ADVANCED HEALTHCARE PROTECTION

Con il patrocinio di:

15 Settembre 2021 - Aula Perraro – Padiglione Ingresso

Santa Maria della Misericordia

AGENDA

09:30 Scenario Generale - Lisa Bassetto e Fabio Tolomelli - Mead
09:45 Sicurezza IT e Cybersecurity – Differenza – Mirko Gorrieri - Mead
10:00 Nuove Normative tecniche e regolamenti Europei per i dispositivi medici – Michele Bava – Burlo Garofolo

10:45 Break

11:15 Analisi dei dati dall'utilizzo dei sistemi Medigate C/o IRCCS Burlo Garofalo – Michele Bava – Burlo Garofolo
11:45 Clinical SOC – Roberto Fantini – Mead
12:30 Tavola Rotonda – domane e risposte

13:00 Pranzo

Con il patrocinio di:

OUTLOOK MERCATO SANITA'

Considerazioni

- Crescita della telemedicina
- Il 76% degli ospedali utilizza tecnologie di Videocomunicazione con i pazienti
- Negli ultimi 3 anni il numero dei referti fatti con sistemi di telemedicina è raddoppiato
  la tendenza è una continua crescita di circa il 20% annuo

Fonte HIMSS: Healthcare Cybersecurity Threts

OUTLOOK MERCATO SANITA'

Il 57% delle aziende sanitarie ha subito cyber attacchi nel corso del 2020

- 65% DOVUTE A NEGLIGENZA DEGLI UTENTI
- 71% DOVUTA A MANUTENZIONE NON ADEGUATA

Il 40% dei device IoT è un device medicale IoMT

OUTLOOK MERCATO SANITA'

Un attacco informatico al sistema sanitario è di fatto un attacco alle persone

- Le vittime siamo noi
- Il personale Sanitario

"We are attacked every day, it varies between twenty and a hundred times […]. We even have days with 400 attacks. Yet we are a small establishment."

The scale of the problem is described by the head of IT following a cyberattack on the Centre Hospitalier de Narbonne, France, 10 December 2020 (Lherbette, Hélène; Centre Hospitalier de Narbonne

HEALTHCARE DATA BREACHES

57% delle Aziende Sanitarie ha subito data Breach nel 2020*

85% Dei data Breaches includevano Ransomware e Phishing*

75% dei sistemi Sanitari sono stati “investiti” da questi attacchi *

Fonte 2020 HIMSS Security Report

Grazie

ADVANCED HEALTHCARE PROTECTION

Con il patrocinio di:

Clusit
Associazione Italiana per la Sicurezza Informatica

AIIC
associazione italiana ingegneri clinici

Sicurezza IT & Cybersecurity

Mirko Gorrieri

Cybersecurity

Information Technology

Biomedicali

Automation / smart Building

Sempre più Oggetti connessi «smart» / **Più oggetti connessi = più vulnerabilità**

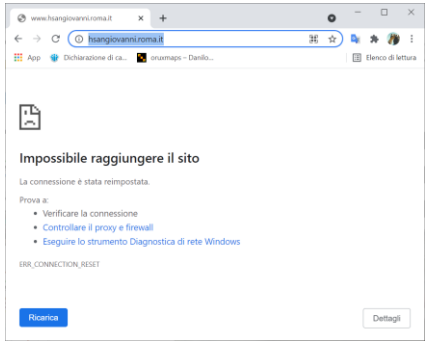
Il Messaggero

NEWS

Roma, attacco hacker all'ospedale San Giovanni: «In tilt tutto il sistema»

di Flaminia Savelli

Martedì 14 Settembre 2021 Ultimo aggiornamento 00:14



mead
YOUR DIGITAL INTEGRATOR

14/09/2021

Cartelle cliniche oscurate. Esami radiologici e di laboratorio cancellati. Registrazione dei pazienti in pronto soccorso "sospesa": così l'intero sistema di rete e telecomunicazioni dell'**ospedale San Giovanni Addolorate** ieri è saltato per un attacco hacker.

