa indispensabile coinvolgere tutti gli operatori del settore: IT, SSI e biomedico.



Sviluppare questa cooperazione significa conciliare le priorità e i ritmi di ciascuna parte: i responsabili IT, che vogliono procedere rapidamente, i team informatici, più o meno preoccupati per gli aspetti legati alla sicurezza (anche se hanno privilegi più elevati), e il reparto biomedico, che non vuole mettere a rischio i pazienti.

Tale collaborazione si svilupperà anche a livello di ufficio, con tecnologie cloud sempre più presenti. Una simile evoluzione di utilizzo va supportata, in quanto rappresenta una vera e propria sfida da affrontare.

Il mondo della sanità dovrà misurarsi con nuove esigenze in termini di governance, cooperazione e tecnica per garantire la sicurezza dei pazienti in un ambiente sempre più digitale.

« Più si percorre la strada della tecnologia, più si deve tenere conto della SSI. Storicamente, i rapporti con i team aziendali sono stati spesso complicati, ma gli RSSI del settore sanitario dovranno impegnarsi a far comprendere alle altre funzioni che la sfida comune è la fiducia. »

JACQUES LABIDURIE — RSSI CINICA UNIVERSITARIA DI LIMOGES

« Comprendere le implicazioni tecniche e tecnologiche sta diventando un obbligo, soprattutto quando assistiamo all'impossibilità di gestire il futuro dei dati sulla salute delle donne in un contesto di criminalizzazione dell'aborto. […] Oggi più che mai, spetta a tutti noi contribuire alla nascita di un sistema intelligente e resiliente che rispetti i diritti e le libertà fondamentali. »

RAYNA STAMBOLIYSKA — ESPERTA DI DIPLOMAZIA DIGITALE, SPECIALISTA IN SICUREZZA INFORMATICA E MEMBRO INDIPENDENTE DEL GRUPPO DI LAVORO SULLE MINACCE EMERGENTI E FUTURE DELL'ENISA

Tuttavia, queste sfide non devono mettere in secondo piano la missione di servizio pubblico e di accoglienza tradizionalmente svolta dal settore: bisognerà riuscire a « *riportare l'elemento umano nella macchina* » come ha affermato l'attivista per i diritti umani Claire Hédon[33] su France Inter nel luglio 2022. —

« Solo il tempo ci dirà se il settore sanitario riuscirà a circoscrivere il rischio informatico. Ma è probabile che la digitalizzazione ad alta velocità e la crescente sofisticazione dei gruppi di ransomware non renderanno facile recuperare il proprio debito tecnico. »

JACKY GRISEY — SECURITY OPERATIONS MANAGER DEDICATO AL SETTORE SALUTE, ADVENS

IL FUTURO DELLA SICUREZZA INFORMATICA NEL SETTORE SANITARIO

INTERVISTA

JACKY GRISEY — SECURITY OPERATIONS MANAGER DEDICATO AL SETTORE SALUTE ADVENS

« La condivisione nel contesto di un SOC gestito contribuisce a una forma di intelligenza collettiva, che è vantaggiosa e caratteristica del settore sanitario. »



Alcune delle aspettative nel settore della sicurezza informatica operativa riguardano l'automazione. In realtà la utilizziamo già nel nostro lavoro di analisi della sicurezza, e questo ci permette di ottimizzare i tempi di rilevamento. Per quanto riguarda le azioni correttive, la posta in gioco è molto alta e l'obiettivo è quello di ridurre il più possibile i tempi di risposta. Dal punto di vista dell'organizzazione, il primo passo verso l'automazione è la delega della risposta al partner all'interno di un quadro operativo specifico. Si può quindi prevedere l'esecuzione automatica di risposte "semplici": blocco di indirizzi IP, blacklist di nomi di dominio di posta elettronica, account utente, ecc. che potrebbero anche richiedere un cambiamento nella mentalità dei team IT.

Un altro sviluppo imminente riguarda il settore biomedico, in particolare la gestione delle vulnerabilità e il rilevamento degli incidenti da parte del SOC. Alcuni nostri clienti hanno iniziato a implementare sonde dedicate, estendendo così l'area di rilevamento. Gli operatori dei sistemi informatici concordano su un punto: il settore è una zona grigia!

