Le conseguenze delle vulnerabilità cyber-fisiche dei dispositivi medicali sulla sicurezza del paziente e dei processi ospedalieri

Dott. Ing. Paolo Abundo

Dirigente Ingegnere Biomedico

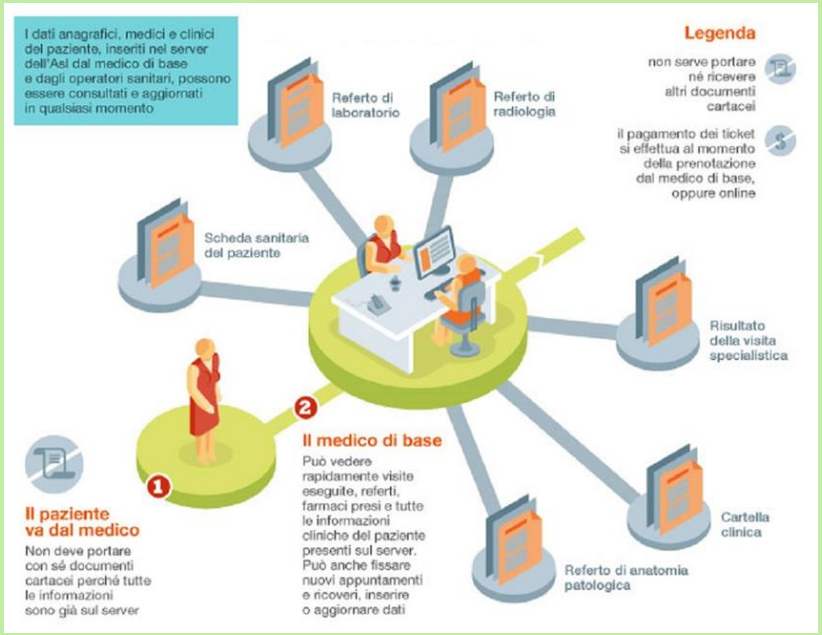
Responsabile Servizio Ingegneria Medica

Fondazione Policlinico Tor Vergata di Roma

paolo.abundo@ptvonline.it

DECRETI LEGISLATIVI SULLA DIGITALIZZAZIONE – Sanità 4.0

Decreto 20 maggio 2022 -> ***Fasciolo sanitario elettronico*** *(Aggiorna art. 12 del decreto legge 179/2012)*



ATTENZIONE «*SICUREZZA DEI DATI SENSIBILI*»

- *Dati anagrafici del cittadino*
- *Documenti sanitari dell'assistito (ricette, prenotazioni per visite specialistiche, referti, Patient Summary, Dossier Farmaceutico)*

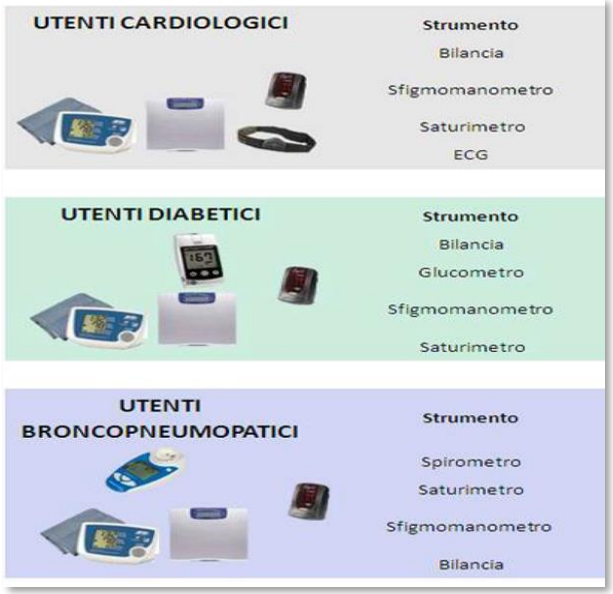
DECRETI LEGISLATIVI SULLA DIGITALIZZAZIONE – Sanità 4.0

