Il Sole 24 ORE

diffusione:87934
tiratura:130903

Cybersecurity

Scenari

Strategie

Ospedali sotto scacco Assalto cybercriminale

Nel mirino degli hacker dispositivi medici come la risonanza magnetica e le macchine per i raggi X

di **Alessandro Longo**

I cyber criminali si stanno specializzando nell'attacco alla Sanità e mirano anche alle macchine a raggi X o per le risonanze magnetiche. Lo segnala un recente rapporto di Symantec e dà bene la cifra di come stia evolvendo il problema della cyber security nel settore sanitario. I numeri sono in crescita, certo – le infezioni sono triplicate nel 2017, secondo McAfee, mentre secondo Data Breach Investigations 2018 di Verizon riguarda la Sanità il 24 per cento degli attacchi "a ricatto" (ransomware), contro il 17 per cento dell'anno prima.

La notizia riportata da Symantec, però, segnala anche qualcosa di più rispetto a una crescita quantitativa del fenomeno. È indizio di un suo cambio di passo, per due motivi. Ci dice che c'è un gruppo di hacker specializzato nella Sanità ("Orangeworm"). E che ha preso il controllo macchine della sanità (soprattutto negli Usa) al solo scopo apparente di studiarle, scoprirne le vulnerabilità, per poi probabilmente – questa l'ipotesi degli analisti – condurre un attacco su larga scala.

Finora le cronache ci dicono che ci sono stati due tipi di attacchi in Sanità: per rubare i dati degli utenti e per chiedere un riscatto via ransomware (con Wannacry e Petya, malware che hanno paralizzato molti ospedali nel mondo). I dati più a rischio, secondo McAfee, sono quelli nei Pacs, i sistemi usati dai laboratori per archiviare i risultati degli esami e renderli disponibili via internet.

In pericolo sono quindi sia la privacy sia il funzionamento delle strutture sanitarie. Il tutto con ricadute, sulle persone, potenzialmente molto più gravi rispetto ad altri attacchi cyber. Primo perché quelli sanitari sono tra i dati più sensibili che ci siano, come riconosciuto anche dalle norme in materia di privacy. Secondo perché il blocco di un ospedale (a scopo di ricatto o anche, in futuro, terroristico) può causare una strage.

Come ricorda Luigi Romano, docente all'università di Napoli, tutto questo è il rovescio della medaglia rispetto alla trasformazione digitale, "che ha diffuso le soluzioni di tele monitoraggio, gli archivi digitali dei dati sanitari, la connessione di macchine, apparecchi". Succede anche in Italia, sebbene con lentezza, con progetti come il Fascicolo sanitario elettronico e la Cartella clinica elettronica.

"I punti critici sono la conservazione dei dati, l'accesso, lo scambio e la loro modifica", aggiunge.

"La crescita del cyber crime in Sanità si spiega con facilità. Questa infatti è una vittima perfetta", dice Corrado Giustozzi, tra i massimi esperti di cyber security. Per tre motivi. "La Sanità ha molto da perdere da un attacco cyber; vi è molto esposta (per via della crescente digitalizzazione) ed è ben poco protetta (le infrastrutture ict sanitarie sono spesso obsolete, molti apparecchi vanno ancora su Windows XP)".

Ad accrescere il problema è che le istituzioni solo di recente hanno cominciato a inquadrare la questione. A partire dagli Stati Uniti, dove la Food and Drug Administration ha appena lanciato un piano di azione per la sicurezza dei dispositivi medici, chiedendo la collaborazione dei produttori. In Italia il tutto sarà più complicato a causa della frammentazione della governance in Sanità.

"Bisogna sfruttare non solo la leva normativa (le prescrizioni di Agid – Agenzia per l'Italia Digitale -, il framework nazionale per la Cybersecurity del Cini, il GDPR), ma anche portare a fattor comune casistiche, problemi ed esigenze", dice Gabriele Faggioli, presidente del Clusit, docente del Politecnico di Milano e ceo di P4I.

"Sarebbe utile anche un accentramento delle infrastrutture, delle applicazioni e delle basi dati per poter razionalizzare il sistema, ridurre i costi e liberare risorse per investire in sicurezza", aggiunge. Adesso è in corso la seconda fase censimento Agid dei datacenter, per poi accentrarli.

La sensazione è che – stavolta molto più del solito – i "buoni" siano parecchio in ritardo, rispetto alla corsa che i "cattivi" hanno avviato per mettere le mani sulla Sanità. Le manovre di Orangeworm lasciano pensare che il brutto, per la Sanità di fronte al rischio cyber, deve ancora venire.

L'appuntamento

nòva Cyber Security L'EVOLUZIONE DELLA SICUREZZA NELL'ECOSISTEMA 4.0

TAPPA A NAPOLI PER LA CYBERSECURITY

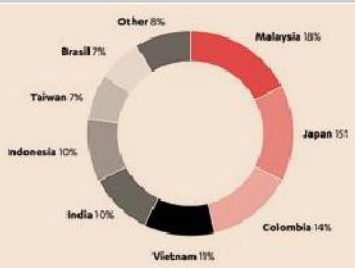
L'evoluzione della sicurezza nell'ecosistema 4.0 è al centro della nuova tappa del roadshow di Nòva che si svolgerà a Napoli, a Villa Doria D'Angri il 21 maggio prossimo.


Ospedali sotto scacco
Assalto cybercriminale

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

Il Sole 24 ORE

diffusione:87934
tiratura:130903



LA FINE DEI RANSOMWARE

Gli attacchi ransomware sono cresciuti in volume di oltre il 400% nel 2017 rispetto al2016. In un nuovo report F-Secure attribuisce questa crescita al cryptoworm WannaCry, ma sottolinea anche che altri attacchi ransomware sono diventati meno comuni nel corso del 2017, un cambiamento nell'utilizzo del malware

160 HACKER A ROMA

Alla fine di giugno a Roma si terrà la competizione finale della seconda edizione di CyberChallenge.IT, il programma annuale organizzato dal Laboratorio Nazionale di Cybersecurity del CINI per selezionare i migliori talenti informatici del paese tra i 16 e i 22 anni. In lizza 160 giovani hacker.

GIORNATA DELLE PASSWORD

Secondo una ricerca della società di sicurezza McAfee, gli utenti hanno in media 23 account online per cui è necessaria una password, ma utilizzano solo 13 password uniche per questi account. Il modo più comune per ricordare le parole chiave è quello di tenere una lista scritta o digitale di tutte (52%)

La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato