Healthcare e Cybersecurity

Contesto e Sfide

Dott. Antonino Ruggeri

Regione Piemonte

Contesto di riferimento

Alcuni dati raccolti dai principali studi di settore descrivono **un settore sotto attacco**

La normativa di riferimento

I requisiti cogenti, allineati alle necessità dettate dal contesto, abilitano **il rafforzamento della resilienza cyber e la protezione dei dai personali**

Le sfide cyber per la sanità

La sanità pubblica in Italia presenta **alcune sfide peculiari** rispetto ad uno scenario cyber generico

SANITÀ SOTTO ATTACCO

Attacco all'Azienda Ospedaliera di Verona: dati in vendita, ma quelli sanitari sono una minima parte

SANITÀ SOTTO ATTACCO

Ransomware colpisce tre Asl di Modena: c'è la rivendicazione del gruppo Hunters, primi dati rubati online

RANSOMWARE

Attacco al sistema sanitario lucano: unità di crisi attivata su ASP Basilicata

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

RANSOMWARE

ASL di Torino colpita da attacco informatico, molti disagi per i pazienti

Home > Malware E Attacchi Hacker: Come Affrontare La Sicurez:

Sanità pubblica nuovamente sotto attacco informatico, si assiste alle difficoltà trascorse in questi giorni dalla Asl Città di Torino colpita da quello che potrebbe essere un tipico attacco ransomware. Computer degli ospedali bloccati, compare una nota di riscatto e le indagini proseguono

Pubblicato il 24 Ago 2022

MISURE D'URGENZA

Ospedali londinesi messi in ginocchio da un ransomware: cosa impariamo

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti > Ransomware

Sono diversi gli ospedali londinesi interessanti dall'attacco ransomware e, in tutto, sono stati cancellati 800 interventi chirurgici. Notizie simili costringono a rivedere l'idea stessa di cyber security

Pubblicato il 4 lug 2024

RANSOMWARE

Attacco all'ASST Rhodense, online 1 TB di dati: c'è la rivendicazione del ransomware Cicada3301

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

I dati personali dei pazienti dell'ASST Rhodense sono stati pubblicati online e sono ora liberamente scaricabili. La rivendicazione è del gruppo ransomware Cicada3301. Ecco le implicazioni e le misure che servono per impedire che attacchi del genere si verifichino di nuovo

Pubblicato il 21 giu 2024

Il Contesto di riferimento: Rischi e tendenze

Il settore sanitario è diventato un **bersaglio privilegiato per la criminalità informatica**, che **sfrutta la crescente digitalizzazione** e la necessità di garantire continuità operativa per massimizzare l'impatto dei propri attacchi

Obiettivo prioritario del cybercrime: Tra gennaio e marzo 2024, gli attacchi puntano soprattutto alla sottrazione di dati sensibili (cartelle cliniche, dati pazienti), mentre i DDoS risultano marginali

Sfide chiave:
- Obsolescenza tecnologica e complessità dei sistemi
- Vulnerabilità della supply chain (fornitori esterni)

Impatto della digitalizzazione:
- Superficie d'attacco in espansione
- Necessità di sicurezza delle terze parti e modelli di cyber insurance

Azioni prioritarie:
Aggiornamento sistemi legacy e monitoraggio continuo
Piani di risposta per attacchi critici (es. ransomware)
Collaborazione con partner tecnologici e assicurativi

Il Contesto di riferimento: la minaccia cibernetica al settore sanitario

A partire da gennaio 2022, secondo il report dell'Agenzia per la Cybersicurezza Nazionale (ACN) **si sono verificati in media almeno due attacchi informatici malevoli al mese contro le strutture sanitarie italiane**

Impatto

- Circa il 50% degli attacchi si traduce **in incidenti di sicurezza** con conseguenze su disponibilità, riservatezza dei servizi e privacy per gli utenti
- **Picco registrato a luglio**, con un attacco a un fornitore IT che ha colpito molti clienti del settore sanitario

Principali criticità

- Pratiche di sicurezza spesso **ignorate o inadeguate**
- **Scarsa formazione** del personale sanitario sulla cybersicurezza

Vulnerabilità

Ospedali, cliniche e strutture sanitarie rimangono **bersagli facili** per la criminalità informatica.