Ma nessuno è più riuscito ad accedere al sistema operativo che ha messo fuori uso **300 server e 1500 client**

«Stiamo lavorando alacremente per ripristinare tutte le funzioni nel più breve tempo possibile, garantendo la continuità dell'assistenza ospedaliera» ha scritto in una nota ufficiale la dirigente sanitaria Maria Pia Ruggieri

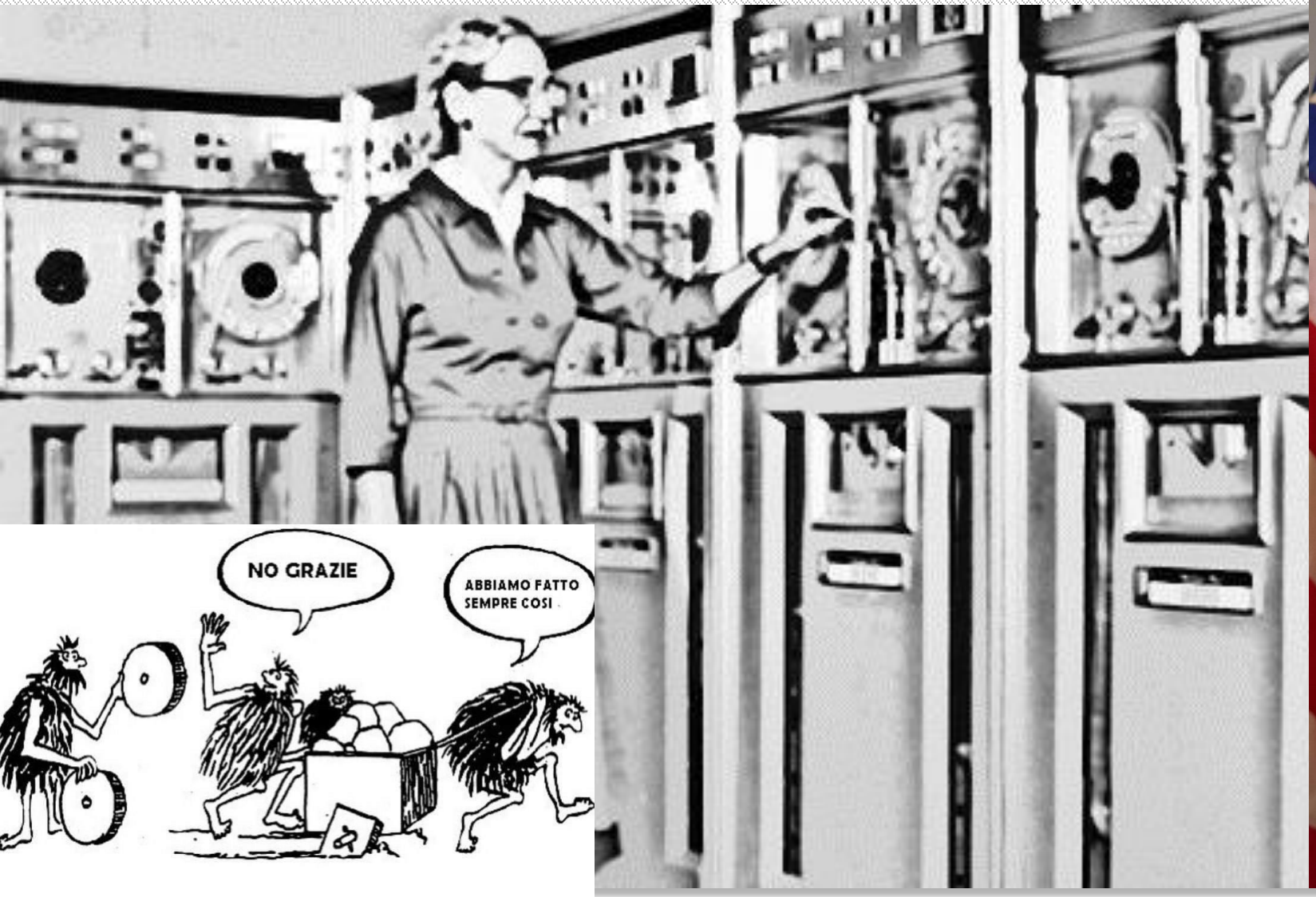
«**Bloccare un ospedale, significa causare dei morti tra persone indifese**» commentano i sanitari della struttura

https://www.ilmessaggero.it/AMP/roma/attacco_hacker_ospedale_san_giovanni_roma_cosa_e_successo-6193603.html