Decreto ministeriale 21 settembre 2022 -> "Approvazione delle linee guida per i servizi di telemedicina - Requisiti funzionali e livelli di servizio"

TELEASSISTENZA

TELECONSULTO

TELEVISITA

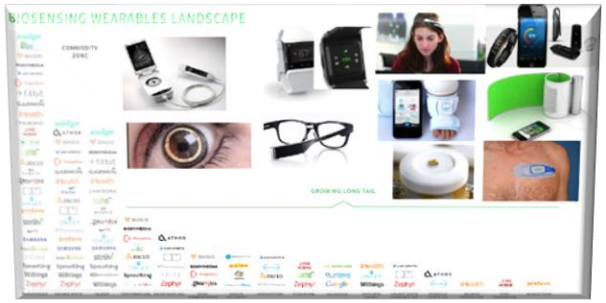


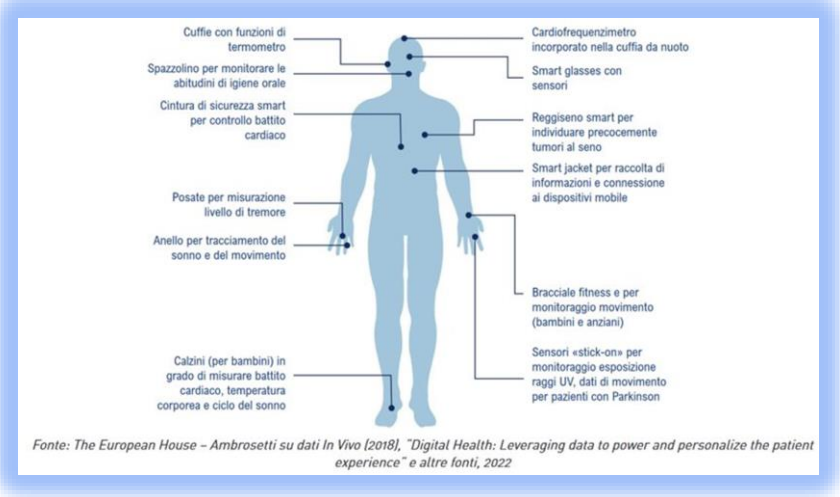
DATO DI FATTO

Maggior numero di tecnologie sempre più costantemente connesse a rete

DECRETI LEGISLATIVI SULLA DIGITALIZZAZIONE – Sanità 4.0

Avanzamento tecnologico e DM connessi a rete





Fonte: The European House – Ambrosetti su dati In Vivo (2018), "Digital Health: Leveraging data to power and personalize the patient experience" e altre fonti, 2022

Ruolo dei BIG DATA

I dispositivi di **comunicazione mobile**, i **cloud**, i sensori di trasmissione a radiofrequenza, **dispositivi per il monitoraggio** dei dati del paziente, etc…sono ad oggi **sempre più diffusi e trasmettono dati utili per ricercare soluzioni**

NUOVE TECNOLOGIE E INTEROPERABILITÀ – Sanità 4.0

Intelligenza Artificiale – Precision Medicine

COMPUTED TOMOGRAPHY

Intelligenza artificiale e tecnologia Photon-Counting nel presente (e futuro) della diagnostica per immagini

Home > Digital Health > Intelligenza Artificiale

Condividi questo articolo

Nel cuore della tecnologia che promette di aprire una nuova era della Tomografia Assiale Computerizzata consentendo un enorme passo avanti nell'ambito della ricerca e della diagnosi

Investimenti nel settore Sanitario

Il **PNRR** (Piano Nazionale di Ripresa e Resilienza) prevede complessivamente **29,78 Mld Euro** dedicati direttamente o indirettamente al settore dell'IoT, di cui **4 Mld Euro per la Telemedicina**

OTTIMA OPPORTUNITÀ, MA….ATTENZIONE….

In tale contesto è necessario **garantire il mantenimento della sicurezza delle persone, dei pazienti**, incoraggiando al contempo l'**innovazione** e consentendo l'accesso tempestivo dei pazienti a dispositivi medici sicuri ed efficaci.