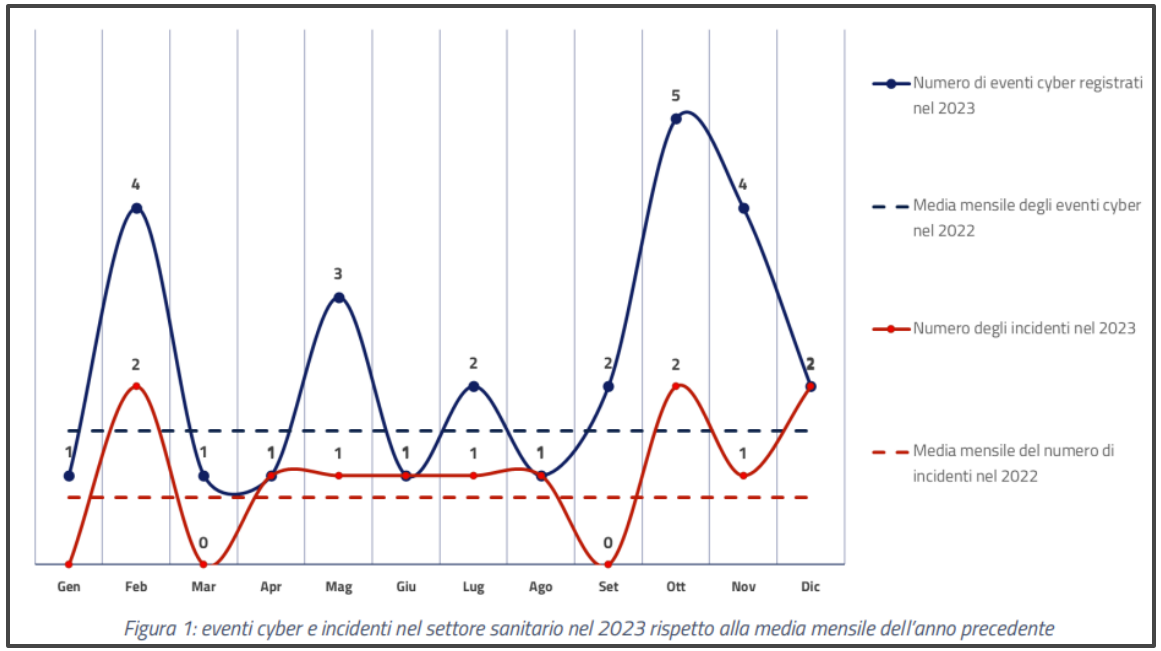
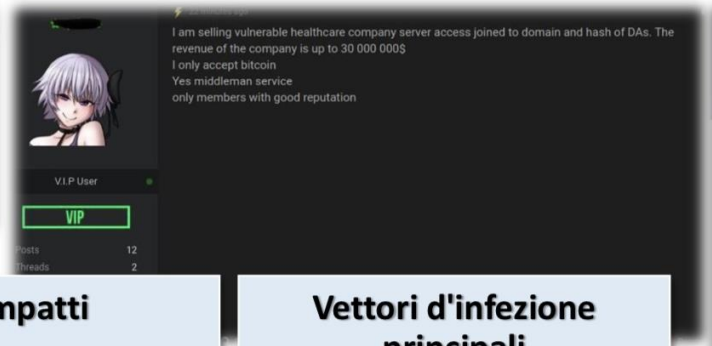
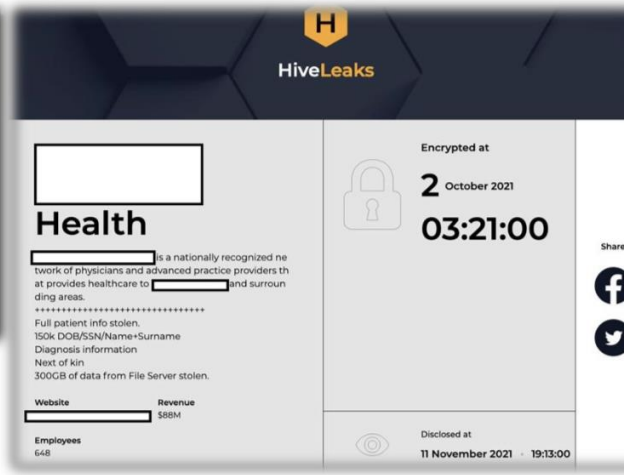


Figura 1: eventi cyber e incidenti nel settore sanitario nel 2023 rispetto alla media mensile dell'anno precedente

Le minacce cyber al settore sanitario





Evoluzione della minaccia

Da attacchi automatizzati ad attacchi **"Human Operated"**

Impatti

- **Cifratura dei dati**
- **Interruzione del servizio sanitario**
- Data Breach

Vettori d'infezione principali

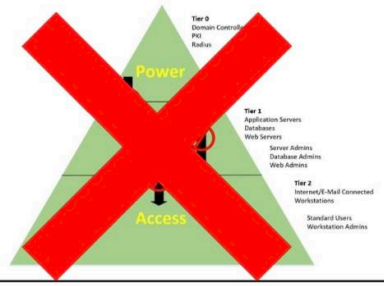
- **Phishing e Business Email Compromise**
- Sfruttamento di vulnerabilità perimetrali

PERCHÉ LA SANITÀ ?