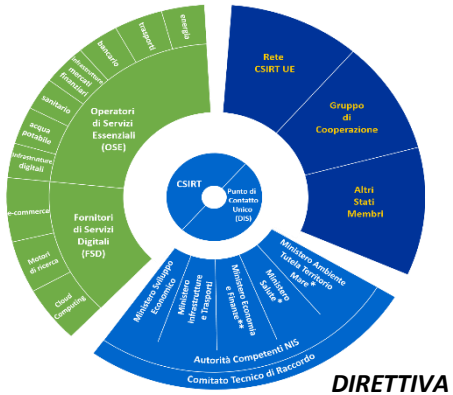
“La frase più pericolosa in assoluto è: Abbiamo sempre fatto così”

(Contrammiraglio Grace Murray Hopper)

mead
YOUR DIGITAL INTEGRATOR



Conferenza Stato Regioni Atto 183/CSR Linee guida per gli operatori di servizi essenziali (OSE)
Allegato 2: Misure di sicurezza - settore Salute



DIRETTIVA NIS

Emergenza Urgenza	Ricovero per Acuti	Lungodegenza, riabilitazione e regime Ambulatoriale

ALLEGATO 2: Misure di sicurezza – Scadenze settore Salute

Function	Category	Subcategory	Controlli Essenziali di Cybersecurity (PMI)	ABSC AgID	Emergenza-urgenza	Ricovero per acuti	Lungodegenza, riabilitazione e regime ambulatoriale
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	1. Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale. 2. I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. 3. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti	1.1.1	Alta	Media	Media
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione		2.1.1	Alta	Media	Media

http://www.statoregioni.it/it/conferenza-stato-regioni/sedute-2019/seduta-del-07112019/atti/repertorio-atto-n-183csr/

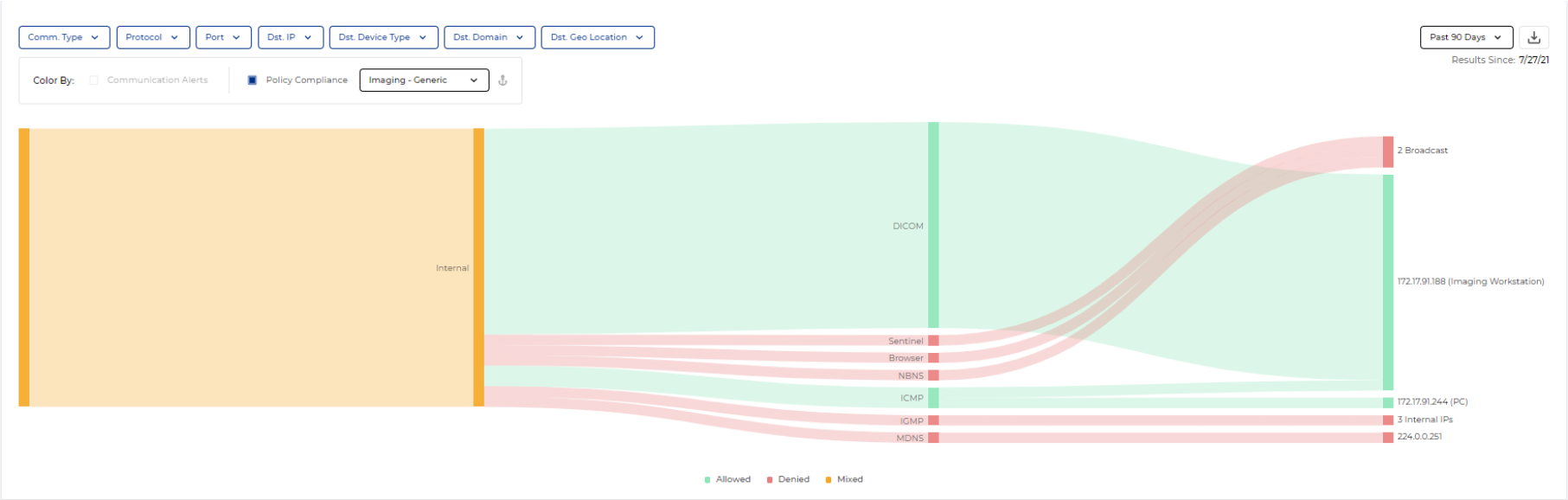
Differenze tra Information Technology e Biomedicali

