CYBERSECURITY E SANITÀ

UN CAMBIO DI PARADIGMA

Relatore: Luca Francioso

Novembre 2024

CAMBIA MENTO DI PARA DIGMA

EVOLUZIONE DELLA CYBERSECURITY SANITARIA

Il panorama della cybersecurity sta vivendo un cambiamento radicale. Non è più solo difesa dai comuni attacchi informatici, ma un pilastro nella **protezione delle infrastrutture sanitarie** essenziali e dei dati dei pazienti, rafforzando non solo la sicurezza tecnica ma anche operativa delle organizzazioni.

CONTESTO DEGLI ATTACCHI CYBER

Negli ultimi anni, gli **attacchi cyber nel settore sanitario sono aumentati considerevolmente**. Gli hacker mirano ai dati sensibili dei pazienti, sfruttando spesso vulnerabilità nei sistemi IT. Soprattutto dal 2020, è diventato un **bersaglio primario**, accentuando la necessità di rafforzare la sicurezza.

EVOLUZIONE DELLA SICUREZZA

VECCHIO PARADIGMA

In passato, la sicurezza informatica era maggiormente focalizzata sulla protezione dei dati, considerata un aspetto tecnico. Le cartelle cliniche elettroniche e i sistemi IT operativi erano i principali focus.

NUOVO PARADIGMA

Oggi, la cybersecurity è vista come una priorità strategica per garantire la continuità operativa delle strutture sanitarie. Include la gestione di attrezzature IoT e la protezione delle infrastrutture critiche.

INTEGRAZIONE NELLE OPERAZIONI

La cybersecurity è ora una componente fondamentale della gestione operativa sanitaria, non più solo un elemento accessorio. Implica la formazione del personale e processi integrati.

GESTIONE DEI RISCHI

GESTIONE PROATTIVA

Il settore sanitario si sta spostando verso una gestione proattiva dei rischi, con monitoraggio continuo, analisi predittiva dei rischi e preparazione per risposte rapide. Le normative supportano questa transizione.

GESTIONE REATTIVA

Tradizionalmente, la risposta ai rischi informatici avveniva in modo reattivo, dopo che si verificavano gli incidenti. La protezione era limitata a difese contro attacchi già avvenuti.

SETTORE CRITICO

PROTEZIONE DIGITALE TRADIZIONALE

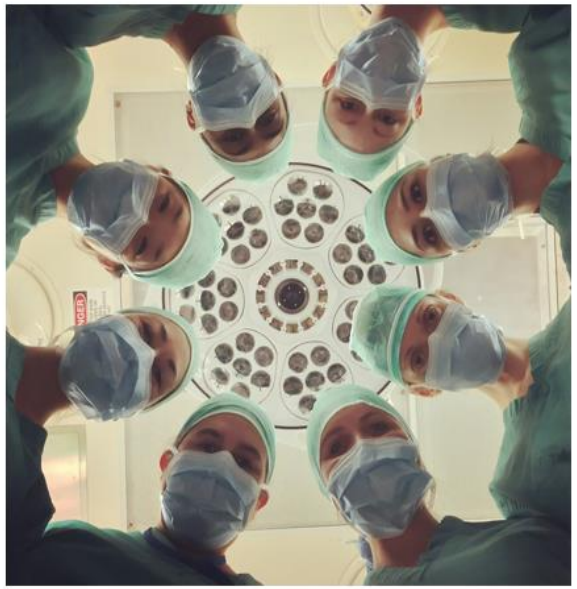
La protezione era mirata solo ai dati digitali e informazioni elettroniche. Non si consideravano le infrastrutture fisiche un obiettivo per attacchi informatici.

CONVERGENZA TRA IT E OT

Oggi, con attrezzature mediche IoT, la sicurezza delle tecnologie operative diventa cruciale. Ciò include dispositivi medici critici e sistemi di controllo.

PROTEZIONE INFRASTRUTTURE MEDICHE

L'attenzione si è ampliata per proteggere l'ecosistema sanitario. Le infrastrutture critiche, come dispositivi di monitoraggio remoto e attrezzature chirurgiche digitali, sono priorità.



SANITÀ: TARGET VULNERABILE

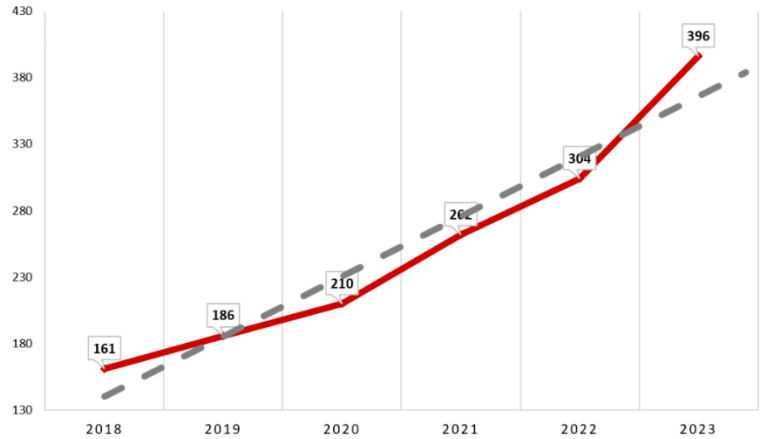
ESEMPI RECENTI DI ATTACCHI

In questi ultimi anni, diversi attacchi hanno paralizzato ospedali, mettendo a rischio informazioni sensibili e cure essenziali. Tali incidenti sottolineano la necessità di forti misure di protezione per evitare danni irrimediabili.

