"Ecco perché la Sanità è sotto attacco dei cyber criminali. Anche IA e Cyber Threat Intelligence per proteggere i dati"

LUIGI GAROFALO — 12 GIUGNO 2023 — CYBER CHAT, ITALIA

L'intervista a Roger Cataldi, CISO & Head of Cyber Security – Almaviva.

Cybersecurity Italia. *Secondo lei, perché la Sanità italiana, sempre più spesso, è vittima, con successo, dei cyber criminali?*

Roger Cataldi. Il fatto che la Sanità sia sotto attacco è un segnale e una conferma dell'evoluzione della catena del (dis-)valore del Sistema Criminale. È ormai noto, infatti, che il cybercrime è sempre più integrato in un ecosistema delinquenziale che prende di mira i settori su cui strategicamente è possibile massimizzare i profitti criminali. La spesa sanitaria pro-capite in Italia è pari a **2.473 euro**, stando all'ultimo report dell'**OCSE** *"Health at Glance Europe 2020"*, per un totale di oltre **146 miliardi di euro l'anno**, in un settore complesso, disomogeneo e frammentato e poco maturo dal punto di vista dei sistemi IT e IOT. Questa condizione

Roger Cataldi

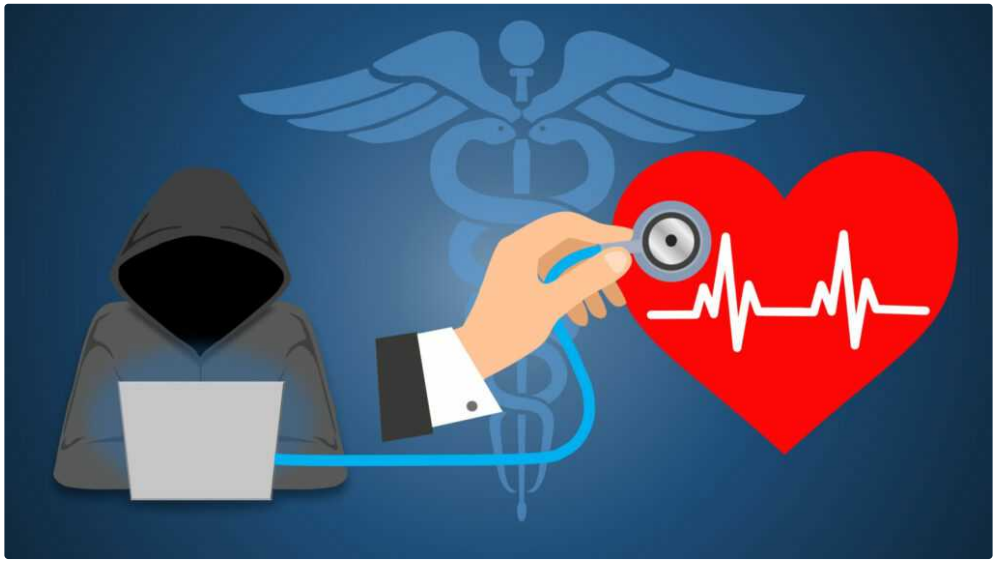
rappresenta un ghiotto bersaglio per la criminalità organizzata e in particolare, per la criminalità che accede al *Cybercrime as a Service,* ovvero professionisti e organizzazioni delittuose che hanno sviluppato tool e servizi "pronti all'uso" acquistabili per portare avanti attacchi complessi anche senza il know-how tecnico necessario.

Un ulteriore problema è rappresentato dalla mancanza di consapevolezza dell'importanza della sicurezza informatica nel settore sanitario. A differenza di altre organizzazioni più orientate verso la digitalizzazione, le strutture sanitarie spesso hanno dedicato meno risorse alla sicurezza dei dati e alla formazione del personale in materia di cybersecurity. Questo ritardo nell'affrontare le minacce informatiche ha reso le strutture sanitarie più vulnerabili agli attacchi.

Il settore sanitario deve affrontare sfide specifiche a causa delle dimensioni complesse dell'informatica nel contesto medico. Oltre alla gestione dei dati amministrativi e sanitari, ci sono anche aspetti tecnici legati all'ingegneria clinica, come la sicurezza dei dispositivi medici e dei macchinari. La compromissione di tali dispositivi potrebbe causare danni gravi ai pazienti.

Affrontare queste sfide richiede un impegno congiunto da parte delle strutture sanitarie, del personale medico, degli esperti di sicurezza informatica e delle istituzioni.

È fondamentale investire nella formazione del personale sanitario per aumentare la consapevolezza della sicurezza informatica e promuovere una cultura della cybersecurity nelle strutture sanitarie. Anche se è incoraggiante rilevare che fino ad oggi gli attacchi subìti siano stati principalmente di natura opportunistica, le strutture sanitarie, specialmente quelle di emergenza, sono considerate infrastrutture critiche e devono essere protette adeguatamente perché un attacco informatico coordinato con altre azioni potrebbe avere conseguenze importanti per il funzionamento dei servizi sanitari.