IT				
Riservatezza - **Integrità** del Dato	occasionali downtime accettabili	**Standard**	**Aggiornamenti semplici** con sistemi automatici - Approcio **Agile**	Dai **3 ai 5 anni**
Risk Management	**Affidabilità**	**Sistemi e Protocolli**	**Change Management**	**Vita dei componenti**
Safety (Persone, rischio biologico, Ambientale) - **Disponibilità**, continuità dei servizi	downtime **non** accettabili	**Propietari**	**Aggiornamenti complicati - Test e validazione di ogni modifica**	Dai **10 ai 15 e più anni**
Ingegneria Clinica				

Ad oggi il principale rischio è che i device biomedicali vengano coinvolti in un attacco **Ransomware** e questo ne comprometta la disponibilità, occorre quindi iniziare a gestire la cybersecurity di questi asset per migliorarne la **Resilienza** in caso di attacco informatico

IDENTIFY Inventario: per proteggere occorre prima di tutto

Non solo la lista degli asset



mead
YOUR DIGITAL INTEGRATOR

IDENTIFY – Protect – Responde Vulnerabilità e accessi amministrativi

VULNERABILITY NAME	TYPE	CVEs	CVSS	UPDATED BY	STATUS
CVE-2021-24074	Platform	CVE-2021-24074	9.8 (v3)	Medigate	Potentially Relevant
CVE-2021-26424	Platform	CVE-2021-26424	9.8 (v3)	Medigate	Potentially Relevant
CVE-2021-26432	Platform	CVE-2021-26432	9.8 (v3)	Medigate	Potentially Relevant
CVE-2021-31166	Platform	CVE-2021-31166	9.8 (v3)	Medigate	Potentially Relevant
ADV200006 (VU#354840 / CVE-2020-1020 / CVE-2020-0938)	Platform	2 CVEs	8.8 (v3)	Medigate	Potentially Relevant
CVE-2021-33742	Platform	CVE-2021-33742	8.8 (v3)	Medigate	Potentially Relevant
CVE-2021-34448	Platform	CVE-2021-34448	8.8 (v3)	Medigate	Potentially Relevant
VU#383432 (PrintNightmare)	Platform	2 CVEs	8.8 (v3)	Medigate	Potentially Relevant
CVE-2020-0601 (Curveball)	Platform	CVE-2020-0601	8.1 (v3)	Medigate	Potentially Relevant
MS17-010 - EternalBlue (WannaCry)	Platform	6 CVEs	8.1 (v3)	Medigate	Potentially Relevant
CVE-2020-0787	Platform	CVE-2020-0787	7.8 (v3)	Medigate	Potentially Relevant
WinCodecs (CVE-2020-1425 / CVE-2020-1457)	Platform	2 CVEs	7.8 (v3)	Medigate	Potentially Relevant
CVE-2020-17087	Platform	CVE-2020-17087	7.8 (v3)	Medigate	Potentially Relevant
CVE-2021-31199	Platform	CVE-2021-31199	7.8 (v3)	Medigate	Potentially Relevant
CVE-2021-31201	Platform	CVE-2021-31201	7.8 (v3)	Medigate	Potentially Relevant

Risolvere o mitigare le vulnerabilità senza compromettere la funzionalità

Virtual Patching

Vulnerabilità CVE-2017-0143 (WannaCry)

WannaCry

Da Wikipedia, l'enciclopedia libera.

WannaCry, chiamato anche **WanaCrypt0r 2.0**, è un worm, di tipologia ransomware, responsabile di un'*epidemia* su larga scala avvenuta nel maggio 2017 su computer con Microsoft Windows. In esecuzione cripta i file presenti sul computer e chiede un riscatto di alcune centinaia di dollari per decriptarli.[2][3]

Il 12 maggio 2017 il malware ha infettato i sistemi informatici di numerose aziende e organizzazioni in tutto il mondo, tra cui Portugal Telecom, Deutsche Bahn, FedEx, Telefónica, Tuenti, Renault, il National Health Service, il Ministero dell'interno russo, l'Università degli Studi di Milano-Bicocca.

Al 28 maggio sono stati colpiti oltre 230.000 computer in 150 paesi, rendendolo uno dei maggiori contagi informatici mai avvenuti.[4][5]

Indice [nascondi]

1 Funzionamento
2 Attacco del maggio 2017
3 Note
4 Voci correlate
5 Altri progetti
6 Collegamenti esterni

WannaCry
software

La schermata in cui il virus richiede il pagamento del riscatto per decrittare i dati.

