Versione italiana

GLI ATTACCHI AL SISTEMA SANITARIO AI TEMPI DEL COVID-19

I GAP DI SICUREZZA, CONFORMITÀ NORMATIVA E CONSAPEVOLEZZA DEL PERSONALE SANITARIO

ALESSANDRO SCARAFILE

« La ricerca del consenso crea mediocrità.
La creatività si annida nel momento di massima insicurezza. »

Alessandro Scarafile

ex Operations Manager
Hacking Team

SOMMARIO

INTRODUZIONE

Il 4 Aprile 2020 l'Interpol ha lanciato un allarme a tutti gli organi di polizia dei 27 Paesi membri dell'Unione Europea, sull'incremento degli attacchi informatici alle strutture sanitarie. L'allarme ha seguito quello lanciato a metà Marzo dall'agenzia inglese NCSC (National Cyber Security Center).

Il 23 Aprile 2020 l'Organizzazione Mondiale della Sanità ha pubblicamente dichiarato di aver registrato un drammatico aumento del numero di attacchi informatici, diretti al proprio personale via e-mail: oltre 450 utenti e password di personale OMS sono stati divulgati online, insieme ad altre migliaia di indirizzi relativi a soggetti esterni che collaborano sulla risposta al Covid-19.

L'industria sanitaria è un **obiettivo primario** per i criminali informatici. Le informazioni sanitarie protette valgono migliaia di euro sul mercato nero: la sanità è quindi vista come una gallina dalle uovo d'oro.

Il crescente utilizzo di dispositivi medici connessi, attrezzature e altri dispositivi IoT, ha registrato un significativo aumento di attacchi basati principalmente sull'ingenuità del personale sanitario e normalmente realizzati con l'invio di e-mail che richiedono l'apertura di link o allegati, causando l'installazione di Ransomware all'interno della rete dell'intera struttura sanitaria.

Questo white paper esamina i principali problemi di sicurezza che devono affrontare le normative di settore e di conformità sanitaria, oltre ai vantaggi della formazione sulla consapevolezza della sicurezza per l'intera forza lavoro.

1. LE PREOCCUPAZIONI

Un rapporto del 2019 di Egress ha rilevato che il 79% dei leader IT affermava che i dipendenti avevano accidentalmente posto dati sensibili a rischio di esposizione. Il 60% ha inoltre affermato di temere una violazione accidentale dei dati nei 12 mesi successivi.

Alcuni esempi di esposizione accidentale di informazioni sanitarie protette:

Caso	Scenario
Smarrire o non proteggere dispositivi contenenti dati medici sensibili	Lasciare un laptop in un ristorante o collegare un dispositivo USB di dubbia provenienza
Non seguire appropriati standard aziendali di sicurezza	Utilizzare password deboli sui dispositivi
Pubblicazione inappropriata di informazioni private	Condividere informazioni sul trattamento di un paziente con un amico o un familiare che non ne ha diritto
Invio di dati sanitari sensibili al destinatario errato	Inoltrare informazioni ad un destinatario sbagliato (ad es. CC)
Violare la privacy di un paziente semplicemente per curiosità	Visualizzare le cartelle cliniche di pazienti noti e successivamente condividerne le informazioni con persone non autorizzate
Conservazione di informazioni riservate dopo il termine previsto	Cedere backup contenenti informazioni sensibili a qualcuno che non ha il diritto di visualizzarle
Abuso di privilegi	Fornire a qualcuno un accesso inappropriato ad un sistema per svolgere rapidamente un lavoro

1.1 ERRORI UMANI

Molti incidenti di sicurezza sanitaria derivano da errori umani prevenibili. Nel suo studio annuale sulla sicurezza dei dati sanitari, il Ponemon Institute ha riferito che la maggior parte dei furti di identità medica è prevenibile attraverso la formazione dei dipendenti sulla consapevolezza della sicurezza.

Il rapporto ha inoltre evidenziato che un aumento della formazione del personale, associato all'assunzione di professionisti della sicurezza IT più qualificati, potrebbe contribuire in modo significativo a migliorare le difese informatiche.

Il Data Breach Investigation Report del 2019 sottolinea che nell'assistenza sanitaria, più che in altri settori, le violazioni di sicurezza derivano da **abuso di privilegi**, **beni smarriti o rubati** e **attacchi web**.