- **Appetibilità dei dati** esfiltrabili
- Soggetti spesso privi di adeguate **misure di cybersicurezza**.
- In caso di attacco ransomware, la **necessità di ripristinare** nel più breve tempo possibile il servizio sanitario aumenta la probabilità di pagamento di un riscatto.

Principali criticità rilevate sul campo

- Utilizzo di password deboli
- Assenza di MFA



- Reti non adeguatamente strutturate
- Gestione scorretta delle credenziali amministrative

- Limitata governance degli aggiornamenti software

- Limitata formazione sulla cybersicurezza del personale

- Eccessiva
- frammentazione delle competenze tra fornitori

- Limitata stabilità del personale IT nell'incarico

Prime riflessioni sui controlli di sicurezza (mitigare le potenziali vulnerabilità)

Sotto-Categoria Framework	Controllo	Descrizione
PR-AC.4 I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	**Limitare i Privilegi Amministrativi agli Account dell'Amministratore**	Limitare i privilegi amministrativi agli account di amministratore riservati alle risorse aziendali. Effettuare attività informatiche generali, navigazione in Internet, posta elettronica e simili da un account utente non privilegiato.
PR-AC.5 L'integrità di rete è protetta (es. segregazione di rete, segmentazione di rete)	**Filtrare il Traffico tra i Segmenti di Rete**	Filtrare il traffico tra i segmenti di rete ove appropriato, assicurando adeguata segmentazione e controllo tra gli ambienti esposti su Internet e gli ambienti interni
PR-AC.7 Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione	**Richiedere MFA per l'Accesso Amministrativo**	Richiedere l'autenticazione multi fattore per l'accesso di tutti gli account amministrativi, se supportata, per tutte le risorse aziendali, sia gestite in locale sia utilizzando un fornitore esterno

La normativa di riferimento: NIS

La Direttiva UE 2016/1148 (**Direttiva NIS - Network and Information Security**) nasce per migliorare la sicurezza delle reti e dei sistemi informativi all'interno dell'Unione Europea, **imponendo agli operatori di servizi essenziali di garantire la resilienza digitale delle proprie infrastrutture**

1

D.Lgs. 65/2018

l'Italia ha dato **attuazione alla Direttiva (UE) 2016/1148 ("Direttiva NIS"),** definendo le misure necessarie a conseguire un elevato livello di sicurezza delle relative reti e dei sistemi informativi

2

Individuazione soggetti OSE

Nel 2019 il MdS, d'intesa con Regioni e PA di Trento e Bolzano, in quanto autorità competenti NIS, ha **individuato i soggetti che forniscono servizi essenziali («OSE»)** dipendenti dalla rete e dai sistemi informativi, per i quali un incidente cyber avrebbe effetti negativi rilevanti sulla fornitura di tali servizi

3

Linee guida OSE

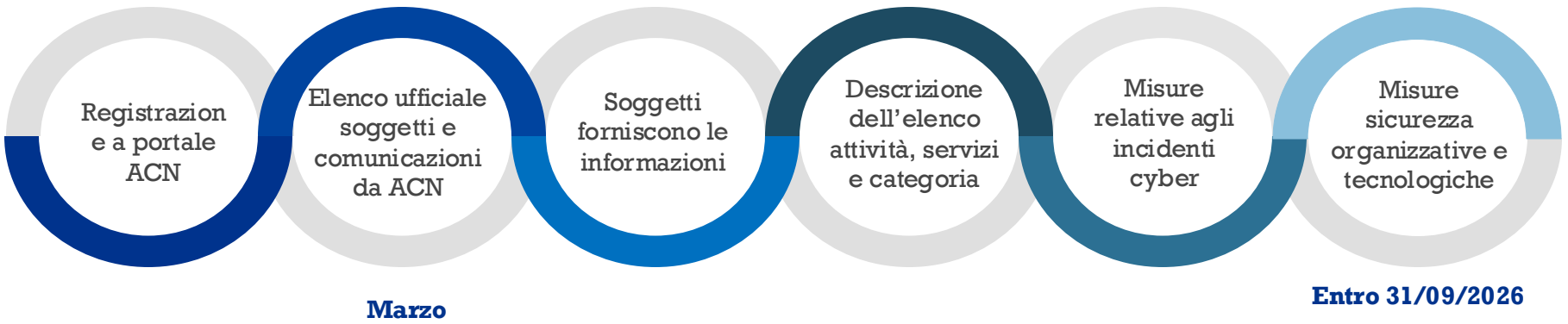
Il Ministero ha poi emesso le Linee Guida per gli OSE per il Settore Salute per fornire le indicazioni e le tempistiche degli adempimenti richiesti agli OSE del settore specifico

