La nuova inquietante tendenza nel Cybercrime: colpire gli ospedali

Date : 1 settembre 2016

Il 2016 ha visto tra le strutture più colpite dagli hackers proprio gli ospedali.

Nella maggior parte dei casi registrati, i sistemi di attacco agiscono infettando le reti ospedaliere tramite programmi Trojan, ovvero malware che nascondono il loro funzionamento all'interno di altri programmi apparentemente innocui, i quali a loro volta innescano un ransomware che cripta e rende dunque incomprensibili i dati nel sistema colpito. Per riottenere il ripristino dei dati in molti casi si richiede il pagamento di un riscatto alle strutture ospedaliere coinvolte.

Per riportare qualche esempio: a febbraio l'Hollywood Presbyterian Medical Center di Los Angeles ha perso l'accesso ai propri sistemi informatici e ha dovuto pagare un riscatto; nello stesso mese due strutture ospedaliere tedesche, il Lukas Hospital e la Klinikum Arnsberg, hanno subito un attacco simile.

Analizzando la situazione, questa nuova tendenza non stupisce affatto.

Le reti ospedaliere, supportate da sistemi obsoleti e spesso gestite da dipendenti con minima e insufficiente formazione informatica, risultano vittime perfette per questo tipo di attacchi.

A volte gli ospedali non possono permettersi la sospensione dell'attività dei loro sistemi necessaria ad eseguire un backup e tanto meno sono disposti a combattere l'attacco, dovendo dunque sospendere i servizi, preferendo pagare e rendendosi così molto vulnerabili. Simili accessi non autorizzati possono risultare più pericolosi di quanto si possa immaginare; il rischio non riguarda solamente il furto di dati personali, già molto grave di per sè, ma potrebbe influenzare direttamente la salute degli stessi pazienti. Immaginate uno scenario in cui i criminali informatici abbiano ottenuto pieno accesso alle infrastrutture mediche e siano in grado di manipolare i risultati dei sistemi di diagnosi e di trattamento.

In molti casi risultati e analisi cliniche dipendono in larga misura da sistemi d'elaborazione tecnologica e una manipolazione degli stessi potrebbe comportare la somministrazione di un trattamento sbagliato ad un qualsiasi paziente peggiorandone eventualmente la condizione medica.

Fortunatamente finora non è stato registrato nessun attacco di simile portata.

Nel caso del Lukas Hospital, ospedale tedesco sopracitato e vittima d'attacco, un ransomware ha criptato dati medici relativi solamente a qualche ora d'attività.

Tuttavia, nonostante l'efficienza tedesca nel rilevare l'emergenza ed elaborare una strategia di difesa, i danni non sono stati affatto trascurabili. Gli hackers sono penetrati nella email della struttura impedendo l'accesso agli addetti, lo staff tecnico ha impiegato settimane per far tornare il sistema di posta elettronica alla normalità.

Il personale è stato costretto a contattare telefonicamente ogni paziente per informarlo dell'accaduto e nelle settimane necessarie al ripristino la comunicazione struttura-fruitori è tornata ad essere quella di almeno 15 anni fa: telefono, fax, carta e penna. Sebbene in piccola percentuale, circa 1 su 5, alcuni interventi chirurgici ad alto rischio sono stati rimandati.

Questo ci fa comprendere come non sia necessario un attacco di enormi dimensioni per causare disagi gravissimi, basta infatti rallentare l'attività medica per, ad esempio, intralciare interventi chirurgici d'urgenza in cui la velocità d'azione è fondamentale.

Anche la Klinikum Arnsberg ha subito l'attacco di un ransomware, si pensa che l'innesco sia stato causato dall'apertura da parte dello staff di un allegato infetto in una mail ricevuta. Fortunatamente uno solo dei 200 software della clinica è stato attaccato prima che venisse staccata la connessione e quindi fermata la crittografia dei files; il recupero degli stessi è avvenuto senza troppe difficoltà grazie a precedenti ed efficienti backup.

Più ingenti sono stati invece i danni al già citato Hollywood Presbyterian Medical Center, tanto che l'FBI e il Dipartimento di Polizia di Los Angeles sono stati chiamati ad indagare sull'accaduto. L'attacco ha praticamente "spento" il sistema informatico dell'ospedale, il personale ha cominciato a notare significativi problemi IT ed è stato dichiarato uno stato di emergenza interna. Il Presidente e Direttore della struttura ha sostenuto che la salute dei pazienti non è stata influenzata dall'attacco del ransomware ammettendo però che i pazienti sono stati dirottati verso altri ospedali. Indiscrezioni sembrano rivelare che inizialmente, in cambio delle chiavi di crittografia per ripristinare il sistema, gli hackers avrebbero richiesto 9.000 BTC - il valore del bitcoin varia di giorno in giorno, al momento dei fatti l'equivalente era di circa 3,6 milioni di dollari.

Alla fine, dopo ben dieci giorni di paralisi, i dirigenti dell'ospedale hanno ceduto pagando il riscatto ai criminali informatici che gestivano l'attacco: 40 bitcoin, equivalenti al momento del pagamento a circa 17.000 dollari.

Questa nuova "moda criminale" colpirà anche i nostri ospedali?