SETTORE SANITARIO NEL MIRINO

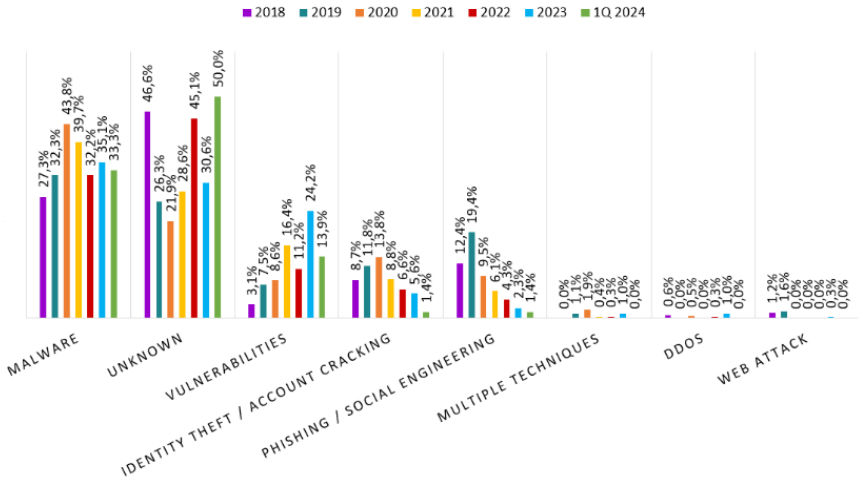
Gli attacchi informatici contro il settore sanitario sono in aumento. Vi sono casi documentati di ransomware che hanno colpito ospedali, causando interruzione dei servizi essenziali. La loro vulnerabilità è dovuta all'infrastruttura spesso obsoleta e al valore intrinseco dei dati sanitari.

CYBER ATTACCHI HEALTHCARE 2018 - 2023



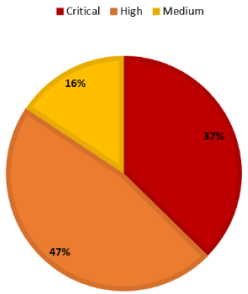
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

TECNICHE % HEALTHCARE 2018 -1Q24

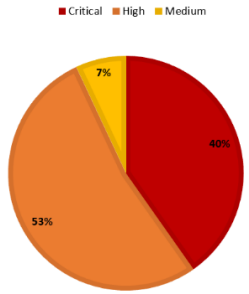


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

SEVERITY HEALTHCARE 2023

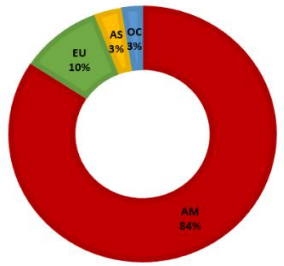


SEVERITY HEALTHCARE 1Q24

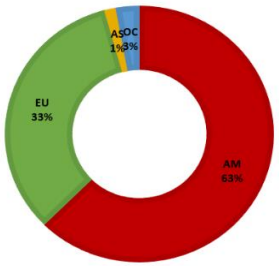


© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

GEOGRAFIE VITTIME HEALTHCARE 2023



GEOGRAFIE VITTIME HEALTHCARE 1Q24



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

FORMAZIONE CONTINUA

EDUCAZIONE DEL PERSONALE SANITARIO

La cybersecurity richiede che **tutto il personale**, dai medici agli amministrativi, **sia coinvolto** nella protezione delle informazioni. La **formazione continua è fondamentale** per preparare il personale ai rischi cibernetici. Aumenta la **consapevolezza** sulla sicurezza e integra la cybersecurity nelle operazioni quotidiane delle strutture sanitarie.

FORMAZIONE CONTINUA

I piani di formazione devono includere corsi regolari e workshop per garantire che tutto il personale sia informato sulle nuove minacce e come affrontarle, sostenendo una cultura di sicurezza consapevole.

PROGRAMMA	OBIETTIVO	COINVOLGIMENTO
Corsi regolari	Aggiornare competenze	Tutti i livelli
Workshop pratici	Simulazioni di attacchi	Tecnici e staff
Certificazioni	Convalidare conoscenze	Dipendenti IT
Check-up periodici	Valutare preparazione	Intera organizzazione

RUOLO DELLE NORMATIVE

NORMATIVE COME FATTORI DI CAMBIAMENTO

Le normative, come la **NIS2**, stanno accelerando **la trasformazione della cybersecurity in sanità**.