Il rapporto ha anche identificato come gli incidenti interni, sia dannosi che accidentali, siano più comuni degli attacchi esterni.

Immagine 1: **Principali Cause di Violazioni alle Strutture Sanitarie**

1.2 ATTACCHI “CLASSICI”

I vettori di attacco “classici” continuano ad essere prevalenti. Un rapporto di Malwarebytes del 2019 sui tipi di attacchi all'assistenza sanitaria, ha rilevato un utilizzo massiccio dei seguenti metodi:

- Vulnerabilità in software di terze parti, sfruttando falle di sicurezza note e senza patch;
- Tecniche di Social Engineering come phishing e spear phishing, inviando e-mail, allegati e collegamenti dannosi.

Immagine 2: **Attacchi “Classici” alle Strutture Sanitarie**

Queste evidenze dimostrano come i criminali informatici sfruttino sia le vulnerabilità software che quelle degli utenti.

Fortunatamente, la formazione sulla consapevolezza della sicurezza e le simulazioni di attacco possono insegnare ai dipendenti come riconoscere le minacce più comuni come il phishing e la manipolazione dei collegamenti.

1.3 RANSOMWARE

Secondo Comparitech, tra il 2016 e il 2019 ci sono stati 172 attacchi ransomware mirati alle organizzazioni sanitarie statunitensi; i costi per l'industria sono di circa 157 milioni di $. Tra gli obiettivi colpiti, il 74% erano ospedali o cliniche.

Poiché queste strutture di terapia intensiva richiedono l'accesso H24 alle cartelle cliniche dei pazienti, hanno maggiori probabilità di accettare il pagamento di riscatti: ciò rende le strutture mediche un **obiettivo primario** per gli attacchi basati su ransomware.

La maggior parte degli incidenti ransomware deriva dalla condivisione involontaria di informazioni o da risorse rubate. Le vittime sono di solito colpite attraverso attacchi di phishing, che riscuotono molto successo poiché molti utenti sono inconsapevoli del funzionamento di questi metodi di attacco.

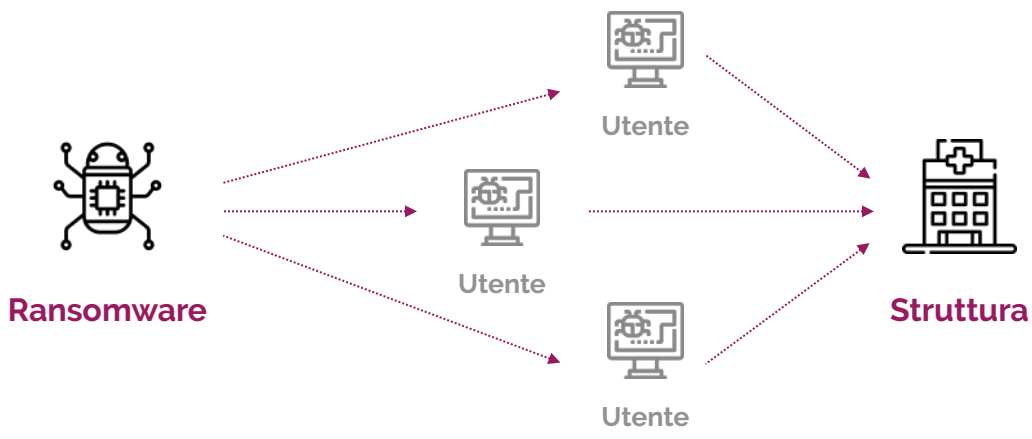

Immagine 3: **Attacchi Ransomware**

1.4 SICUREZZA ENDPOINT

L'uso di dispositivi medici connessi nell'assistenza sanitaria è cresciuto notevolmente, aumentando ulteriormente la vulnerabilità del settore agli attacchi esterni.

In un recente sondaggio Nuix svolto con 70 hacker professionisti e penetration tester, solo il 36% dei partecipanti ha identificato la sicurezza degli endpoint come un'efficace contromisura di hacking. Il 22% di questi white hacker, vantava inoltre come “nessuna contromisura di sicurezza potesse fermarli e che realizzare un accesso completo ai sistemi sarebbe stato solo una questione di tempo”.

Le strutture sanitarie con vincoli di bilancio per la sicurezza informatica dovrebbero prendere in considerazione l'assistenza professionale di un partner esterno per contrastare gli attacchi informatici ai dispositivi connessi.

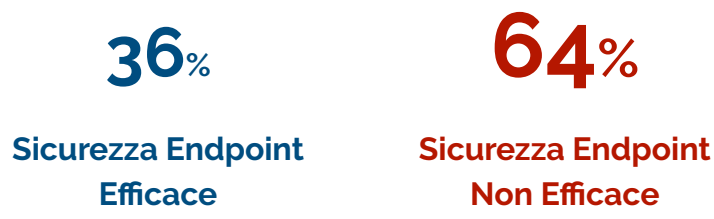

Immagine 4: **Percentuali Sicurezza Endpoint**

1.5 MINACCE INTERNE

Le minacce interne intenzionali continuano a tormentare il settore sanitario. In uno specifico rapporto su questo tipo di attacchi, Verizon ha scoperto che il 46% delle organizzazioni sanitarie risulta affetto.

Si tratta di una tra le più difficili tipologie da rilevare e mitigare. Il rapporto ha rilevato che gli addetti compromessi vengono “costretti, reclutati o corrotti” per rubare dati per conto di criminali informatici.

Altri motivi alla base di questi comportamenti scorretti possono essere i rancori, soprattutto nel caso di dipendenti scontenti. Dalla più grande struttura ospedaliera, alle strutture più piccole, nessuno è immune da questo tipo di violazioni interne.

All'inizio del 2020, un dipendente di una struttura ospedaliera del Maryland (Stati Uniti) ha utilizzato il suo accesso privilegiato alla rete per rubare i dati dei pazienti. Ha quindi usato i dati per ottenere in modo fraudolento i codici di diverse carte di credito. L'attività è stata scoperta dopo oltre due anni.

Immagine 5: **Cause di Minacce Interne**

1.6 TERZE E QUARTE PARTI

Molte strutture sanitarie esternalizzano oggi servizi come catering, buste paga e sviluppo web a fornitori di terzi parti. Questi fornitori hanno spesso accesso a informazioni riservate, che possono essere più vulnerabili agli attacchi dall'esterno dell'organizzazione, in particolare se la struttura sanitaria non ha piena visibilità su come un fornitore gestisce la sicurezza.

Nel 2019, il 54% delle violazioni di informazioni sanitarie protette negli Stati Uniti ha avuto origine a causa della scarsa valutazione del rischio nell'ecosistema del fornitore. Una violazione di questa natura costa in media ad un'organizzazione sanitaria una cifra di 2,75 milioni di $.

Di recente, la Croce Rossa australiana ha ingaggiato una società chiamata Precedent Communications per lo sviluppo di siti Web e la gestione di database. Un dipendente di Precedent che lavorava ad un progetto, ha eseguito il backup di un file di database contenente informazioni su donatori e lo ha inavvertitamente salvato su un server Web pubblico. Il server è stato successivamente violato, esponendo i record di 550.000 donatori di sangue.

La gestione dei rischi di quarte parti sta inoltre emergendo come nuova area di preoccupazione, per le organizzazioni sanitarie che esternalizzano certi servizi, poiché i fornitori di terze parti a loro volta si affidano ad altri fornitori. Questo pericolo è strettamente collegato all'IoT e al crescente utilizzo di dispositivi connessi. I dirigenti sanitari devono capire di avere poco o nessun controllo sui dati che escono dalle loro reti.

Negli Stati Uniti, l'HIPAA (Health Insurance Portability and Accountability Act) si applica praticamente a tutte le aziende e organizzazioni del settore sanitario e ai loro partner, anche se tali partner non sono tecnicamente coinvolti nell'assistenza sanitaria in alcun modo.

L'HIPAA richiede l'implementazione di un programma che garantisca la consapevolezza della sicurezza e la formazione di tutto il personale dell'organizzazione, e in particolare:

- Implementare procedure specifiche per rilevare o prevenire violazioni della sicurezza;
- Effettuare un'analisi dei rischi per determinare le potenziali vulnerabilità;
- Garantire che siano state prese adeguate misure di sicurezza per ridurre il rischio;
- Creare una politica di sanzioni per i membri del personale che non rispettano le procedure;
- Garantire che i registri delle attività del sistema informativo siano regolarmente rivisti.