Cybersecurity Italia. ***Gli attaccanti per quale motivo, dal suo punto di vista, prendono di***

mira Asl e ospedali italiani pubblici se nel nostro Paese il riscatto, a livello di pubblica amministrazione, non viene mai pagato?

Roger Cataldi. Fino ad oggi, non sono stati segnalati casi noti di strutture sanitarie italiane che abbiano pagato riscatti a seguito di attacchi informatici. Tuttavia, diversi studi di settore hanno dimostrato che una percentuale dei soggetti ricattati paga, come evidenziato nelle analisi riferite ai crypto wallet.

Le strutture sanitarie sono particolarmente vulnerabili agli attacchi informatici a causa della loro complessità IT/OT, della quantità considerevole di dati sanitari e dei servizi critici forniti ai cittadini e ai pazienti. Ciò le rende appetibili per l'underground e le associazioni criminali che operano nel mercato illegale dei servizi di attacco informatico e rivendita di dati. L'utilizzo di acronimi come **CaaS** (Crime as a Service) o **RaaS** (Ransomware as a Service) rappresenta questa realtà.

La notorietà delle strutture sanitarie colpisce sia nell'underground sia sui media globali, creando una pressione aggiuntiva per cedere al ricatto. Questo dimostra che gli attaccanti non stanno bluffando e aumenta la percezione della minaccia.

È fondamentale che le strutture sanitarie rafforzino le misure di sicurezza informatica per mitigare il rischio di attacchi. Ciò include l'implementazione di sistemi di protezione avanzati, l'aggiornamento regolare del software e la sensibilizzazione del personale sulla sicurezza informatica. Inoltre, la condivisione delle informazioni e la collaborazione tra le organizzazioni sanitarie sono essenziali per sviluppare strategie comuni di difesa e prevenire futuri attacchi.

Cybersecurity Italia. ***E all'estero, la PA paga il riscatto?***

Roger Cataldi. La situazione varia da Paese a Paese e da caso a caso ma lo stato di fragilità che viviamo non è affatto un'esclusiva italiana, anzi. Le cybergang in questi ultimi anni stanno trovando particolare soddisfazione con i Paesi in via di sviluppo in particolare l'Africa e il sud America, dove gli analisti di settore dicono che sono i maggiori pagatori di riscatti. C'è da considerare anche che la sanità in molti Stati è gestita da privati e questo potrebbe essere anche una delle ulteriori ragioni per cui il pagamento del riscatto può risultare più semplice rispetto una pubblica amministrazione.

Cybersecurity Italia. ***Dal suo osservatorio, le risulta che, invece, nel mondo privato italiano il riscatto venga pagato per riavere i dati? Se sì, a quanto ammonta questa percentuale?***

Roger Cataldi. Non ho informazioni a riguardo ma da quello che osserviamo sui crypto wallet dei cyber criminali c'è movimento e, seppur in forma minore, anche in Europa si pagano riscatti e le primarie categorie coinvolte sono i settori finanziari, industriali e di servizi legali.

Cybersecurity Italia. ***In generale, quali sono i motivi per cui i cyber attaccanti sferrano un attacco informatico a una struttura sanitaria?***

Roger Cataldi. Le strutture sanitarie sono vulnerabili a livello tecnologico e organizzativo, principalmente a causa della commistione tra ambienti IT e OT, sistemi operativi obsoleti e mancanza di supporto.

Questi fattori ampliano la superficie di attacco e rendono le strutture più fragili. Il non aggiornamento dei sistemi porta al blocco di applicazioni personalizzate e alla mancata installazione delle patch di sicurezza, aumentando il rischio complessivo.

La nostra indagine ha evidenziato un'alta esposizione alle vulnerabilità, rendendo relativamente facile per i malintenzionati ottenere il controllo dell'amministrazione. I dati possono essere esfiltrati in modo discreto e i sistemi possono essere cifrati, coinvolgendo anche i backup, se presenti.

Un altro aspetto critico è la mancanza di una gestione efficace delle identità degli amministratori di sistema. Le cyber gang possono acquistare identità già qualificate e verificate attraverso intermediari, ottenendo l'accesso alle reti aziendali tramite VPN, operando come amministratori senza ostacoli e in modo persistente.

Per garantire una maggiore sicurezza, è necessario affrontare le vulnerabilità tecniche, migliorare la gestione delle identità e adottare misure preventive adeguate a proteggere le strutture sanitarie in ambito Cyber.

Cybersecurity Italia. ***La Sanità è il terzo settore più colpito al mondo dai cyber gang. Come mettere meglio in sicurezza i dati sanitari e sensibili dei pazienti in Italia?***

Roger Cataldi. Per migliorare la sicurezza dei dati sanitari e sensibili dei pazienti in Italia, è necessario che il personale sanitario venga adeguatamente formato sulle pratiche di sicurezza

informatica; l'utente è sempre la prima vulnerabilità in un sistema perfetto e il consapevolizzarlo dei rischi è determinante nella prevenzione degli attacchi informatici.