Esse **obbligano** le strutture **a implementare** protezioni più strutturate e a rispondere agli incidenti tempestivamente.

Così, la cybersecurity diventa un **obiettivo legale e operativo**, non solo tecnologico, promuovendo sicurezza trasparente e strutturata.

NORME DIRETTIVA NIS2

IMPATTO DELLA DIRETTIVA NIS2

La direttiva NIS2 rappresenta un cambiamento significativo nel panorama normativo per il settore sanitario. Essa impone rigidi standard di sicurezza, obbligando le organizzazioni a rafforzare le proprie difese e protocolli, per proteggere le infrastrutture critiche da potenziali minacce informatiche.

NUOVI OBBLIGHI PER GLI OSPEDALI

Gli ospedali devono ora aderire a standard più elevati di gestione del rischio e segnalazione degli incidenti. Questi obblighi forzano le strutture a un approccio più sistematico, consentendo di mitigare le minacce prima che possano causare gravi danni.

OBBLIGHI DI SICUREZZA

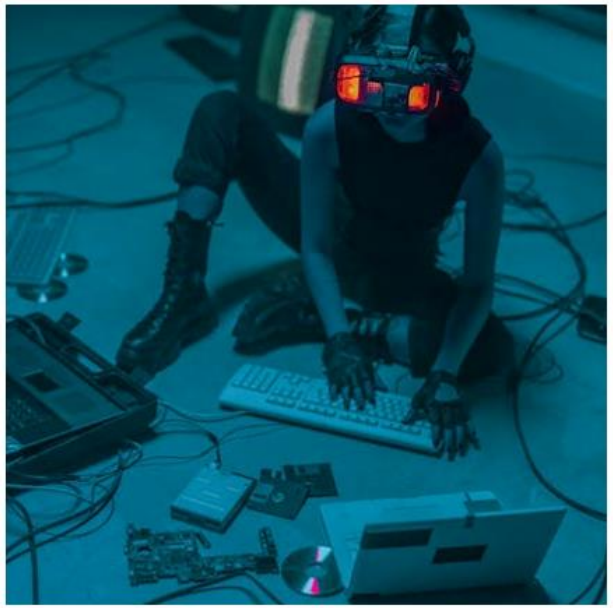
Gli obblighi di sicurezza imposti dalla NIS2 sono estesi e dettagliati, spingendo le strutture sanitarie a migliorare metodologie e pratiche di sicurezza.
Questo sforzo mira a creare un quadro più coerente e resiliente contro le minacce.

GESTIONE DEL RISCHIO	RAFFORZAMENTO DELLE PROCEDURE PER IDENTIFICARE E MITIGARE I RISCHI POTENZIALI
Segnalazione Incidente	Tempestiva comunicazione alle autorità competenti in caso di attacco
Verifica di Conformità	Regolari audit per garantire il rispetto delle normative
Formazione Continua	Programmi di formazione per migliorare la consapevolezza delle minacce tra il personale
Collaborazione Inter-settoriale	Lavoro congiunto con altre realtà sanitarie per rafforzare le difese

CYBERSECURITY: VECCHIO VS NUOVO

Il *vecchio paradigma* si concentrava su un approccio reattivo, con focus primario sulla protezione dati. Nel **nuovo paradigma**, l'accento è sulla *continuità operativa*, *integrando IoT* e una *gestione sistema proattiva*.
Le normative ora hanno un ruolo cruciale, richiedendo **coinvolgimento di tutto il personale**.

ASPETTI	VECCHIO PARADIGMA	NUOVO PARADIGMA
Approccio	Reattivo	Proattivo
Focus	Protezione Dati	Continuità Operativa
Tecnologie Coinvolte	IT Tradizionale	IoT e Infrastructure
Ruolo Normative	Minimo o Assente	Cruciale per il Cambiamento
Coinvolgimento Personale	Limitato a Specialisti	Formazione Continua di Tutti



SFIDE FUTURE

SFIDE EMERGENTI

Le nuove tecnologie portano nuove sfide, come l'uso crescente di **intelligenza artificiale** e **machine learning**. Mentre esse offrono soluzioni innovative, introducono anche complessi rischi di sicurezza.

CONCLUSIONI FINALI

IMPORTANZA DELLA CYBERSECURITY IN SANITÀ

La cybersecurity è un **pilastro fondamentale nel settore sanitario moderno**.

È essenziale per proteggere i dati dei pazienti, **garantire la continuità operativa e costruire la fiducia**. Investire in sicurezza tecnologica e **culturale** rappresenta un passo cruciale per affrontare le sfide future. Il focus sulla cybersecurity deve rimanere costante e adattarsi a nuovi sviluppi e minacce emergenti.

GRAZIE

Luca Francioso

Direzione Business Unit Cyber Security | WeTech'S
Business Unit WeSecure's

Mail
luca.francioso@wetechs.it

Website
www.wesecures.it www.nisgroup.it