RISCHI PER LA SANITÀ

COSA PUÒ ESSERE ATTACATO?

- Sistema informativo Ospedaliero (**HIS**)
- Software **RIS-PACS**
- **Server** fisici di archiviazione dati
- **Apparecchiature elettromedicali e Software medicali connessi a rete (LAN-WLAN) -> *Internet of Medical Things (IoMT)***
  - Radiologia;
  - Medicina di laboratorio;
  - Sale di Terapie intensiva/Sub Intensiva/UTIC;
  - Catena del freddo
  - Sistemi per Teleassistenza …
- Intera **Rete LAN ospedaliera**

STRUMENTI UTILIZZATI PER GLI ATTACCHI INFORMATICI

Gli attacchi utilizzano software programmati che possono propagarsi attraverso le apparecchiature collegate in rete (anche MD) provocando malfunzionamento sulla rete informatica

RISCHI PER LA SANITÀ

COSA COMPORTANO LE INTERRUZIONI…?

- CHIUSURA DI INTERE UNITÀ OPERATIVE
- FURTO DI DATI SENSIBILI
- POSSIBILE DANNEGGIAMENTO DI DISPOSITIVI MEDICI
- ELEVATI RISCHI PER LA SICUREZZA PAZIENTE
- BLOCCO DEL SERVIZIO SANITARIO ANCHE PER DIVERSI GIORNI

ATTACCHI INFORMATICI, CONSEGUENZE CONCRETE

Richiami del Food and Drug Administration

FDA Recalls Medtronic Insulin Pump Controller, Cites Cybersecurity Risks

The FDA issued a medical device recall on all Medtronic MiniMed remote controllers due to potential cybersecurity risks.

Source: Getty Images

By Jill McKeon

October 08, 2021 - The US Food and Drug Administration (FDA) issued a
Medtronic MiniMed remote controllers used with the Medtronic MiniMed
the MinMed Paradigm family of insulin pumps, citing significant cybersecu

FDA warns of security flaw in Hospira infusion pumps

31 luglio 2015

finance.yahoo.com

July 31 04:11 PM

BOSTON, July 31 (Reuters) - The U.S. Food and Drug Administration on Friday advised hospitals to stop using Hospira Inc's Symbiq infusion system, saying a security vulnerability could allow cyber attackers to take control of the system remotely.

The agency issued the advisory some 10 days after the U.S. Department of Homeland Security warned of the vulnerability in the pump, which is used to deliver medications directly into the bloodstream of patients.

The FDA and DHS cited research from independent cyber security expert Billy Rios, who found that remote attacks could be launched on patients by accessing a hospital's network.

Both government agencies said they know of no cases where such an attack has been launched, but the FDA said in its advisory that it strongly encouraged healthcare facilities to stop using the Symbiq infusion pump system and move to other devices.

"This (vulnerability) could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies," the agency said in its warning.

ators are placing unprecedented
abilities in products with embedded

3/5/2023 Illumina gets cybersecurity warning from FDA over sequencing software | MedTech Dive

MEDTECHDIVE

Illumina gets cybersecurity warning from FDA over sequencing software

The vulnerability could result in an attacker gaining remote control of an instrument and altering genomic data results, the agency said.

Published April 27, 2023 • Updated April 28, 2023

By Susan Kelly
Reporter

An Illumina MiSeq gene sequencing machine. Courtesy of Illumina

ATTACCHI INFORMATICI, CONSEGUENZE CONCRETE

Attacchi che hanno causato gravi conseguenze al paziente e alle Regioni

TD

Redazione

18 settembre 2020 16:55

Si parla di

Germania

hacker

indagini

morti

ospedali

Sullo stesso argomento

RASSEGNA

Boom di truffe online: hacker scatenati anche grazie ai "bonus coronavirus"

Attacco informatico contro l'ospedale, muore una donna: si indaga per omicidio colposo

Con i sistemi in tilt, gli operatori hanno dovuto trasferire in altre strutture le ambulanze in arrivo al pronto soccorso

L'attacco hacker ha costretto l'ospedale a trasferire le ambulanze in arrivo al pronto soccorso in altre strutture (foto di repertorio)

Le autorità tedesche stanno indagando sull'attacco **hacker** che ha colpito i sistemi di un ospedale di **Dusseldorf** a causa del quale sarebbe morta una donna.