Immagine 6: **Programma per la Consapevolezza alla Sicurezza**

In sintesi, le organizzazioni sanitarie devono disporre di un solido programma di sensibilizzazione e formazione sulla sicurezza e tutti i membri dell'organizzazione devono effettuare la formazione, inclusi dirigenti e management.

L'HIPAA è solo un esempio delle numerose normative americane di conformità che incidono sull'assistenza sanitaria. Oltre ad altre normative come PCI DSS, ogni stato americano ha anche un proprio insieme sovrapposto di leggi e regole applicabili al settore.

1.7 VINCOLI DI BILANCIO

Secondo Symantec, il settore sanitario spende molto meno in termini di tecnologia e personale per la sicurezza informatica rispetto ad altri settori regolamentati.

Per fare un confronto, nel 2019, il bilancio federale degli Stati Uniti ha stanziato 15 miliardi di $ per attività legate alla sicurezza informatica, con un aumento del 4,1% rispetto all'esercizio 2018. Tuttavia, la sanità ha visto dedicarsi solo il 5% del budget speso per la sicurezza.

Un recente sondaggio dell'HIMSS (Healthcare Information and Management Systems Society), ha tuttavia individuato notizie migliori. Nel rapporto del 2019, risulta che *"si stanno verificando molti progressi positivi nelle pratiche di cyber security sanitaria e le organizzazioni sanitarie sembrano stanziare budget più alti per la loro sicurezza"*.

Per quanto la spesa per la cyber security venga spesso vista in maniera molto simile all'acquisto di un'assicurazione, le sempre più crescenti minacce informatiche rivolte al settore sanitario si stanno lentamente traducendo in cambiamenti di atteggiamento e aumento dei budget.

Un intervento troppo lento, tuttavia, può tradursi in una catastrofe nel medio e lungo termine. Un recente studio del Ponemon Institute ha rilevato che le violazioni dei dati sanitari sono aumentate del 5% nell'ultimo anno e il costo dei dati esposti è stato di 429 $ per singolo record.

1.8 MANCANZA DI LEADERSHIP

Molti operatori sanitari non dispongono ancora un dirigente esecutivo assegnato alla sicurezza.

Un sondaggio HIMSS del 2019 sulla leadership e sulla forza lavoro, ha mostrato che la metà delle strutture non impiega un responsabile delle informazioni e della tecnologia (come ad es. un CISO).

La cosa va di pari passo con altri settori. Lo studio ISACA sullo stato della sicurezza informatica del 2020, ha rilevato che il 62% degli intervistati ha dichiarato come il proprio team di sicurezza informatica fosse “a corto di personale”.

Ad aggravare il problema, è anche la mancanza di qualifiche: Il 70% degli intervistati ha dichiarato che meno della metà dei candidati alla sicurezza erano ben qualificati per svolgere il lavoro. Naturalmente resta da capire quanto possa essere efficace un CISO con una mancanza di personale qualificato.

2. LA FORMAZIONE

La formazione sulla consapevolezza dei rischi è un prerequisito per molti standard di sicurezza. Inoltre, un efficace programma di sensibilizzazione sulla sicurezza aggiunge anche un considerevole valore alla strategia di sicurezza globale degli operatori sanitari.

L'elemento umano è spesso la causa principale di molte violazioni dei dati attraverso semplici errori come il download di malware. Insegnando agli operatori sanitari come rilevare le minacce informatiche, l'intera struttura sarà meglio attrezzata per prevenire violazioni dei dati.

Secondo il Data Breach Investigations Report del 2019 di Verizon, l'81% delle violazioni all'assistenza sanitaria sono state causate da errori vari, tra cui abuso di privilegi e vulnerabilità delle applicazioni web. Altri risultati includono:

- Il 33% di tutte le violazioni è stato causato da attacchi di Social Engineering;
- Il 32% delle violazioni è stato realizzato con attacchi di Phishing;
- Il 69% è stato perpetrato da aggressori esterni;
- Il 29% ha utilizzato credenziali sottratte.

I criminali hanno “umanizzato” i loro metodi di attacco e - come mostrano i dati - con grande successo.