Genere	Ransomware (non in lista)
Sviluppatore	Possibile attribuzione agli hacker Nord Coreani[1]
Sistema operativo	Microsoft Windows

Modifica dati su Wikidata · Manuale

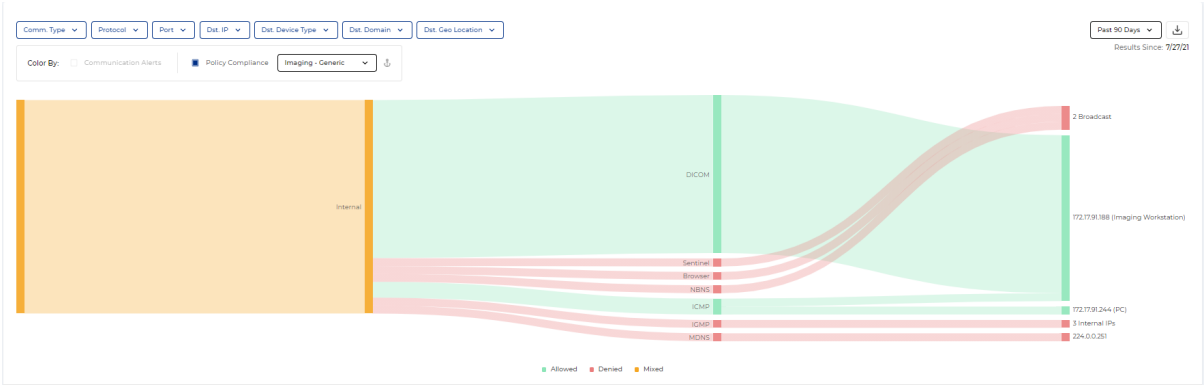
- **Nonstate i danni che causato il malware WannaCry**
- **Nonostante che la vulnerabilità sfruttata dal malware per propagarsi sia del 2017**

Sono ancora presenti, soprattutto nel mondo degli oggetti, molte machine che presentano la vulnerabilità CVE-2017-0143

AFFECTED MEDICAL DEVICES
18

RELEASE DATE	VULNERABILITY NAME	VULNERABILITY TYPE	CVEs	CVSS V3	CVSS V2	DESCRIPTION	AFFECTED PRODUCTS	RECOMMENDATIONS	SOURCE	AFFECTED DEVICES	AFFECTED MEDICAL DEVICES
3/14/17 01:00	MS17-010 - EternalBlue (WannaCry)	Platform	6 CVEs	8.1	9.3	EternalBlue is the name given to a software vulnerability in Microsoft's Windows operating system. Microsoft issued a securit...	Microsoft Windows Vista Microsoft Windows 7 Microsoft Windows 8.1...	* Microsoft has released a patch for the MS17-010 SMB vulnerability dated March 14, 2017. Apply the patch as soon as possible. For...	Microsoft	159	18

Protect – Hardenig, NAC Network Access Control, segmentazione e micro segmentazione



POLICY RULES

Showing: **24 Rules**

Sorted By: PROTOCOL (ASC)