NETWORK DIGITAL 360

CYBERSECURITY360 | Cybersecurity Nazionale | Malware e attacchi | Norme e adeguamen

L'ANALISI

Regione Lazio e ransomware, lieto fine amaro: troppi errori fatti

Home > Malware e attacchi hacker

Condividi questo articolo

Un attacco ransomware non ha nulla di sofisticato, e dovrebbe ben rientrare nelle capacità di gestione di un'infrastruttura critica come la Regione Lazio, che dovrebbe aver adottato un piano di risposta agli incidenti di questo tipo, e per il ripristino delle operatività nel più breve tempo possibile. Ma così non è stato, con molti errori, tecnici e di comunicazione

Pubblicato il 08 Ago 2021

Matteo Navacci

Co founders Privacy Network

ATTACCHI INFORMATICI, CONSEGUENZE CONCRETE

Attacchi in Italia

COME SI PUÒ/DEVE AFFRONTARE IL PROBLEMA IN SANITÀ….?

Approccio **proattivo**

Investire sulla **Cultura della Cyber Security**

Approfondire le **conoscenze** del quadro Normativo

+

Creare un Team **multidisciplinare**

Collaborazione tra **Alta direzione, IT, l'Ingegneria Clinica, DPO**

+

Lavorare sul **presente e futuro**

Gestione della sicurezza ad Alto livello della rete ospedaliera

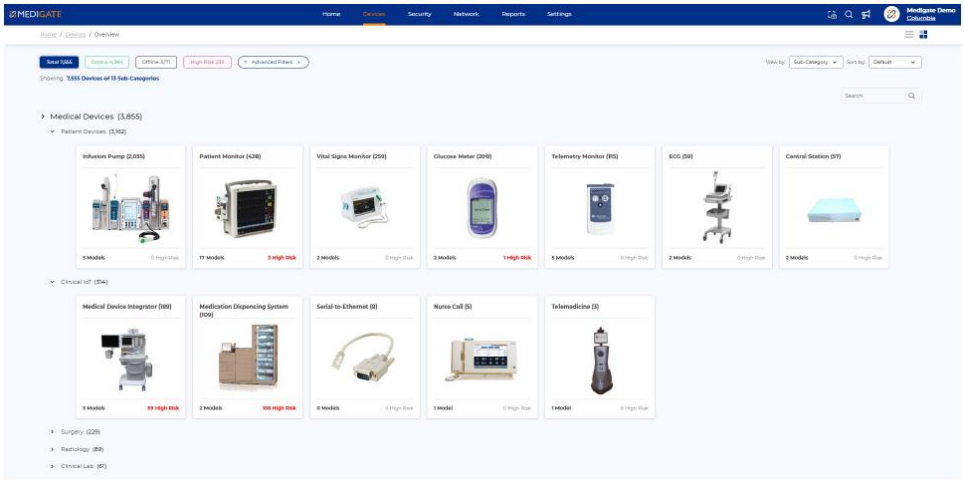
Gestione della sicurezza delle **apparecchiature già collegate a rete**

Gestione dell'acquisizione di **nuovi** DM in rete, *stressando* gli aspetti di Cyber Security

CON QUALI STRUMENTI…?

Alert, predizione, intercettazione e mitigazione e business continuity

CON QUALI STRUMENTI…?

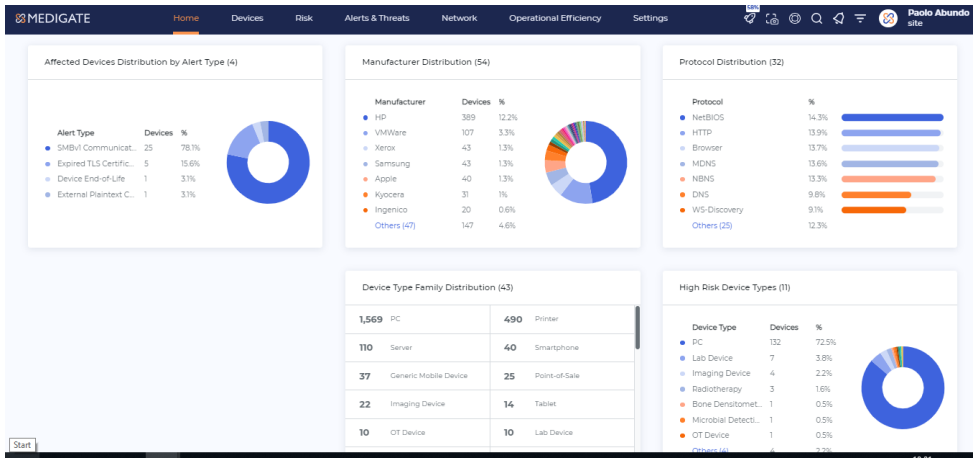


Identificazione di tutti i dispositivi medici e tutti dispositivi IoT e IT connessi

Assegnazione di un **punteggio di rischio** a ogni dispositivo

Aggregazione dei punteggi di rischio in **report dettagliati e operativi**

	10.140.26.77	A4:4E:31:96:FA:2F	STRONA	Anesthesia Cart	DeviceConX Fanless PC	Windows 10/Server 2016...	103	8/28/2019 11:05 AM	Online / Medium
	10.140.26.77 / 2203	A4:4E:31:96:FA:2F	GE	Anesthesia Monitor	Datex-Ohmeda S5	Datalight ROM-DOS	103	8/28/2019 11:33 AM	Online / Low
	10.140.26.77 / 2204	A4:4E:31:96:FA:2F	GE	Anesthesia Machine	Datex-Ohmeda Aisys CS2	Nucleus	103	8/19/2019 9:09 AM	Offline / Low
	10.140.26.78	10:62:E5:27:62:3F	STRONA	Anesthesia Cart	DeviceConX Fanless PC	Windows 10/Server 2016...	103	8/28/2019 11:40 AM	Online / Medium
	10.140.26.78 / 802	10:62:E5:27:62:3F	GE	Anesthesia Monitor	Datex-Ohmeda S5	Datalight ROM-DOS	103	8/28/2019 11:14 AM	Offline / Low



VANTAGGI

Aiuta il team di rifermento a **gestire i rischi delle reti mediche** in collaborazione con i produttori.

Propone anche **misure di mitigazione personalizzate** e l'imposizione di **policy di sicurezza tramite i firewall** o le soluzioni di **controllo degli accessi (NAC) esistenti**

TUTTO QUESTO DEVE ESSERE CONTINUAMENTE IMPLEMENTATO, NON BASTA INIZIARE…

TAKE HOME MESSAGE: LAVORARE, LAVORARE…

ASPETTI DA OTTIMIZZARE

- GESTIRE IL RAPPORTO CON IL FORNITORE/PRODUTTORE DEL DM E SW
- FASE DI ACQUISIZIONE RICHIEDE COLLABORAZIONE MULTIDISCIPLINARE (IC-IT-DPO)
- SOFTWARE DI ULTIMA GENERAZIONE, INNOVATIVI PER IMPLEMENTARE SISTEMI ANTIVIRUS PER I DM E SW
- MAGGIORE COLLABORAZIONE TRA IC-IT
- ACQUISTI DI DISPOSITIVI MEDICI PIÙ MIRATI SULLA SICUREZZA INFORMATICA


“La misura dell'intelligenza è data dalla capacità di cambiare quando è necessario”
(Albert Einstein)

Le conseguenze delle vulnerabilità cyber-fisiche dei dispositivi medicali sulla sicurezza del paziente e dei processi ospedalieri

Grazie per l'attenzione

Dott. Ing. Paolo Abundo

Dirigente Ingegnere Biomedico

Responsabile Servizio Ingegneria Medica

Fondazione Policlinico Tor Vergata di Roma

paolo.abundo@ptvonline.it