Sfruttando driver comuni di comportamento umano, come l’entusiasmo, la distrazione, la curiosità e l’incertezza, gli hacker possono facilmente convincere gli utenti non sensibilizzati a condividere informazioni o installare malware.

2.1 CONSENSO ESECUTIVO

La sicurezza informatica oggi è sotto la responsabilità di un'ampia gamma di dirigenti C-level (CFO, CTO, CEO e COO), che riportano direttamente al consiglio di amministrazione dell'organizzazione e ad altri stakeholder.

Quando questi leader raggiungono il livello C, l'esperienza tecnica conta meno delle capacità di leadership e di business. Detengono ora più influenza, privilegi di più ampia portata, migliore accesso alle risorse, maggiore autonomia e maggior supporto da parte della dirigenza senior. Questa suite di persone ha le capacità di sfruttare competenze specializzate di settori specifici, come la consapevolezza della sicurezza.

I dirigenti non solo devono comprendere in che modo gli incidenti di sicurezza possono influire negativamente sui profitti della propria organizzazione, ma anche in che modo la formazione sulla consapevolezza può contribuire ad aggiungere valore sotto forma di fiducia e reputazione dei clienti.

Collegare una corretta formazione sulla sicurezza a questi obiettivi aziendali, può contribuire in maniera determinante a creare una cultura di protezione per l'intera organizzazione.

3. LA SITUAZIONE ITALIA

Con un comunicato stampa datato 1 Aprile 2020, il SISR (Sistema per l'Informazione e la Sicurezza della Repubblica) ha dichiarato di aver registrato una serie di *"attacchi informatici ai danni di strutture italiane d'eccellenza attualmente impegnate nel fronteggiare l'emergenza sanitaria relativa al Covid-19"*.

I sabotaggi si collocano all'interno di una tipologia di attacchi hacker che non hanno necessariamente l'obiettivo di sottrarre dati sensibili, bensì a scopo di lucro. Stiamo quindi parlando di Ransomware, un fenomeno di portata mondiale che sta ora interessando direttamente anche l'Italia.

La rete dei CSIRT (Computer Security Incident Response Teams) europei ha innalzato il livello d'allerta per l'aumento di cyber-crimini, che in questo particolare momento fanno leva su timori e confusione generale dei cittadini per la pandemia di Covid-19.

Per quanto siano le più grandi strutture sanitarie ad attirare oggi particolare attenzione, nessuna entità può considerarsi sicuro, dalla ricerca e distribuzione farmaceutica fino agli studi medici.

Le pagine che seguono descrivono 3 casi chiave accaduti sul suolo italiano nei primi mesi della pandemia di Covid-19 (Mar-Apr-Mag 2020).

3.1 ISTITUTO NAZIONALE MALATTIE INFETTIVE SPALLANZANI (ROMA)

Durante l'ultima settimana di Marzo, un attacco hacker indirizzato verso l'ospedale Spallanzani di Roma è stato sventato e neutralizzato in tempo.

L'attacco non era finalizzato alla sottrazione di dati, bensì a richieste di denaro a seguito dell'installazione di un Ransomware, intercettato prima che potesse propagarsi all'interno dell'intera struttura sanitaria.

L'utilizzo di Ransomware, che - come sappiamo - rappresenta una problematica mondiale, è una tipologia d'attacco estremamente efficace. Una volta infettato il primo sistema, infatti, il codice sorgente è in grado di propagarsi attraverso l'intera rete informatica, individuando automaticamente le condivisioni presenti e tentando di attaccare tutti i sistemi e i dispositivi raggiungibili.

Sebbene l'attacco sia stato sventato, è bene riflettere sulle logiche che hanno spinto i criminali informatici a scegliere proprio questa struttura sanitaria come bersaglio.

L'istituto Spallanzani è stato il primo ad isolare il Covid-19 e a metterlo a disposizione della comunità scientifica per consentire l'individuazione di cure adatte e indirizzare la preparazione di un vaccino.

Se l'attacco fosse andato a buon fine, è del tutto lecito chiedersi se il pagamento di un riscatto Ransomware sarebbe stato considerato "accettabile", dettato dall'importanza di poter riaccedere ai dati scientifici per la corsa contro il tempo dovuta alla pandemia.