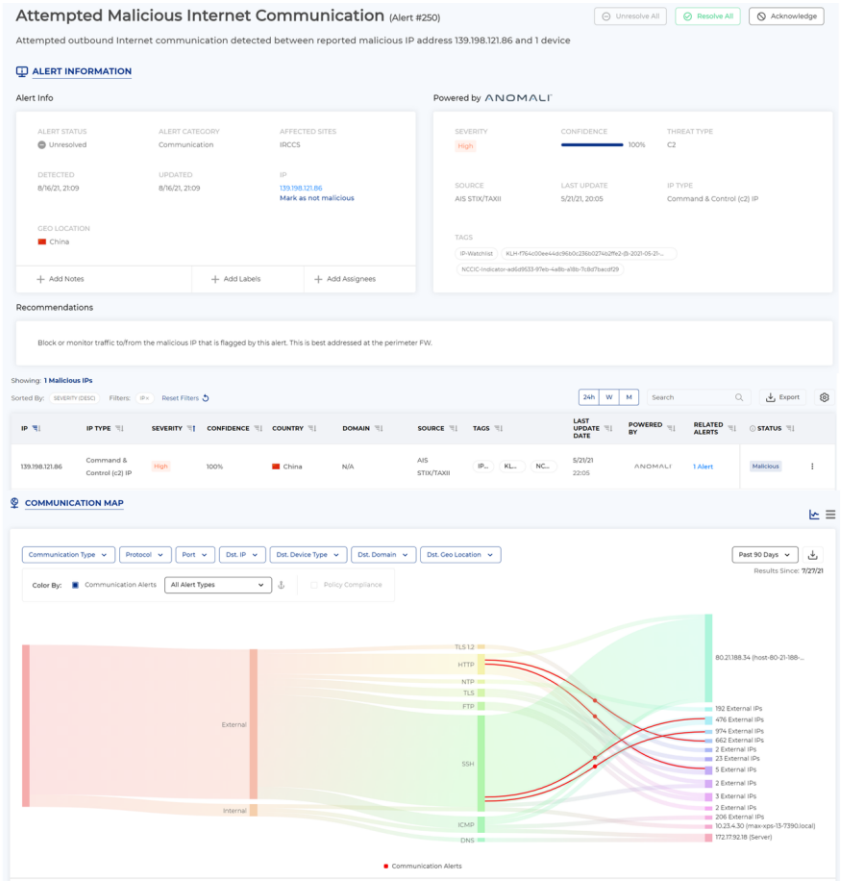
Recommendation

Search

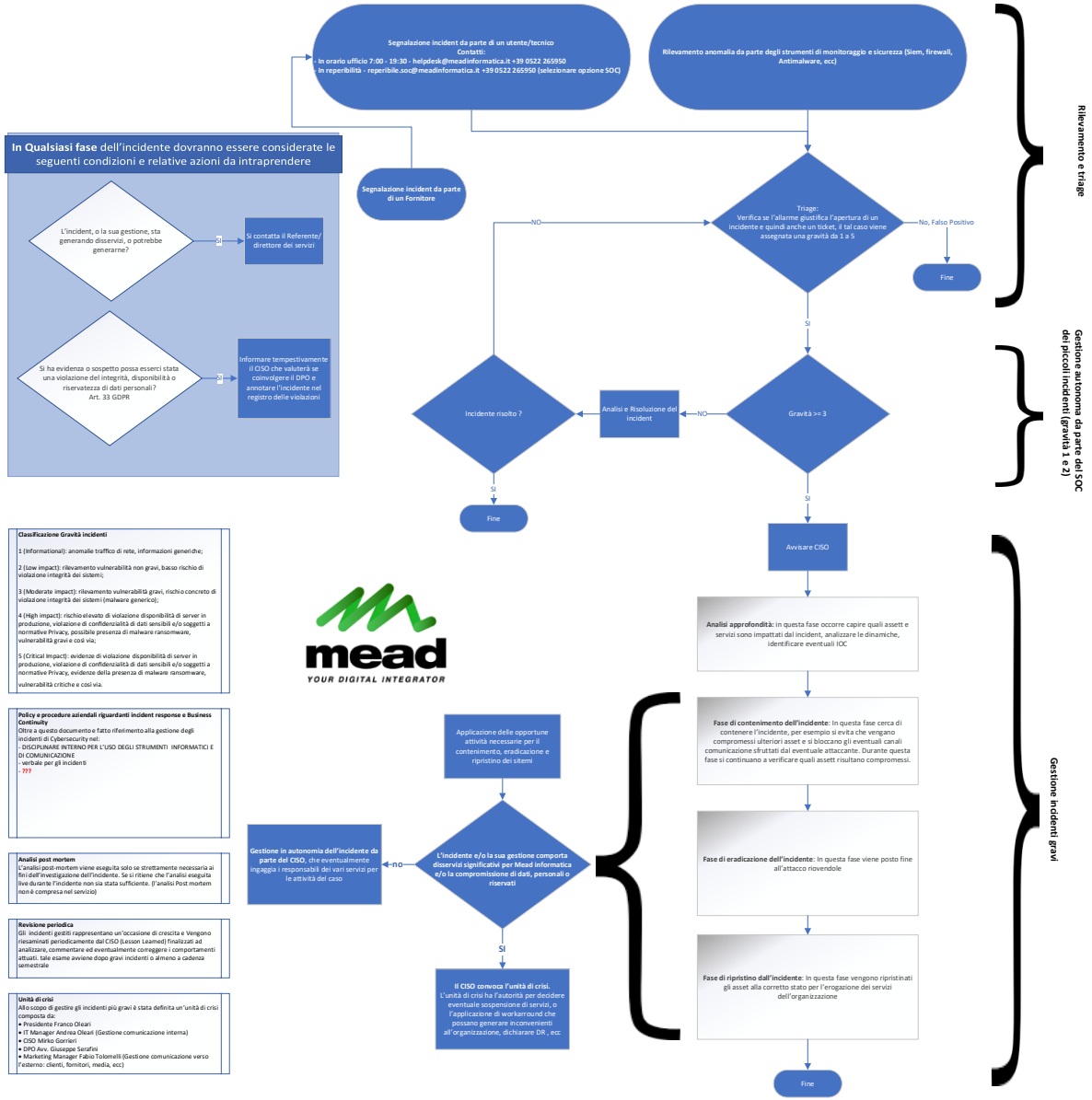
RULE NAME	IP PROTOCOL	PROTOCOL	DEVICE PORTS	DST PORTS	DST IP	DST DEVICE CONDITIONS	RULE SOURCE	RULE ACTION
DHCP	UDP	DHCP	68	67	any	N/A	Medigate	Allow
DICOM	TCP	DICOM	1177	any	any	N/A	Medigate	Allow
DICOM	TCP	DICOM	any	1177	any	N/A	Medigate	Allow