In definitiva, solo il tempo ci dirà se il settore sanitario riuscirà a circoscrivere il rischio informatico. Per il momento, dobbiamo destreggiarci tra il debito tecnico, la digitalizzazione aziendale, che continua ad avanzare rapidamente, e l'industrializzazione dei gruppi di aggressori informatici. Tuttavia, la condivisione delle risorse nell'ambito di un SOC gestito, ovvero il fatto che alcuni traggano vantaggio da ciò che viene fatto per altri (vulnerabilità rilevate, indicazioni di compromissione, regole di rilevamento o persino funzionalità di integrazione specifiche) contribuisce a una forma di intelligenza collettiva, che è vantaggiosa per tutti. —

FONTI E ALLEGATI

[1]CERT Santé
[2]https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise
[3]https://health-trends.co.uk/wi-ga-la-hospitals-confirm-recent-healthcare-cyberattacks/
[4]https://health-trends.co.uk/wi-ga-la-hospitals-confirm-recent-healthcare-cyberattacks/
[5]https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyberattack-update-march-29-22-1.6401700
[6]lefigaro.fr/secteur/high-tech/covid-19-des-cyberattaques-contre-la-chaine-logistique-des-vaccins-20201203
[7]https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[8]https://www.usine-digitale.fr/article/le-gouvernement-injecte-20-millions-d-euros-dans-l-anssi-pour-renforcer-son-accompagnement-des-hopitaux.N2036952
[9]https://www.ssi.gouv.fr/actualite/lanssi-et-le-bsi-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemagne-dans-le-contexte-de-la-crise-sanitaire/
[10]https://www.psychiaclic.fr/
[11]https://www.dsih.fr/article/4790/effacer-une-donnee-medicale-d-un-patient-vraiment.html
[12]https://www.france24.com/fr/%C3%A9co-tech/20220705-fuite-de-donn%C3%A9es-il-affirme-mettre-en-vente-la-vie-priv%C3%A9e-des-deux-tiers-des-chinois
[13]https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[14]https://www.ibm.com/security/data-breach
[15]https://www.stormshield.com/fr/webinar-sante-face-aux-cybermenaces/
https://www.dsih.fr/article/4790/effacer-une-donnee-medicale-d-un-patient-vraiment.html
[16]https://www.leparisien.fr/faits-divers/coronavirus-le-milieu-medical-nouvelle-cible-des-arnaques-au-president-01-04-2020-8292336.php
[18]https://www.lemondeinformatique.fr/actualites/lire-dedalus-biologie-ecope-d-une-amende-d-1-5-meteuro-par-la-cnil-86527.html
[19]https://www.lemonde.fr/pixels/article/2020/10/27/la-finlande-secouee-par-le-piratage-de-milliers-de-dossiers-de-patients-en-psychotherapie_6057561_4408996.html
[20]https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf
[21]https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/documents-secteur-sante/ACSS_Sensibilisation_s%C3%A9curit%C3%A9_mot_passe.pdf
[22]https://www.esante-centre.fr/portail_pro/services-d-accompagnement/ssi-securite-des-systemes-d-information-131-111.html
[23]https://www.lemagit.fr/etude/Cybersecurite-du-systeme-de-sante-beaucoup-reste-a-faire
[24]https:/esante.gouv.fr/sites/default/files/media_entity/documents/webinaires_ie-usagers_2022-05-09_v2.pdf
[25]https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en
[26]https://esante.gouv.fr/actualites/lespace-europeen-des-donnees-de-sante-cest-parti
[27]https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf
[28]https://esante.gouv.fr/sites/default/files/media_entity/documents/Doctrine_du_numerique_en%20santé_Version%202021_Février%2022_VF.pdf
[29]https://sante-achat.info/performance/charlotte-drapeau-anssi-le-secteur-de-la-sante-est-une-cible-particulierement-vulnerable/
[30]https://sesali.fr/ncpehfr-gui/index.html
[31]https://www.ligence.io
[32]https://www.fondsfhf.org
[33]https://www.francetvinfo.fr/societe/services-publics-il-n-est-pas-possible-d-imposer-a-tout-le-monde-d-avoir-un-smartphone-alerte-la-defenseure-des-droits_5238622.html

LA SCELTA EUROPEA DELLA SICUREZZA INFORMATICA

WWW.STORMSHIELD.COM

Qualsiasi diffusione, riproduzione o rappresentazione, anche parziale, del presente white paper per scopi diversi dall'uso privato su qualsiasi supporto è vietata e può comportare la responsabilità civile e penale per chiunque non si attenga a tale divieto.

Copyright © 2022 Stormshield

STORMSHIELD