3.2 AZIENDA OSPEDALIERA SAN CAMILLO - FORLANINI (ROMA)

Durante gli stessi giorni in cui un attacco Ransomware interessava l'ospedale Spallanzani, l'azienda ospedaliera San Camillo di Roma si è trovata a fare i conti con un sabotaggio alle apparecchiature informatiche del laboratorio per i test del Covid-19.

L'atto vandalico, questa volta andato a segno, è stato pubblicamente confermato dall'Assessore alla Sanità della Regione Lazio e ha causato lo stop dei test previsti sul virus, che sarebbero dovuti partire proprio la mattina successiva.

Il risultato dell'attacco ha visto la sottrazione di preziosi dati scientifici attraverso la totale rimozione di hard disk presenti all'interno di computer del laboratorio.

Si è trattato di un attacco premeditato, studiato a mente fredda, che è andato a colpire esattamente dove voleva, evidentemente supportato da un troppo facile accesso fisico al laboratorio e sprovvisto di misure di sicurezza atte ad impedirne l'ingresso.

Un tipico esempio, quindi, di come la sicurezza informatica non sia sufficiente all'interno di determinate strutture, dove anche la sicurezza fisica deve essere implementata in tutte le sue forme.

3.3 ISTITUTO SCIENTIFICO UNIVERSITARIO SAN RAFFAELE (MILANO)

L'attacco informatico subito dall'ospedale San Raffaele di Milano è probabilmente il più grave tra quelli ad oggi registrati. Reso pubblico il 21 Maggio, sembra però essere stato realizzato nel mese di Marzo.

Un noto gruppo hacker denominato LulzSec, ha postato via Twitter alcuni screenshot come prova del superamento delle difese di sicurezza informatica della struttura sanitaria milanese.

In base agli screenshot, i dati sottratti contenevano account e password del personale sanitario, oltre che codici fiscali e altri dati sensibili di pazienti ricoverati o semplicemente passati dall'accettazione.

Per quanto questi post possano apparire come tanti annunci per vantarsi del risultato, LulzSec più che segnalare le scarse difese del sistema di difesa, sembrava essere interessata a far scoppiare una polemica: *"Perché l'ospedale non ha ancora avvisato le autorità e contattato le persone interessate dal data breach?"*. Il GDPR, infatti, impone che questo avvenga entro 72 ore dalla scoperta.

A differenza di altri attacchi mossi da interessi di lucro, oppure dalla sottrazione di informazioni, questo caso è diverso. L'obiettivo di LulzSec è stato quello di mettere in evidenza un'altra questione: l'immobilità del San Raffaele che - a mesi dalla violazione - non avrebbe avvisato chi di dovere, nonostante vi siano leggi comunitarie che obbligano a farlo, per evitare pesanti sanzioni.

Per quanto non si possa escludere a priori che LulzSec abbia bluffato sui dati raccolti o il tempo effettivamente trascorso dall'attacco, il San Raffaele non ha né confermato né smentito e la questione è senza dubbio utile per prendere in considerazione la modalità di gestione di situazioni di questo tipo, per eventuali simili eventi futuri.

CONCLUSIONI

L'industria sanitaria è e rimarrà un obiettivo principale per gli hacker. Le strutture sanitarie ospitano una moltitudine di informazioni preziose ed **altamente commerciabili**, relative a pazienti e addetti ai lavori.

Le informazioni sanitarie a cui è possibile accedere attraverso innumerevoli endpoint vulnerabili, possono essere rivendute sul mercato nero molto prima che vengano rilevate le violazioni stesse.

Sebbene i quadri normativi e di sicurezza possano aiutare a proteggere i dati dei pazienti, in ultima analisi gli stessi dipendono da **persone e processi** per la gestione di informazioni sanitarie protette.

Un programma completo di sensibilizzazione alla sicurezza può aiutare le strutture sanitarie a contrastare molte delle preoccupazioni trattate in questo documento.

Con le giuste risorse e il supporto della leadership, la formazione sulla consapevolezza può insegnare al personale delle strutture come identificare, evitare e segnalare gli attacchi prima che si verifichino.

A una frazione del costo di una singola violazione di dati, gli operatori sanitari possono attivare specifici **programmi interni** per proteggere le proprie informazioni, mantenere la fiducia dei pazienti ed evitare pesanti ricadute reputazionali causate da una violazione dei dati.