Control Room

Detect - Responde - Monitoraggio degli eventi e gestione degli incidenti



Flusso di gestione degli incidenti di Cybersecurity



RECOVERY - Data Recovery

plore

Forbes

May 17, 2017, 09:00am EDT

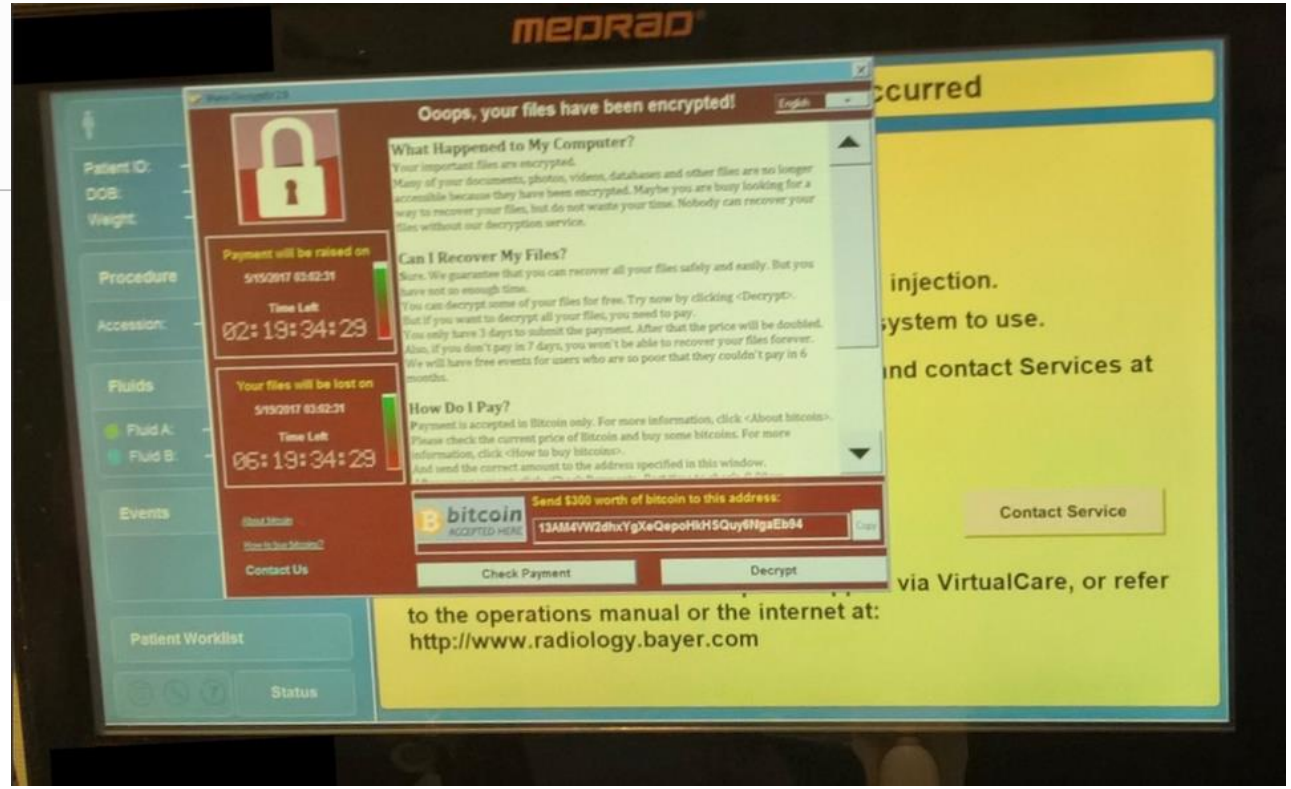
Medical Devices Hit By Ransomware For The First Time In US Hospitals