Analizzando la kill chain dei recenti attacchi, vanno messe in priorità:

- le attività di bonifica delle utenze mai attivate, delle utenze inutilizzate da tempo e quelle che non rispettano le policy della complessità della password.
- Implementare misure di sicurezza informatica avanzate come crittografare i dati sensibili,
- creare copie di backup regolari,
- utilizzare l'autenticazione multi-fattore per confermare gli accessi ai sistemi aziendali
- e, naturalmente, mantenere i sistemi e i software in uso aggiornati.
- Infine, la conduzione periodica di assessment per identificare e mitigare le vulnerabilità, concentrando l'attenzione sulle piattaforme dismesse o abbandonate che potrebbero estendere la superficie d'attacco. Ovviamente per affrontare seriamente questa domanda servirebbe molto più tempo ma le recenti analisi identificano essere questi gli elementi da attenzionare.

Cybersecurity Italia. ***In che modo "una mano" può venire dall'intelligenza artificiale?***

Roger Cataldi. L'intelligenza artificiale potrà offrire un aiuto significativo anche nella protezione dei dati sanitari. Può essere utilizzata per rilevare e prevenire attacchi informatici, identificare comportamenti anomali nei sistemi informatici, migliorare la sicurezza delle reti e dei dispositivi, nonché per analizzare grandi quantità di dati al fine di individuare potenziali vulnerabilità. L'IA può quindi svolgere un ruolo importante nella difesa delle infrastrutture sanitarie da minacce cibernetiche.

Nel breve e medio termine sarà sempre più utilizzato nell'ambito sanitario lo strumento tecnologico dell'Intelligenza Artificiale in tutte le sue possibili declinazioni e potenzialità.

A questo proposito sarà sempre più strategica la sinergia tra specialisti di settore verticali nell'ambito della Sanità con analisti e professionisti della cybersecurity, fin dalle prime fasi della progettazione dei nuovi sistemi sanitari.

Cybersecurity Italia. ***Cos'altro vuole aggiungere?***

Roger Cataldi. Al miglioramento delle difese informatiche sarebbe fondamentale abbinare servizi di Cyber Threat Intelligence con focus dedicato all'universo sanitario.

Fare intelligence sulle minacce può giocare un ruolo fondamentale nella prevenzione migliorando l'esposizione al rischio delle organizzazioni, in questo caso, sanitarie.

Elenco alcuni modi in cui, un servizio di intelligence dedicato, può essere fattore di successo nell'ambito della prevenzione:

1. **Rilevazione precoce delle minacce**: la threat intelligence permette di monitorare costantemente l'ambiente digitale alla ricerca di segnali di attività sospette o di potenziali minacce. Questo consente di rilevare precocemente gli attacchi informatici in corso o in fase di preparazione, consentendo alle strutture sanitarie di prendere misure preventive o reattive tempestive.

2. **Analisi delle tendenze:** la threat intelligence fornisce un'analisi approfondita delle tendenze nel panorama delle minacce informatiche. Questo permette alle strutture sanitarie di comprendere meglio le tattiche, le tecniche e le procedure utilizzate dagli attaccanti, nonché le nuove minacce emergenti. Questa conoscenza consente di adattare e potenziare le difese per affrontare le minacce più recenti.

3. **Informazioni sulle vulnerabilità**: la threat intelligence fornisce informazioni sulle vulnerabilità dei sistemi, delle applicazioni e delle infrastrutture utilizzate nelle strutture sanitarie. Questo permette di identificare le debolezze e prendere le misure necessarie per mitigare i rischi associati. Ad esempio, consente di applicare patch di sicurezza, configurare correttamente i sistemi e implementare misure di protezione aggiuntive.

4. **Condivisione delle informazioni**: la threat intelligence favorisce la condivisione di informazioni tra le strutture sanitarie, consentendo loro di apprendere dalle esperienze degli altri e di beneficiare di best practice condivise. Questa collaborazione può contribuire a una migliore comprensione delle minacce e delle strategie di difesa efficaci.

5. **Valutazione del rischio**: la threat intelligence fornisce una valutazione continua del rischio associato alle minacce digitali. Attraverso l'analisi dei dati e delle tendenze, è possibile valutare il livello di rischio specifico per le strutture sanitarie e concentrare le risorse di sicurezza sulle aree più critiche.

Complessivamente, l'utilizzo della threat intelligence aiuterebbe le strutture sanitarie a migliorare la loro preparazione e capacità di risposta agli attacchi informatici, riducendo l'esposizione al rischio e proteggendo i dati sensibili dei pazienti.

PRECEDENTE

International Cybersecurity Challenge (ICC), presentato il Team europeo. Lepassaar (Enisa): "Abbiamo talenti pronti a soddisfare le esigenze del mercato del lavoro europeo della cybersecurity"

SUCCESSIVO

Leonardo e Roma Capitale, al via l'accordo per formare i giovani in cybersicurezza