La normativa di riferimento: NIS2

La Direttiva sulla Sicurezza delle Reti e dei Sistemi Informativi (Direttiva EU 2022/2555 - NIS2) fa parte della **strategia di cybersecurity dell'Unione Europea con la Direttiva Europea per la Resilienza delle Entità Critiche** (Direttiva EU 2022/2557 – CER) e il Digital Operational Resilience Act (Regolamento EU 2022/2554 – DORA) con **l'obiettivo di migliorare la Resilienza digitale europea.**

- **Nuovo Perimetro:** Estensione degli obblighi a nuovi settori con una categorizzazione aggiornata dei soggetti coinvolti
- **Notifica Incidenti:** Obbligo di segnalare eventi con impatto rilevante alle Autorità entro **24 ore**
- **Autorità/ACN:** Competenze rafforzate per indagare e vigilare sulla conformità.
- **Misure di Sicurezza:** Adozione obbligatoria di misure tecniche e organizzative specifiche per la gestione dei rischi cyber
- **Sanzioni:** Fino a **10 milioni di euro** o il **2% del fatturato annuo mondiale** per violazioni

Prossimi adempimenti



Le sfide cyber per la sanità

Lo scenario cyber per la sanità è caratterizzato da alcune peculiarità che lo rendono particolarmente **appetibile e vulnerabile**

Catena di fornitura eterogenea: Diversi livelli di maturità cybersecurity rendono vulnerabile l'intera rete, dipendente dall'anello più debole

Capitolati regolamentati: Le norme sugli appalti complicano l'integrazione di requisiti stringenti di sicurezza (in evoluzione con la Legge 90).

Mancanza di standardizzazione: Rischi legati all'interoperabilità e alla condivisione dei dati; necessità di crittografia, gestione delle vulnerabilità e standard comuni.

Violazioni dei dati: Dati sanitari personali sono un obiettivo redditizio, con impatti su conformità, reputazione e fiducia dei pazienti

Tecnologia obsoleta: Sistemi e dispositivi datati aumentano le vulnerabilità; l'aggiornamento è costoso e complesso

Formazione insufficiente: Personale sanitario poco preparato ai rischi cyber, aumentando la vulnerabilità a minacce come il phishing

Complessità degli endpoint: Numerosi dispositivi e utenti rendono difficile la gestione e la sicurezza delle infrastrutture

Esemplificativo per attività di incremento delle competenze: Formazione e consapevolezza

La sicurezza del **Fascicolo Sanitario Elettronico**, che connette e custodisce i dati per la cura del paziente, è cruciale per un'assistenza sanitaria sicura.

La Missione 6 del PNRR stanzia **311 milioni di euro** per migliorare le competenze digitali del personale del SSN, con focus su MMG e PLS, rafforzando così il ruolo del FSE in un sistema sanitario sempre più tecnologico.

Esempio di proposta offerta formativa per l'accrescimento delle competenze digitali in ambito FSE2.0

Focus Formazione ** Cybersecurity (alcuni esempi)	Cluster 1*	Cluster 2*			Cluster 3*	
	MMG e PLS	Personale Medico	Personale Infermieristico	Altre professioni	Organi direttivi	Personale tecnico-amministrativo
Introduzione alla Cybersecurity	✓	✓	✓	✓	✓	✓
Disciplina della protezione dei dati nell'era del GDPR	✓	✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓	✓
Cyber in the Board					✓	
…						
Sicurezza delle terze parti	✓	✓	✓	✓		✓

* Fonte: Operatori Fascicolo Sanitario Elettronico 2.0

** La durata e la modalità di erogazione dei corsi (nonché i contenuti) saranno definite in fase di pianificazione dei percorsi formativi