Thomas Brewster Forbes Staff

Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

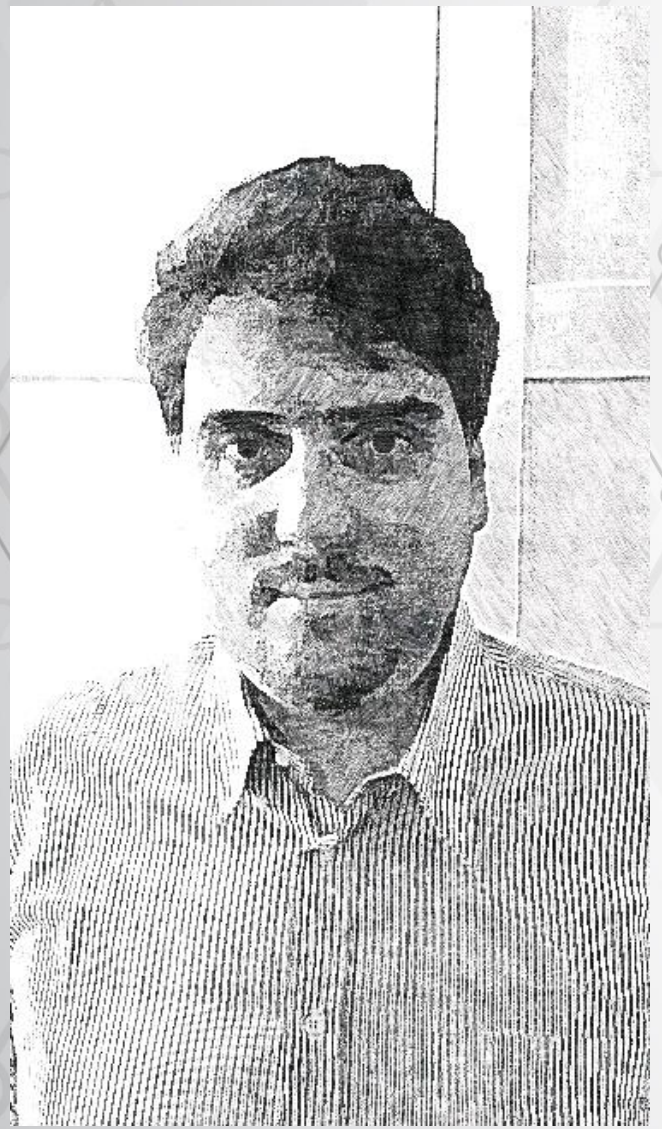
This article is more than 4 years old.



A Bayer MedRad device used to assist in MRI scans infected with the WannaCry ransomware.
WANNACRY RANSOMWARE ON A BAYER RADIOLOGY SYSTEM

mead
YOUR DIGITAL INTEGRATOR

Fonte https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/?sh=6d7ade37425c



Vi ringrazio per la vostra attenzione

Mirko Gorrieri

m.gorrieri@meadinformatica.it

https://www.linkedin.com/in/mirko-gorrieri-21b37399

www.meadinformatica.it

Qualificato **Privacy Manager**

Qualificato Lead Auditor UNi ISO/IEC 27001:2017 **Sistemi di gestione per la sicurezza della informazioni**

Qualificato UNI ISO 31000:2018 **Risk Management**

Qualificato Lead Auditor UNi ISO/IEC 22301:2019 **Continuità operativa**

Microsoft Certified Professional

BooleBOx Core Technical Specialist

Qualys certified specialists

Trend Micro Certified Professional