28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

L'evoluzione della sicurezza nella sanità 4.0

Camillo Bucciarelli – Sales Engineer Trend Micro

@ForumRisk www.forummediterraneosanita.it

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI

6° Forum Mediterraneo 2022 in Sanità®

Trend Micro: 30 anni nella sicurezza informatica

Oltre $1.9B di fatturato nel 2021 e sempre in attivo dal 1998.

Oltre 500,000 client in oltre 200 nazioni, incluse 9 aziende su 10 del Global Fortune 500

7000 persone appassionate di sicurezza in 65 nazioni

Oltre 40 persone nel team italiano

Eva Chen, CEO e Co-founder

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Ransomware e **attacchi avanzati** verso sanità ed enti governativi in aumento

- Gli attacchi Ransomware continueranno ad aumentare nei numeri e nei profitti generati
- Nel 2021 la sanità ha rappresentato il **13% del totale degli attacchi** Cyber in italia, **in crescita del 24,8%** rispetto al 2020*
- Il furto e la vendita di dati della vittima si accompagna sempre più spesso alla richiesta di riscatto

Come proteggersi?

- Strumenti di Endpoint Protection di nuova generazione, Virtual patching ed eXtended Detection and Response riducono il rischio di attacchi avanzati
- Una buona strategia di backup, anche offline, riduce il rischio di perdita dei dati
- Riconoscere e bloccare nel più breve tempo possibile l'azione di ransomware e botnet, in aggiunta a funzionalità DLP, riduce il rischio di furto dei dati.

@ForumRisk www.forummediterraneosanita.it

* Fonte: rapporto clusit 2022

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Sistemi obsoleti in produzione sono facili vittime

- Apparati elettromedicali o industriali hanno una vita molto più lunga dei sistemi di controllo
- Computer con sistemi di gestione obsoleti o apparati non aggiornabili presentano **vulnerabilità** facilmente sfruttabili
- Anche in presenza di patch l'installazione richiede tempi lunghi ed espone le reti a rischio di attacco

Come proteggersi?

- Soluzioni di sicurezza di tipo network con virtual patching, unite a segmentazione della rete, riducono il rischio di infezione e propagazione del malware
- Soluzioni Endpoint Protection in grado di assicurare funzionalità (anche ridotte) su sistemi obsoleti riducono la finestra di rischio
- Definire finestre di manutenzione critica per i sistemi ancora supportati

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Aumentano gli attacchi a reti OT, spesso meno protette

- I sistemi elettromedicali sono sempre più connessi e dipendenti dalla rete (es: tramissione dei risultati, tele assistenza)
- Dispositivi IoT e IoMT sono ormai di uso comune
- Soluzioni IT tradizionali sono poco o del tutto inefficaci in reti OT ed IoT
- Il blocco del sistema informatico di un ente sanitario può portare al blocco o il ritardo nell'erogazione dei servizi verso i cittadini

Come proteggersi?

- Prodotti di sicurezza specifici per il mondo OT/IoT sono più efficaci di soluzioni pensate per l'IT, non in grado di analizzare protocolli native di impianti industriali
- L'utilizzo di una soluzione di sanificazione senza agent (portable) consente un rapido ripristino dei servizi su macchine che non possono utilizzare un agent a bordo.

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Il mercato richiede **competenze specifiche** sempre più rare

- L'utilizzo di strumenti di sicurezza avanzati richiede **competenze specifiche** sempre più difficili da reperire sul mercato*
- La frammentazione degli strumenti di sicurezza aumenta il tempo di analisi e riduce l'efficacia, perdendo il quadro d'insieme
- Attacchi di Social Engineering che fanno leva sulle persone e strumenti leciti (Es: VNC, E-Mail) sono i più difficili da intercettare e mitigare

Come proteggersi?

- Soluzioni eXtended Detection and Response correlano in modo autonomo le informazioni da fonti eterogenee ed evidenziano solo situazioni di reale pericolo.
- Servizi di Managed Detection and response consentono di sgravare i propri specialist dei compiti di analisi concentrandosi solo su attività a valore aggiunto e di risposta.
- La formazione continua del personale, coadiuvata da materiale formativo aggiornato, rimane la migliore strategia di difesa.

28-30 SETTEMBRE 2022
BARI | VILLA ROMANAZZI CARDUCCI
6° Forum Mediterraneo 2022 in Sanità®

Grazie

Camillo Bucciarelli – Sales Engineer Trend Micro
camillo_bucciarelli@trendmicro.com

@ForumRisk www.forummediterraneosanita.it

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Torna all'inizio